## Contents

**Preface**

<table>
<thead>
<tr>
<th>Audience</th>
<th>xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation Accessibility</td>
<td>xx</td>
</tr>
<tr>
<td>Feature Limitations</td>
<td>xx</td>
</tr>
<tr>
<td>Related Resources</td>
<td>xxi</td>
</tr>
<tr>
<td>Conventions</td>
<td>xxi</td>
</tr>
</tbody>
</table>

**Part I  Get Started**

### 1 Get Started with Oracle Identity Cloud Service

<table>
<thead>
<tr>
<th>About Oracle Identity Cloud Service</th>
<th>1-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Oracle Identity Cloud Service Pricing Models</td>
<td>1-4</td>
</tr>
<tr>
<td>Understand the User Per Month Pricing Model</td>
<td>1-4</td>
</tr>
<tr>
<td>Understand the Active User Per Hour Pricing Model</td>
<td>1-9</td>
</tr>
<tr>
<td>About Multiple Instances</td>
<td>1-16</td>
</tr>
<tr>
<td>Before Creating a Secondary Instance</td>
<td>1-25</td>
</tr>
<tr>
<td>Create a Secondary Instance</td>
<td>1-26</td>
</tr>
<tr>
<td>Identify and Switch Instances</td>
<td>1-28</td>
</tr>
<tr>
<td>Modify a Secondary Instance</td>
<td>1-31</td>
</tr>
<tr>
<td>Remove a Secondary Instance</td>
<td>1-31</td>
</tr>
<tr>
<td>About Oracle Identity Cloud Service Concepts</td>
<td>1-32</td>
</tr>
<tr>
<td>Oracle Cloud Services</td>
<td>1-32</td>
</tr>
<tr>
<td>Identity Domain</td>
<td>1-33</td>
</tr>
<tr>
<td>SAML, OAuth, and OpenID Connect</td>
<td>1-34</td>
</tr>
<tr>
<td>SCIM</td>
<td>1-35</td>
</tr>
<tr>
<td>Other Oracle Identity Cloud Service Key Concepts</td>
<td>1-35</td>
</tr>
<tr>
<td>About Oracle Identity Cloud Service Interfaces</td>
<td>1-38</td>
</tr>
<tr>
<td>How to Begin with Oracle Identity Cloud Service Subscriptions</td>
<td>1-38</td>
</tr>
<tr>
<td>Supported Web Browsers</td>
<td>1-39</td>
</tr>
<tr>
<td>How to Access Oracle Identity Cloud Service</td>
<td>1-39</td>
</tr>
</tbody>
</table>
2 Understand Application Integration

What Is Application Integration? 2-1
Why Should You Integrate Your Applications? 2-2
What Are the Types of Application Integrations? 2-3
  Which Integration Method to Use? 2-3
  Integrate Oracle Identity Cloud Service with Applications from the App Catalog 2-4
    Why Integrate with SaaS Applications? 2-5
    What Is the App Catalog? 2-5
    What Are the Advantages of Using the App Catalog? 2-5
Use Bridges to Integrate Oracle Identity Cloud Service with Microsoft Active Directory (AD) and an Enterprise LDAP 2-5
  Why Integrate with Microsoft Active Directory (AD) and an Enterprise LDAP? 2-6
  What Are the Types of On-Premises Application Integrations? 2-6
Use the SCIM Interface to Integrate Oracle Identity Cloud Service with Custom Applications 2-6
  Why Integrate with Custom Applications? 2-7
  What Is SCIM? 2-7
  Why Use SCIM? 2-8
  How Do You Use the Generic SCIM App Template? 2-9
Part II  Perform User Tasks

3  Configure User Settings

Typical Workflow for Configuring User Settings  3-1
Change Your Password  3-2
Recover Your Account  3-3
Set Up or Modify Your Profile  3-3
Set Your Email Options  3-4
Set Your Security Options  3-4
  Set Your Account Recovery Options  3-4
    Set a Recovery Email Address as an Account Recovery Factor  3-5
    Set Your Mobile Number as an Account Recovery Factor  3-6
    Set Security Questions as an Account Recovery Factor  3-7
    Modify Your Recovery Email Address  3-7
    Modify Your Mobile Number  3-7
    Modify Your Security Questions  3-8
Remove Your Mobile Number as an Account Recovery Factor  3-8
Remove Security Questions As an Account Recovery Factor  3-9
Understand Social Login  3-9
  Use Case: Log in Using Social Login  3-9
  Use Case: Link Social Accounts  3-10
  Use Case: Unlink Social Accounts  3-10
  Link and Unlink Social Accounts  3-11
Access My Apps  3-11
  Use Form Fill Applications  3-11
Manage Group and Application Access  3-12
  Request Group and Application Access  3-13
  View Group and Application Access  3-13
  View Group and Application Access Requests  3-13
Access Your Consents  3-13

4  Manage 2-Step Verification

Typical Workflow for Managing 2–Step Verification  4-1
Enroll in 2–Step Verification for Your Account  4-2
  Set Up a Mobile Number As An Authentication Method  4-3
  Use a Mobile Number as an Authentication Method  4-3
Set Up the Oracle Mobile Authenticator App as an Authentication Method 4-4
Use the Oracle Mobile Authenticator App as an Authentication Method 4-4
Set Up a Third-Party Authenticator App as an Authentication Method 4-6
Use a Third-Party Authenticator App as an Authentication Method 4-6
Set Up Security Questions as an Authentication Method 4-7
Use Security Questions as an Authentication Method 4-8
Set Up Email as an Authentication Method 4-8
Use Email as an Authentication Method 4-9
Add Backup Verification Methods 4-10
Trust a Device 4-10
Set a Default Verification Method 4-10
Change Your Default Verification Method During Login 4-11
Manage 2–Step Verification from the My Profile Console 4-11
  Add a 2–Step Verification Method from the My Profile Console 4-12
  Remove a 2–Step Verification Method 4-12
  Rename a 2–Step Verification Method 4-13
  Manage Security Questions 4-13
  Generate a Bypass Code 4-13
  Use a Bypass Code 4-14
  Remove a Trusted Device 4-14
  Set a Default Verification Method 4-15
  Change Your Default Verification Method Using the My Profile Console 4-15

5 Use the Oracle Mobile Authenticator App

Typical Workflow for Managing the Oracle Mobile Authenticator App 5-1
Use the Oracle Mobile Authenticator App 5-1
  Add an Account to the OMA App by Scanning the QR Code 5-2
  Add an Account to the OMA App by Entering the Key Manually 5-2
  Add an Account to the OMA App Using the Enrollment URL 5-3
Manage the Oracle Mobile Authenticator App 5-3
  Switch Between Grid View and List View 5-3
  Manually Check for Pending Notifications 5-4
  Edit Accounts in the OMA App 5-4
  Sync an Account 5-4
  Reorder Accounts in the OMA App 5-5
  Delete an Account in the OMA App 5-5
  Enable App Protection 5-6
  Change Your OMA App PIN 5-7
  Disable OMA App PIN Protection 5-7
Part III  Perform Identity Administration

6  Manage Oracle Identity Cloud Service Users

   Typical Workflow for Managing Oracle Identity Cloud Service Users  6-2
   Understand the User Life Cycle  6-3
   Understand Administrator Roles  6-6
   Create User Accounts  6-8
   View Details About User Accounts  6-9
   Edit Attribute Values for the User Account  6-13
   Assign Groups to the User Account  6-14
   Remove Groups from the User Account  6-15
   Assign Applications to the User Account  6-15
   Remove Applications from the User Account  6-16
   Activate User Accounts  6-16
   Deactivate User Accounts  6-17
   Import User Accounts  6-17
   Export User Accounts  6-19
   Generate Bypass Codes for User Accounts  6-21
   Reset Authentication Factors for User Accounts  6-22
   Unlock User Accounts  6-22
   Add or Remove a User Account from an Administrator Role  6-23
   Generate Personal Access Tokens  6-23
   Send Invitations to Users to Activate Their Accounts  6-24
   Reset Passwords for User Accounts  6-25
   Remove User Accounts  6-25

7  Manage Oracle Identity Cloud Service Groups

   Typical Workflow for Managing Oracle Identity Cloud Service Groups  7-1
   Understand Groups  7-2
   Create Groups  7-3
   View Details About Groups  7-3
   Edit Attribute Values for the Group  7-4
   Assign User Accounts to the Group  7-4
   Remove User Accounts from the Group  7-5
   Assign Applications to the Group  7-5
   Remove Applications from the Group  7-6
   Import Groups  7-6
# Manage Oracle Identity Cloud Service Applications

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Workflow for Managing Oracle Identity Cloud Service Applications</td>
<td>8-1</td>
</tr>
<tr>
<td>Understand Cloud Applications</td>
<td>8-2</td>
</tr>
<tr>
<td>About Cloud Applications</td>
<td>8-3</td>
</tr>
<tr>
<td>About Oracle and Custom Applications</td>
<td>8-3</td>
</tr>
<tr>
<td>About Enterprise Applications</td>
<td>8-4</td>
</tr>
<tr>
<td>About the Relationship Between Oracle Identity Cloud Service and Applications</td>
<td>8-4</td>
</tr>
<tr>
<td>Architecture: SAML and Provisioning Integration with Oracle Identity Cloud Service</td>
<td>8-5</td>
</tr>
<tr>
<td>Architecture Diagram Defining Oracle Identity Cloud Service and SAML Integration</td>
<td>8-5</td>
</tr>
<tr>
<td>Architecture Diagram Defining Oracle Identity Cloud Service and Provisioning Integration</td>
<td>8-7</td>
</tr>
<tr>
<td>Use Case: Adding Applications</td>
<td>8-8</td>
</tr>
<tr>
<td>About Adding Applications</td>
<td>8-9</td>
</tr>
<tr>
<td>Add Applications</td>
<td>8-10</td>
</tr>
<tr>
<td>Add a Confidential Application</td>
<td>8-11</td>
</tr>
<tr>
<td>Configure Authorized Resources</td>
<td>8-19</td>
</tr>
<tr>
<td>Access All Resources</td>
<td>8-20</td>
</tr>
<tr>
<td>Access Resources With Matching Tags</td>
<td>8-21</td>
</tr>
<tr>
<td>Access Resources With Specific Scopes</td>
<td>8-22</td>
</tr>
<tr>
<td>Add a Mobile Application</td>
<td>8-22</td>
</tr>
<tr>
<td>Add a SAML Application</td>
<td>8-27</td>
</tr>
<tr>
<td>Upgrade a SAML Application</td>
<td>8-34</td>
</tr>
<tr>
<td>Secure Enterprise Applications with App Gateway</td>
<td>8-34</td>
</tr>
<tr>
<td>Typical Workflow for Securing Enterprise Applications with App Gateway</td>
<td>8-34</td>
</tr>
<tr>
<td>Understand App Gateway</td>
<td>8-35</td>
</tr>
<tr>
<td>Secure Enterprise Applications</td>
<td>8-39</td>
</tr>
<tr>
<td>How to Use App Gateway</td>
<td>8-46</td>
</tr>
<tr>
<td>How to Enable and Access App Gateway Logs</td>
<td>8-55</td>
</tr>
<tr>
<td>Troubleshoot App Gateway</td>
<td>8-57</td>
</tr>
<tr>
<td>About the App Catalog Application</td>
<td>8-58</td>
</tr>
<tr>
<td>Add an App Catalog Application</td>
<td>8-58</td>
</tr>
<tr>
<td>Enable Provisioning for an App Catalog Application</td>
<td>8-60</td>
</tr>
<tr>
<td>Enable Synchronization for an App Catalog Application</td>
<td>8-62</td>
</tr>
<tr>
<td>Import User Accounts from a Software as a Service Application</td>
<td>8-62</td>
</tr>
<tr>
<td>Synchronize User Accounts</td>
<td>8-63</td>
</tr>
<tr>
<td>Work with the Synchronization Failure Report</td>
<td>8-64</td>
</tr>
<tr>
<td>Add Tags to an Application</td>
<td>8-65</td>
</tr>
</tbody>
</table>
9 Manage Oracle Identity Cloud Service Jobs

Understand Bulk Loading Data 9-1
Typical Workflow for Bulk Loading Data 9-1
Use Best Practices for Bulk Loading Data 9-3
  Bulk Loading File Specifications 9-3
  Sample Files 9-5
  Workflow 9-6
  Deactivate Notifications 9-6
  Testing 9-6
View Jobs and Job Details 9-6
Export Job Errors 9-7

10 Run Oracle Identity Cloud Service Reports

Typical Workflow for Running Oracle Identity Cloud Service Reports 10-1
Understand the Types of Reports 10-1
Organize the Report Data 10-2
Run Reports 10-2
  Run the Successful Login Attempts Report 10-3
  Run the Unsuccessful Login Attempts Report 10-3
  Run the Application Access Report 10-4
  Run the Application Role Privileges Report 10-4
  Run the Diagnostic Data Report 10-5

Part IV Configure Administrator Settings

11 Change Oracle Identity Cloud Service Default Settings

Change Default Settings 11-1
Purge Audit Data for the Deleted User 11-2
Obtain the Root CA Certificate from Oracle Identity Cloud Service 11-2

12 Manage User Settings in Oracle Identity Cloud Service

Typical Workflow for Managing User Settings in Oracle Identity Cloud Service 12-1
Change User Settings 12-1
## Manage Oracle Identity Cloud Service Trusted Partner Certificates

Typical Workflow for Managing Oracle Identity Cloud Service Trusted Partner Certificates
Understand Trusted Partner Certificates
Import a Trusted Partner Certificate
View Details About a Trusted Partner Certificate
Delete a Trusted Partner Certificate

## Customize Oracle Identity Cloud Service Notifications

Typical Workflow for Customizing Oracle Identity Cloud Service Notifications
Understand the Types of Notifications
  - About User Notifications
  - About Administrator Notifications
Understand How to Customize Notifications
Activate Notifications
Select Notifications
Specify Recipients for Notifications
Modify Notification Templates
Verify Notifications
Deactivate Notifications

## Manage Oracle Identity Cloud Service Password Policies

Typical Workflow for Managing Oracle Identity Cloud Service Password Policies
Understand the Types of Password Policies
Understand the Criteria for Password Policies
Set the Password Policy for Your Identity Domain
Test a Password Policy
Modify the Custom Password Policy
Evaluate Password Policies

## Brand the Oracle Identity Cloud Service Interface

Typical Workflow for Branding the Oracle Identity Cloud Service Interface
Customize the Sign In Page
Brand the Consoles
Brand Notification Templates
## Manage Provisioning Bridges for Oracle Identity Cloud Service

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Workflow for Managing Provisioning Bridges for Oracle Identity Cloud Service</td>
<td>17-1</td>
</tr>
<tr>
<td>Understand the Provisioning Bridge</td>
<td>17-2</td>
</tr>
<tr>
<td>Why Use the Provisioning Bridge?</td>
<td>17-5</td>
</tr>
<tr>
<td>Create a Provisioning Bridge</td>
<td>17-6</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>17-6</td>
</tr>
<tr>
<td>Create a Provisioning Bridge</td>
<td>17-6</td>
</tr>
<tr>
<td>Start a Provisioning Bridge</td>
<td>17-10</td>
</tr>
<tr>
<td>Start the Provisioning Bridge on a Generic Machine</td>
<td>17-10</td>
</tr>
<tr>
<td>Start in Normal Mode</td>
<td>17-10</td>
</tr>
<tr>
<td>Start in Background Mode</td>
<td>17-11</td>
</tr>
<tr>
<td>Start the Provisioning Bridge on a Windows Machine</td>
<td>17-12</td>
</tr>
<tr>
<td>View Details About a Provisioning Bridge</td>
<td>17-13</td>
</tr>
<tr>
<td>Activate and Deactivate Provisioning Bridges</td>
<td>17-14</td>
</tr>
<tr>
<td>Activate Provisioning Bridges</td>
<td>17-14</td>
</tr>
<tr>
<td>Deactivate Provisioning Bridges</td>
<td>17-15</td>
</tr>
<tr>
<td>Modify a Provisioning Bridge</td>
<td>17-15</td>
</tr>
<tr>
<td>Modify a Provisioning Bridge</td>
<td>17-15</td>
</tr>
<tr>
<td>Assign a Provisioning Bridge to Apps</td>
<td>17-16</td>
</tr>
<tr>
<td>Change the Provisioning Bridge Assigned to Apps</td>
<td>17-17</td>
</tr>
<tr>
<td>Stop a Provisioning Bridge</td>
<td>17-18</td>
</tr>
<tr>
<td>Remove Provisioning Bridges</td>
<td>17-20</td>
</tr>
<tr>
<td>Manage Log Files for a Provisioning Bridge</td>
<td>17-20</td>
</tr>
</tbody>
</table>

## Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Workflow for Managing Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service</td>
<td>18-1</td>
</tr>
<tr>
<td>About the Microsoft Active Directory (AD) Bridge</td>
<td>18-3</td>
</tr>
<tr>
<td>Understand the Microsoft Active Directory (AD) Bridge</td>
<td>18-3</td>
</tr>
<tr>
<td>Certified Components</td>
<td>18-5</td>
</tr>
<tr>
<td>Statuses</td>
<td>18-6</td>
</tr>
<tr>
<td>Hardware Requirements</td>
<td>18-6</td>
</tr>
<tr>
<td>Why Use the Microsoft Active Directory (AD) Bridge?</td>
<td>18-7</td>
</tr>
<tr>
<td>Set Permissions for Your Microsoft Active Directory (AD) Account</td>
<td>18-7</td>
</tr>
<tr>
<td>Set Permissions to Synchronize Users, Groups, and Group Membership</td>
<td>18-8</td>
</tr>
<tr>
<td>Set Permissions to Propagate Changes to Microsoft Active Directory</td>
<td>18-9</td>
</tr>
<tr>
<td>Set Permissions for Delegated Authentication</td>
<td>18-9</td>
</tr>
<tr>
<td>Create a Microsoft Active Directory (AD) Bridge</td>
<td>18-10</td>
</tr>
</tbody>
</table>
Configure a Microsoft Active Directory (AD) Bridge 18-14
Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge 18-18
Run a Microsoft Active Directory (AD) Bridge 18-21
View Details About a Microsoft Active Directory (AD) Bridge 18-22
Activate and Deactivate Microsoft Active Directory (AD) Bridges 18-23
  Activate a Microsoft Active Directory (AD) Bridge 18-23
  Deactivate a Microsoft Active Directory (AD) Bridge 18-23
  Activate All Microsoft Active Directory (AD) Bridges 18-24
  Deactivate All Microsoft Active Directory (AD) Bridges 18-24
Modify a Microsoft Active Directory (AD) Bridge 18-24
  Modify a Microsoft Active Directory (AD) Bridge 18-25
Remove a Microsoft Active Directory (AD) Bridge 18-26
Understand Best Practices for the Microsoft Active Directory (AD) Bridge 18-28
  Create and Manage Log Files for the Microsoft Active Directory (AD) Bridge 18-28
  Maintain the Microsoft Active Directory (AD) Bridge 18-29
    Transfer the Microsoft Active Directory (AD) Bridge 18-29
    Restart the Microsoft Active Directory (AD) Bridge 18-29

19 Manage Oracle Identity Cloud Service Session Settings
  Change Session Settings 19-1

20 Manage Self-Registration Profiles in Oracle Identity Cloud Service
  Typical Workflow for Managing Self-Registration Profiles 20-1
  Understand Self-Registration Profiles 20-2
  Create Self-Registration Profiles 20-2

21 Download Oracle Identity Cloud Service SDKs and Applications
  Typical Workflow for Downloading Oracle Identity Cloud Service SDKs and Applications 21-1
  Understand Oracle Identity Cloud Service SDKs and Applications 21-3
  Download Oracle Identity Cloud Service SDKs and Applications 21-5
  Use Oracle Identity Cloud Service SDKs and Applications 21-6

22 Customize Schemas in Oracle Identity Cloud Service
  Add Custom Schema Attributes 22-1
  Edit Custom Schema Attributes 22-2
Part V Configure Security Settings

23 Manage Terms of Use

- Understand Terms of Use 23-1
- Add a Terms of Use 23-1
- View Details of Terms of Use 23-2
- Modify Terms of Use 23-2
- Remove Terms of Use 23-3
- Activate and Deactivate Terms of Use 23-3

24 Manage Adaptive Security in Oracle Identity Cloud Service

- Typical Workflow for Managing Adaptive Security in Oracle Identity Cloud Service 24-1
- Understand Adaptive Security 24-3
- Why Use Adaptive Security? 24-3
- Activate and Deactivate Adaptive Security 24-3
  - Activate Adaptive Security 24-4
  - Deactivate Adaptive Security 24-4
- Understand Risk Providers 24-4
- Configure Oracle Identity Cloud Service Risk Events 24-5
- View Details About a Risk Provider 24-8
- Add a Third-Party Risk Provider 24-8
- Activate and Deactivate Risk Providers 24-10
  - Activate a Risk Provider 24-10
  - Deactivate a Risk Provider 24-11
- Modify a Third-Party Risk Provider 24-11
- Remove a Third-Party Risk Provider 24-12

25 Manage Oracle Identity Cloud Service Identity Providers

- Typical Workflow for Managing Oracle Identity Cloud Service Identity Providers 25-1
- Understand Identity Providers 25-2
  - About Digital Certificates 25-2
  - About Identity Providers 25-2
- Add an Identity Provider 25-3
  - Import Metadata for a SAML Identity Provider 25-4
  - Enter Metadata for a SAML Identity Provider 25-7
  - Create a SAML Partner and CRL Validation 25-8
    - For Releases 17.4.4 and Greater 25-9
- Add a Social Identity Provider 25-9
26 Manage Oracle Identity Cloud Service Identity Provider Policies

Typical Workflow for Managing Oracle Identity Cloud Service Identity Provider Policies 26-1
Understand Identity Provider Policies 26-2
Add an Identity Provider Policy 26-3
View Details About an Identity Provider Policy 26-4
Modify an Identity Provider Policy 26-4
  Change the Policy Name 26-5
  Assign Identity Providers to the Policy 26-5
  Remove Identity Providers from the Policy 26-5
  Assign Apps to the Policy 26-5
  Remove Apps from the Policy 26-6
Remove Identity Provider Policies 26-6

27 Manage Oracle Identity Cloud Service Sign-On Policies

Typical Workflow for Managing Oracle Identity Cloud Service Sign-On Policies 27-1
Understand Sign-On Policies 27-2
Add a Sign-On Policy 27-3
View Details About a Sign-On Policy 27-8
Activate and Deactivate Sign-On Policies 27-9
  Activate Sign-On Policies 27-9
  Deactivate Sign-On Policies 27-9
Modify a Sign-On Policy 27-10
  Change the Policy Name and Description 27-10
  Add Sign-On Rules to the Policy 27-10
  Change the Priority of a Sign-On Rule for the Policy 27-10
  Edit a Sign-On Rule for the Policy 27-11
  Remove Sign-On Rules from the Policy 27-11
  Assign Apps to the Policy 27-11
  Remove Apps from the Policy 27-12
Remove Sign-On Policies 27-12
<table>
<thead>
<tr>
<th>Page</th>
<th>Manage Oracle Identity Cloud Service Network Perimeters</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Typical Workflow for Managing Oracle Identity Cloud Service Network Perimeters 28-1</td>
</tr>
<tr>
<td></td>
<td>Understand Network Perimeters 28-2</td>
</tr>
<tr>
<td></td>
<td>Add a Network Perimeter 28-3</td>
</tr>
<tr>
<td></td>
<td>View Details About a Network Perimeter 28-3</td>
</tr>
<tr>
<td></td>
<td>Modify a Network Perimeter 28-4</td>
</tr>
<tr>
<td></td>
<td>Remove Network Perimeters 28-4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page</th>
<th>Manage Oracle Identity Cloud Service App Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Typical Workflow for Managing Oracle Identity Cloud Service App Gateways 29-1</td>
</tr>
<tr>
<td></td>
<td>What is App Gateway? 29-2</td>
</tr>
<tr>
<td></td>
<td>Register an App Gateway 29-2</td>
</tr>
<tr>
<td></td>
<td>View Details About an App Gateway 29-4</td>
</tr>
<tr>
<td></td>
<td>Activate and Deactivate App Gateways 29-4</td>
</tr>
<tr>
<td></td>
<td>Activate App Gateways 29-5</td>
</tr>
<tr>
<td></td>
<td>Deactivate App Gateways 29-5</td>
</tr>
<tr>
<td></td>
<td>Modify an App Gateway 29-5</td>
</tr>
<tr>
<td></td>
<td>Remove App Gateways 29-6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page</th>
<th>Manage Account Recovery in Oracle Identity Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Typical Workflow for Managing Account Recovery in Oracle Identity Cloud Service 30-1</td>
</tr>
<tr>
<td></td>
<td>Configure Account Recovery 30-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page</th>
<th>Manage Oracle Identity Cloud Service Multi-Factor Authentication Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Typical Workflow for Managing Oracle Identity Cloud Service Security Settings 31-1</td>
</tr>
<tr>
<td></td>
<td>Understand Multi-Factor Authentication 31-2</td>
</tr>
<tr>
<td></td>
<td>Configure Multi-Factor Authentication Settings 31-2</td>
</tr>
<tr>
<td></td>
<td>Configure Authentication Factors 31-3</td>
</tr>
<tr>
<td></td>
<td>Learn About Using Mobile Authenticator Apps with MFA 31-3</td>
</tr>
<tr>
<td></td>
<td>Configure Mobile OTP and Notifications 31-5</td>
</tr>
<tr>
<td></td>
<td>Configure Security Questions 31-5</td>
</tr>
<tr>
<td></td>
<td>Configure Text Message (SMS) Settings 31-6</td>
</tr>
<tr>
<td></td>
<td>Configure Email Settings 31-6</td>
</tr>
<tr>
<td></td>
<td>Multi-Factor Authentication Authorization Flow 31-7</td>
</tr>
</tbody>
</table>
Troubleshoot App Gateway

I Made Changes in Oracle Identity Cloud Service but the App Gateway Server Doesn't Reflect the Changes

Error Log Files Contain Invalid_session Message

Error Log Files Contain GET 127.0.0.1:53 Command Responding Error Number 500

37 Supported Languages

Part VII Complete Oracle Identity Cloud Service Scenarios

38 Enable Multi-Factor Authentication Security for Oracle Cloud

Scenario Description
Understand MFA Options in Oracle Identity Cloud Service
Create the Partners Group
Enable the Factors
Configure MFA for Email
Configure MFA for the Mobile Authenticator App
Create Users
Verify that Users Can Access Oracle Cloud
Generate and Use the Bypass Code

39 Migrate from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service

Typical Workflow for Migrating from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service
About Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service
About Migrating Services from a Traditional Cloud Account to a Cloud Account with Identity Cloud Service
Before You Begin
Migrate Users
Migrate Role Memberships
Migrate Identity Domain Administrator Roles
Provision and Synchronize Users Between Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service
Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service
Manage Linux Authentication using the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)

Typical Workflow for Managing the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) 40-1
- About the PAM 40-2
- What is the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)? 40-2
- Why use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) 40-2
- Certified Components 40-3

Install and Configure the PAM 40-3
- Download the PAM 40-3
- Install the PAM 40-3
- Configure a Confidential Application 40-4
- Create a Wallet 40-5
- Configure the PAM 40-5
  - Configure the PAM using SSSD 40-6
  - Configure the PAM using NSCD 40-8

Configure PAM-enabled Groups and Users 40-10
- Obtain an Access Token 40-10
- Create a Group with POSIX Attributes 40-10
- Create a User with POSIX Attributes and Add to Group 40-11
- Add POSIX Attributes to Existing Groups 40-13
- Add POSIX Attributes to Existing Users 40-15
- Verify Endpoints 40-17

Test Authentication into Linux Using Oracle Identity Cloud Service 40-20
Enable Multi-Factor Authentication to Authenticate into Linux 40-20
Preface

Welcome to Administering Oracle Identity Cloud Service.

This guide is intended for all users of Oracle Identity Cloud Service, whether you are an identity domain administrator, security administrator, application administrator, user administrator, user manager, audit administrator, or user.

Topics:
- Audience
- Documentation Accessibility
- Feature Limitations
- Related Resources
- Conventions

Audience

This document is primarily for users who perform administrative functionalities with Oracle Identity Cloud Service. These users are responsible for managing user accounts, groups, applications, notifications, password policies, bridges, identity providers, trusted partners, and reports in Oracle Identity Cloud Service.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Feature Limitations

This guide documents the complete set of Oracle Identity Cloud Service features. Your localized version of Oracle Identity Cloud Service might contain a subset of these features. Therefore, you might find features in this documentation that are not available in your localized version of Oracle Identity Cloud Service.
Related Resources

- Oracle Identity Cloud Service Tutorials and Infographics
- Oracle Identity Cloud Service Videos
- REST API for Oracle Identity Cloud Service
- Known Issues for Oracle Identity Cloud Service
- What’s New for Oracle Identity Cloud Service

Conventions

The following text conventions are used in this guide:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><code>monospace</code></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Part I
Get Started

Learn how to get started with Oracle Identity Cloud Service.

Chapters:

• Get Started with Oracle Identity Cloud Service
• Understand Application Integration
Get Started with Oracle Identity Cloud Service

The following sections describe how to get started with Oracle Identity Cloud Service for Oracle Cloud administrators and users. A reasonable level of familiarity with Oracle Cloud services is assumed.

Topics:

• About Oracle Identity Cloud Service
• About Oracle Identity Cloud Service Pricing Models
• About Multiple Instances
• About Oracle Identity Cloud Service Concepts
• About Oracle Identity Cloud Service Interfaces
• How to Begin with Oracle Identity Cloud Service Subscriptions
• How to Access Oracle Identity Cloud Service
• Access Service Consoles
• About Oracle Identity Cloud Service User Accounts and Groups
• About Oracle Identity Cloud Service Applications and Application Roles
• Typical Workflow for Using Oracle Identity Cloud Service

About Oracle Identity Cloud Service

Oracle Identity Cloud Service provides identity management, single sign-on (SSO), and identity governance for applications on-premises, in the cloud, or for mobile devices. Employees and business partners can access applications at any time, from anywhere, and on any device in a secure manner. Oracle Identity Cloud Service integrates directly with existing directories and identity management systems, and makes it easy for users to get access to applications. It provides the security platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Human Capital Management (HCM) and Oracle Sales Cloud, and platform services such as Oracle Java Cloud Service, Oracle Business Intelligence (BI) Cloud Service, and others.

Administrators and users can use Oracle Identity Cloud Service to help them effectively and securely create, manage, and use a cloud-based identity management environment without worrying about setting up any infrastructure or platform details.

Using Oracle Identity Cloud Service, you can:

• **Perform self-service capabilities.** Set up or modify your profile, change your password, set your primary email address, set your account recovery options, enroll in 2-Step Verification, link your social login accounts to your Oracle Identity Cloud Service user accounts if you're using social login, access all apps assigned
to you, activate your deactivated account, and unlock your account. See Configure User Settings.

- **Manage 2–Step Verification:** Configure security settings for 2–Step Verification for your user account. See Manage 2-Step Verification.

- **Work with the Oracle Mobile Authenticator (OMA) app:** Use this app to increase your security by providing a second verification method to sign in to Oracle Identity Cloud Service. See Use the Oracle Mobile Authenticator App.

- **Manage your users, groups, and applications.** Tailor the relationships that your users and groups have with your cloud-based Oracle applications and custom applications. See About Oracle Identity Cloud Service User Accounts and Groups and About Oracle Identity Cloud Service Applications and Application Roles.

- **Manage jobs.** Bulk load data from other repositories into Oracle Identity Cloud Service, view jobs and job details, and export job errors. See Managing Oracle Identity Cloud Service Jobs.

- **Run reports.** Run operational or historical reports that capture data about Oracle Identity Cloud Service. See Running Oracle Identity Cloud Service Reports.

- **Manage default settings.** Change the default and session settings for your identity domain. See Change Oracle Identity Cloud Service Default Settings.

- **Manage user settings.** Change settings for user accounts. See Manage User Settings in Oracle Identity Cloud Service.

- **Manage certificates for your trusted partners.** Oracle Identity Cloud Service uses trusted partner certificates that have Distinguished Encoding Rules (DER) file extensions. See Manage Oracle Identity Cloud Service Trusted Partner Certificates.

- **Customize notifications.** Create and send notifications to administrators and users using the supplied email templates. Tailor the recipients and content of these notifications to meet your business and security requirements. See Customize Oracle Identity Cloud Service Notifications.

- **Manage password policies.** Create and manage password policies that are applicable for all users in an identity domain. For all new users, Oracle Identity Cloud Service validates their passwords against your password policy to verify that those passwords meet the criteria for the policy. Adjust the strength of your password policy as needed to ensure a strong, secure environment. See Managing Oracle Identity Cloud Service Password Policies.

- **Customize the UI.** In addition to notifications and password policies, you can customize the Sign In page and Identity Cloud Service console. See Customizing the Oracle Identity Cloud Service Interface.

- **Manage bridges.** If you use Microsoft Active Directory as an authoritative source, then the bridge provides a link between your on-premises Microsoft Active Directory and Oracle Identity Cloud Service. Oracle Identity Cloud Service can reconcile with Microsoft Active Directory so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. The state of each record is synchronized between Microsoft Active Directory and Oracle Identity Cloud Service. See Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service.

- **Manage session settings.** Define session expiration, logout and logout redirect URLs, and configure Allow Cross-Origin Resource Sharing (CORS) to allow client applications that run on one domain to obtain data from another domain. See Managing Oracle Identity Cloud Service Session Settings.
• **Manage self-registration profiles.** Create self-registration profiles to manage different sets of users, approval policies, and applications in Oracle Identity Cloud Service. See Manage Self-Registration Profiles in Oracle Identity Cloud Service.

• **Download software development kits (SDKs) and applications.** Oracle Identity Cloud Service provides you with a centralized location in the Identity Cloud Service console where you can download:
  – SDKs, to authenticate and integrate your mobile and Web applications with Oracle Identity Cloud Service
  – The Oracle E-Business Suite (EBS) Asserter, to integrate Oracle E-Business Suite with Oracle Identity Cloud Service
  – The Secure Form Fill Client, to configure Secure Form Fill for your applications

See Download Oracle Identity Cloud Service SDKs and Applications.

• **Customize schemas.** Create, edit, and delete custom schema attributes. You may need to create a custom schema attribute, for example, when you are creating your own user interface and can't find a schema attribute that you need in the base Oracle Identity Cloud Service schema attributes. See Customize Schemas in Oracle Identity Cloud Service.

• **Manage adaptive security.** Manage default and custom risk providers that Oracle Identity Cloud Service uses to evaluate risk-based activity for Oracle Identity Cloud Service users, and generate a risk score for these users, based on this activity. This risk score is a number that varies from risk provider to risk provider, reflecting user threat. See Manage Adaptive Security in Oracle Identity Cloud Service.

• **Manage identity providers.** Add SAML 2.0 and social identity providers so that users can interact with Oracle Identity Cloud Service using websites that are external to Oracle Identity Cloud Service. See Manage Oracle Identity Cloud Service Identity Providers.

• **Manage identity provider policies.** Create identity provider policies to restrict which identity providers appear on the Sign In page when users are accessing particular apps. See Manage Oracle Identity Cloud Service Identity Provider Policies.

• **Manage sign-on policies.** Create sign-on policies to define criteria that Oracle Identity Cloud Service uses to allow or deny access to users for apps that are assigned to them. See Manage Oracle Identity Cloud Service Sign-On Policies.

• **Manage network perimeters.** Define network perimeters to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service. See Manage Oracle Identity Cloud Service Network Perimeters.

• **Manage account recovery.** Configure account recovery in Oracle Identity Cloud Service to help users regain access to their accounts if they have trouble signing in, they’re locked out, or they forget their passwords. See Manage Account Recovery in Oracle Identity Cloud Service.

• **Manage Multi-Factor Authentication settings.** Change the security settings such as Multi-Factor Authentication (MFA) for your identity domain. See Managing Oracle Identity Cloud Service Multi-Factor Authentication Settings.

• **Manage OAuth Settings.** Configure OAuth settings for your environments. See Managing Oracle Identity Cloud Service OAuth Settings Configuring Oracle Identity Cloud Service OAuth Settings.

• **Manage delegated authentication.** Use delegated authentication to enable users to use their Microsoft Active Directory passwords to sign in to Oracle Identity
Cloud Service to access resources and applications protected by Oracle Identity Cloud Service. See Configure Delegated Authentication in Oracle Identity Cloud Service.

- **Transfer configuration data.** Import and export configurations, entities, and customizations as an integral part of migrating an Oracle Identity Cloud Service environment. See Transferring Oracle Identity Cloud Service Configurations.

# About Oracle Identity Cloud Service Pricing Models

There are two pricing models for Oracle Identity Cloud Service:

- **User Per Month:** Beginning with version 18.4.2, Oracle Identity Cloud Service has a new pricing model for its customers. This pricing model bills users on the activity that they perform with Oracle Identity Cloud Service on a monthly basis. This not only streamlines projected billing calculations, but also helps customers to more accurately predict how much money they will spend for any given month.

- **Active User Per Hour:** This pricing model is for existing Oracle Identity Cloud Service customers (as of version 18.3.6). However, because of the benefits associated with the User per Month pricing model, these customers can opt to switch to this model.

## Understand the User Per Month Pricing Model

Learn about the pricing tiers for Oracle Identity Cloud Service for the User per Month pricing model and the features associated with each pricing tier.

For this pricing model, Oracle Identity Cloud Service has two pricing tiers:

- **Oracle Identity Cloud Service Foundation:** Oracle provisions this free version of Oracle Identity Cloud Service for customers that subscribe to Oracle Software-as-a-Service (SaaS), Oracle Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) applications. A customer can use this version to provide basic identity management functionalities, including user management, group management, password management, and basic reporting. For additional features, as indicated in the table below, a subscription to Oracle Identity Cloud Service Standard is required.

- **Oracle Identity Cloud Service Standard:** This licensed edition provides customers with an additional set of Oracle Identity Cloud Service features to integrate with other Oracle Cloud services, including Oracle Cloud SaaS and PaaS, custom applications hosted on-premises, on Oracle Cloud, or on a third-party cloud, as well as third-party SaaS applications. Features listed in this pricing tier are applicable for both Enterprise users and Consumer users.

An incentive of the Standard tier for the User per Month pricing model is the Bring Your Own License (BYOL) program. If you're an Oracle customer who's using certain Oracle identity management on-premises technologies and is paying support for these technologies, then you can subscribe to the BYOL Standard tier and use the features of this tier at the BYOL rate.

See Buying an Oracle Cloud Subscription for more information about the payment plans available with Oracle Identity Cloud Service.

The following table illustrates the features associated with each Oracle Identity Cloud Service pricing tier:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Foundation</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and Group Management</td>
<td>Manage the lifecycle of users and groups in Oracle Identity Cloud Service. Users and groups can be on-boarded manually or can be imported in bulk from a CSV file. You can grant user access to various applications by assigning users to the applications directly, or by assigning users to groups and groups to applications.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-Service Profile Management</td>
<td>Perform self-service capabilities to update user profile attributes, change passwords, manage linked social login accounts, view and manage devices registered for second-factor verification, and generate second-factor bypass codes.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-Service Password Reset</td>
<td>Perform self-service reset of users’ forgotten passwords. (using password challenge questions and answers)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-Service Password Reset</td>
<td>Perform self-service reset of users’ forgotten passwords. (using other factors, including SMS and push notifications)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO for Oracle Cloud Services</td>
<td>Authenticate to Oracle Identity Cloud Service and gain single-click access to Oracle Cloud services.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>External Identity Provider Federation</td>
<td>Configure a SAML 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO to Oracle Identity Cloud Service.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Basic User Provisioning and Synchronization for Oracle Cloud Apps</td>
<td>Provision user accounts to multiple Oracle SaaS and Oracle PaaS applications from a list of pre-configured provisioning templates in the App Catalog. You can also enable account synchronization to detect and synchronize any changes made directly on these target applications. Although you can use the provisioning templates, you can't change the default attribute mappings for provisioning and synchronization, or make any configuration changes to them.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Standard</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Sign-on Policies</td>
<td>Use these policies to define criteria that Oracle Identity Cloud Service uses to determine whether to allow a user to sign in to Oracle Identity Cloud Service or prevent a user from accessing Oracle Identity Cloud Service. By defining this criteria, you control access that users have to your applications based on conditions such as the identity providers that will be used to authenticate the users, the groups to which the users belong, whether the users are assigned to administrator roles in Oracle Identity Cloud Service, or whether the users are accessing Oracle Identity Cloud Service using an IP address that's contained in a network perimeter. Oracle Identity Cloud Service provides you with a default sign-on policy. In addition to the default sign-on policy, you can add sign-on policies and associate them with specific apps. When a user uses one of these apps to attempt to sign in to Oracle Identity Cloud Service, Oracle Identity Cloud Service checks to see if the app has any sign-on policies associated with it. If so, then Oracle Identity Cloud Service evaluates the criteria of the sign-on rules assigned to the policy. If there are no sign-on policies for the app, then the default sign-on policy is evaluated by Oracle Identity Cloud Service. (for the default sign-on policy) (for any sign-on policies that you add)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Application Development</td>
<td>Enable your mobile and web applications to authenticate to Oracle Identity Cloud Service by using software development kits (SDKs).</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Security and Usage Reports</td>
<td>Execute and view operational or historical reports that capture usage data about Oracle Identity Cloud Service users, and applications, and diagnostic level logs.</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Oracle Identity Manager Connector for Oracle Identity Cloud Service</td>
<td>Use this connector in Oracle Identity Manager to manage the complete lifecycle of users and groups in Oracle Identity Cloud Service from Oracle Identity Manager. This connector also enables access certification of SaaS resources, Segregation of Duties (SoD) violation checks during the request and approval process, and reports on SaaS app usage in Oracle Identity Manager.</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>App Catalog</td>
<td>The App Catalog is a collection of partially configured application templates for thousands of SaaS applications, such as Amazon Web Services and Google Suite. Using the templates, you can define an application, configure SSO, and configure provisioning. Oracle creates and maintains the App Catalog for you, and provides step-by-step instructions that will help you to configure your applications.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Identity Synchronization</td>
<td>Configure one or more Microsoft Active Directory bridges to synchronize user identities and groups with Oracle Identity Cloud Service.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Standard</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>User Self-Registration</td>
<td>Enable Business-to-Business (B2B) and Business-to-Consumer (B2C) users to register themselves to Oracle Identity Cloud Service. You can also create multiple self-registration profiles to manage different sets of users and access to applications.</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Self-Service Access Request</td>
<td>Enable users to request access to groups and applications from the App Catalog.</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>SSO for Third-Party Cloud Services</td>
<td>Authenticate to Oracle Identity Cloud Service and gain single-click access to third-party SaaS services configured using the App Catalog. The App Catalog is a collection of pre-seeded applications for popular SaaS applications, such as Amazon Web Services, Google Suite, Office 365, and so on, that support federation standards such as SAML 2.0 and OAuth 2.0. It also allows you to configure Secure Form Fill for applications that don't support these standards. Using the App Catalog, you can define the application, configure SSO, and configure provisioning. Oracle creates and maintains the App Catalog for you.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>SSO for Custom Applications</td>
<td>For custom applications developed using Oracle Cloud services and deployed on Oracle Cloud (PaaS and IaaS), authenticate to Oracle Identity Cloud Service and gain single-click access to these applications.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Delegated Authentication with Password Writeback</td>
<td>Remove the need to synchronize user passwords between an on-premises Microsoft Active Directory enterprise directory structure and Oracle Identity Cloud Service. Users can use their Microsoft Active Directory passwords to sign in to Oracle Identity Cloud Service to access resources and applications protected by Oracle Identity Cloud Service.</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Multi-Factor Authentication (MFA)</td>
<td>Enable strong authentication by configuring Multi-Factor Authentication (MFA) during user authentication. Configure device compliance policies and a wide variety of second factors, such as SMS, OTP, push notifications, and knowledge-based questions and answers.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Adaptive Security</td>
<td>Analyze contextual, risk, and threat information about the user, device, and network, and provide an intelligent, secure, and user-friendly way of providing access to corporate applications and resources. This also reduces the likelihood of online identity theft and fraud, which secures business applications even if the user's device or the user's account password is compromised.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Social Authentication</td>
<td>Configure one or more social identity providers so that users can log in to Oracle Identity Cloud Service with their social credentials.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Standard</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Advanced User Provisioning and Synchronization for Oracle Cloud Apps</td>
<td>Support interactive provisioning to allow administrators to grant entitlements and specify values for application account attributes. Administrators can also synchronize entitlements and other application data from the application into Oracle Identity Cloud Service. In addition to interactive provisioning and synchronization, you can customize the pre-configured provisioning templates in the App Catalog by changing the default attribute mappings for provisioning and synchronization and making configuration changes to them.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>User Provisioning and Synchronization for Third-Party Cloud Apps</td>
<td>Configure provisioning of user accounts to multiple third-party cloud apps, such as Google Suite, Office 365, and so on, from a list of pre-configured provisioning templates in the App Catalog. Enable account synchronization to detect and synchronize any changes made directly on these target applications.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>EBS Asserter</td>
<td>Integrate your Oracle E-Business Suite environment with Oracle Identity Cloud Service for authentication and password management purposes by using a lightweight Java application known as the Oracle E-Business Suite (EBS) Asserter.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Present disclaimers and acceptable use policies, also known as Terms of Use, to your users. Terms of Use helps you set the terms and conditions for your users to access your applications, based on user consent. This feature allows identity domain administrators to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service. You can configure Terms of Use on an application basis and collect consent from users before allowing them access to the application.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>App Gate</td>
<td>The Oracle Identity Cloud Service App Gate is a software appliance that you can use to provide Single Sign-On (SSO) and authorization for your on-premises applications. This enables you to use one appliance to provide SSO for multiple applications by allowing external users to access internal applications securely without the need for a VPN client. From the <a href="https://www.oracle.com">App Gateway for Identity Cloud Service</a> application, you can access the documentation for the App Gate. You can find this application on the <a href="https://www.oracle.com">Downloads</a> page of the Identity Cloud Service console. To access this page, in the Identity Cloud Service console, expand the <a href="https://www.oracle.com">Navigation Drawer</a>, click <a href="https://www.oracle.com">Settings</a>, and then click <a href="https://www.oracle.com">Downloads</a>.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Standard</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>WebGate</td>
<td>WebGate is a web-server plug-in that Oracle Access Management uses to protect on-premises web applications. It can be deployed on different web applications and web servers including, but not limited to, the Apache HTTP Server and Microsoft's Internet Information Services (IIS) web server. Instead of relying on Oracle Access Manager as an authentication service, WebGate can now interact with Oracle Identity Cloud Service to protect these applications by authenticating users to access the applications. When an unauthenticated user tries to access any applications that are protected by Oracle Identity Cloud Service, the user is redirected to the <strong>Sign In</strong> page of Oracle Identity Cloud Service for authentication.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Schema Extension</td>
<td>If you're creating your own UI, and can't find a schema attribute that you need from the base Oracle Identity Cloud Service schema attributes, then you can add your own custom attributes using the Identity Cloud Service console.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Generic SCIM App Template</td>
<td>With this template, you can provision or synchronize users between your custom applications and Oracle Identity Cloud Service. You can use this template to configure your custom applications so that the SCIM APIs are exposed, and you don't have to develop a single line of code. All that's required is to go to the App Catalog and search for a SCIM-managed app template. To use this template, you only have to provide your endpoint URL and the details that Oracle Identity Cloud Service requires to connect to your application, and then map the attributes between your application and Oracle Identity Cloud Service.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SMS Messaging</td>
<td>The total SMS message count is a pool based on the total number of users who have enabled MFA with SMS multiplied by the number of messages per user per month. Enterprise users are limited to 10 messages per user per month. Consumer users are limited to three messages per user per month. Any additional SMS messaging used beyond the limit is billed as additional Monthly users.</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Understand the Active User Per Hour Pricing Model**

Learn about the pricing tiers for Oracle Identity Cloud Service for the Active User per Hour pricing model and the features associated with each pricing tier.

For this pricing model, Oracle Identity Cloud Service has three pricing tiers:
• Oracle Identity Cloud Service Foundation: Oracle provisions this free version of Oracle Identity Cloud Service for customers that subscribe to Oracle Software-as-a-Service (SaaS), Oracle Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) applications. A customer can use this version to provide basic identity management functionalities, including user management, group management, password management, and basic reporting. For additional features, as indicated in the table below, a subscription to Oracle Identity Cloud Service Basic or Oracle Identity Cloud Service Standard is required.

• Oracle Identity Cloud Service Basic: This licensed edition provides all of the features of Oracle Identity Cloud Service Foundation plus the ability to synchronize Microsoft Active Directory user identities and groups into Oracle Identity Cloud Service.

• Oracle Identity Cloud Service Standard: This licensed edition provides customers with an additional set of Oracle Identity Cloud Service features to integrate with other Oracle Cloud services, including Oracle Cloud SaaS and PaaS, custom applications hosted on-premises, on Oracle Cloud, or on a third-party cloud, as well as third-party SaaS applications. Features listed in this pricing tier are applicable for both Enterprise users and Consumer users.

See Buying an Oracle Cloud Subscription for more information about the payment plans available with Oracle Identity Cloud Service.

The following table illustrates the features associated with each Oracle Identity Cloud Service pricing tier:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Foundation</th>
<th>Basic</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and Group Management</td>
<td>Manage the life cycle of users and groups in Oracle Identity Cloud Service. Users and groups can be onboarded manually or can be imported in bulk from a CSV file. You can grant user access to various applications by assigning users to the applications directly, or by assigning users to groups and groups to applications.</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Self-Service Profile Management</td>
<td>Perform self-service capabilities to update user profile attributes, change passwords, manage linked social login accounts, view and manage devices registered for second-factor verification, and generate second-factor bypass codes.</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Self-Service Password Reset</td>
<td>Perform self-service reset of users' forgotten passwords.</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SSO for Oracle Cloud Services</td>
<td>Authenticate to Oracle Identity Cloud Service and gain single-click access to Oracle Cloud services.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

(using password challenge questions and answers)

(using other factors, including SMS and push notifications)
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Foundation</th>
<th>Basic</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic User Provisioning and Synchronisation for Oracle Cloud Apps</td>
<td>Provision user accounts to multiple Oracle SaaS and Oracle PaaS applications from a list of pre-configured provisioning templates in the App Catalog. You can also enable account synchronization to detect and synchronize any changes made directly on these target applications. Although you can use the provisioning templates, you can’t change the default attribute mappings for provisioning and synchronization, or make any configuration changes to them.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Oracle Identity Manager Connector for Oracle Identity Cloud Service</td>
<td>Use this connector in Oracle Identity Manager to manage the complete life cycle of users and groups in Oracle Identity Cloud Service from Oracle Identity Manager. This connector also enables access certification of SaaS resources, Segregation of Duties (SoD) violation checks during the request and approval process, and reports on SaaS app usage in Oracle Identity Manager.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application Development SDKs</td>
<td>Enable your mobile and web applications to authenticate to Oracle Identity Cloud Service by using software development kits (SDKs).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security and Usage Reports</td>
<td>Execute and view operational or historical reports that capture usage data about Oracle Identity Cloud Service users, and applications, and diagnostic level logs.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>External Identity Provider Federation</td>
<td>Configure a SAML 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO to Oracle Identity Cloud Service.</td>
<td>✓ (for one SAML identity provider)</td>
<td></td>
<td>✓ (for more than one SAML identity provider)</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Basic</td>
<td>Standard</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Sign-on Policies</td>
<td>Use these policies to define criteria that Oracle Identity Cloud Service uses to determine whether to allow a user to sign in to Oracle Identity Cloud Service or prevent a user from accessing Oracle Identity Cloud Service. By defining this criteria, you control access that users have to your applications based on conditions such as the identity providers that will be used to authenticate the users, the groups to which the users belong, whether the users are assigned to administrator roles in Oracle Identity Cloud Service, or whether the users are accessing Oracle Identity Cloud Service using an IP address that's contained in a network perimeter. Oracle Identity Cloud Service provides you with a default sign-on policy. In addition to the default sign-on policy, you can add sign-on policies and associate them with specific apps. When a user uses one of these apps to attempt to sign in to Oracle Identity Cloud Service, Oracle Identity Cloud Service checks to see if the app has any sign-on policies associated with it. If so, then Oracle Identity Cloud Service evaluates the criteria of the sign-on rules assigned to the policy. If there are no sign-on policies for the app, then the default sign-on policy is evaluated by Oracle Identity Cloud Service. (for the default sign-on policy) (for any sign-on policies that you add)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identity Synchronization</td>
<td>Configure one or more Microsoft Active Directory bridges to synchronize user identities and groups with Oracle Identity Cloud Service.</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>App Catalog</td>
<td>The App Catalog is a collection of partially configured application templates for thousands of SaaS applications, such as Amazon Web Services and Google Suite. Using the templates, you can define an application, configure SSO, and configure provisioning. Oracle creates and maintains the App Catalog for you, and provides step-by-step instructions that will help you to configure your applications.</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>User Self-Registration</td>
<td>Enable Business-to-Business (B2B) and Business-to-Consumer (B2C) users to register themselves to Oracle Identity Cloud Service. You can also create multiple self-registration profiles to manage different sets of users and access to applications.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Service Access Request</td>
<td>Enable users to request access to groups and applications from the App Catalog.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Basic</td>
<td>Standard</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>SSO for Third-Party Cloud Services</td>
<td>Authenticate to Oracle Identity Cloud Service and gain single-click access to third-party SaaS services configured using the App Catalog. The App Catalog is a collection of pre-seeded applications for popular SaaS applications, such as Amazon Web Services, Google Suite, Office 365, and so on, that support federation standards such as SAML 2.0 and OAuth 2.0. It also allows you to configure Secure Form Fill for applications that don't support these standards. Using the App Catalog, you can define the application, configure SSO, and configure provisioning. Oracle creates and maintains the App Catalog for you.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO for Custom Applications</td>
<td>For custom applications developed using Oracle Cloud services and deployed on Oracle Cloud (PaaS and IaaS), authenticate to Oracle Identity Cloud Service and gain single-click access to these applications.</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Delegated Authentication with Password Writeback</td>
<td>Remove the need to synchronize user passwords between an on-premises Microsoft Active Directory enterprise directory structure and Oracle Identity Cloud Service. Users can use their Microsoft Active Directory passwords to sign in to Oracle Identity Cloud Service to access resources and applications protected by Oracle Identity Cloud Service.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-Factor Authentication (MFA)</td>
<td>Enable strong authentication by configuring Multi-Factor Authentication (MFA) during user authentication. Configure device compliance policies and a wide variety of second factors, such as SMS, OTP, push notifications, and knowledge-based questions and answers.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adaptive Security</td>
<td>Analyze contextual, risk, and threat information about the user, device, and network, and provide an intelligent, secure, and user-friendly way of providing access to corporate applications and resources. This also reduces the likelihood of online identity theft and fraud, which secures business applications even if the user’s device or the user's account password is compromised.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Authentication</td>
<td>Configure one or more social identity providers so that users can log in to Oracle Identity Cloud Service with their social credentials.</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Basic</td>
<td>Standard</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Advanced User Provisioning and Synchronization for Oracle Cloud Apps</td>
<td>Support interactive provisioning to allow administrators to grant entitlements and specify values for application account attributes. Administrators can also synchronize entitlements and other application data from the application into Oracle Identity Cloud Service. In addition to interactive provisioning and synchronization, you can customize the pre-configured provisioning templates in the App Catalog by changing the default attribute mappings for provisioning and synchronization and making configuration changes to them.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Provisioning and Synchronization for Third-Party Cloud Apps</td>
<td>Configure provisioning of user accounts to multiple third-party cloud apps, such as Google Suite, Office 365, and so on, from a list of pre-configured provisioning templates in the App Catalog. Enable account synchronization to detect and synchronize any changes made directly on these target applications.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EBS Asserter</td>
<td>Integrate your Oracle E-Business Suite environment with Oracle Identity Cloud Service for authentication and password management purposes by using a lightweight Java application known as the Oracle E-Business Suite (EBS) Asserter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Present disclaimers and acceptable use policies, also known as Terms of Use, to your users. Terms of Use helps you set the terms and conditions for your users to access your applications, based on user consent. This feature allows identity domain administrators to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service. You can configure Terms of Use on an application basis and collect consent from users before allowing them access to the application.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Foundation</td>
<td>Basic</td>
<td>Standard</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>App Gate</td>
<td>The Oracle Identity Cloud Service App Gate is a software appliance that you can use to provide Single Sign-On (SSO) and authorization for your on-premises applications. This enables you to use one appliance to provide SSO for multiple applications by allowing external users to access internal applications securely without the need for a VPN client. From the <strong>App Gateway for Identity Cloud Service</strong> application, you can access the documentation for the App Gate. You can find this application on the <strong>Downloads</strong> page of the Identity Cloud Service console. To access this page, in the Identity Cloud Service console, expand the <strong>Navigation Drawer</strong>, click <strong>Settings</strong>, and then click <strong>Downloads</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebGate</td>
<td>WebGate is a web-server plug-in that Oracle Access Management uses to protect on-premises web applications. It can be deployed on different web applications and web servers including, but not limited to, the Apache HTTP Server and Microsoft's Internet Information Services (IIS) web server. Instead of relying on Oracle Access Manager as an authentication service, WebGate can now interact with Oracle Identity Cloud Service to protect these applications by authenticating users to access the applications. When an unauthenticated user tries to access any applications that are protected by Oracle Identity Cloud Service, the user is redirected to the <strong>Sign In</strong> page of Oracle Identity Cloud Service for authentication.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schema Extension</td>
<td>If you're creating your own UI, and can't find a schema attribute that you need from the base Oracle Identity Cloud Service schema attributes, then you can add your own custom attributes using the Identity Cloud Service console.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### About Multiple Instances

Customers want to have separate environments for a single cloud service or application (for example, one environment for development and one for production).

Each environment may have different identity and security requirements so customers need to create separate environments to meet this criteria. You can create and manage multiple instances of Oracle Identity Cloud Service to protect your applications and Oracle Cloud services.

There are several benefits of using multiple instances of Oracle Identity Cloud Service. By having separate Oracle Identity Cloud Service environments, the users who work in one environment won't impact the work of users in another environment. Using multiple instances can help you maintain the isolation of administrative control over each environment. This is necessary if, for example, your security standards prevent development user IDs from existing in the production environment, or require that different administrators have control over different environments.

When multiple instances are utilized, you will have a primary instance, the instance which comes with your Oracle Cloud account, and one or more secondary (additional) instances. The cloud account administrator is the owner of the primary instance. This administrator can:

- Create secondary instances and be the identity domain administrator for them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Foundation</th>
<th>Basic</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic SCIM App Template</td>
<td>With this template, you can provision or synchronize users between your custom applications and Oracle Identity Cloud Service. You can use this template to configure your custom applications so that the SCIM APIs are exposed, and you don't have to develop a single line of code. All that's required is to go to the App Catalog and search for a SCIM-managed app template. To use this template, you only have to provide your endpoint URL and the details that Oracle Identity Cloud Service requires to connect to your application, and then map the attributes between your application and Oracle Identity Cloud Service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS Messaging</td>
<td>The total SMS message count is a pool based on the total number of users who have enabled MFA with SMS multiplied by the number of messages per user per month. Enterprise users are limited to 10 messages per user per month. Consumer users are limited to three messages per user per month. Any additional SMS messaging used beyond the limit is billed as additional Active users.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Create secondary instances and, as part of the instance creation process, assign users to be identity domain administrators of the instances.

• Delegate the creation of secondary instances to other administrators.

The identity domain administrator is assigned to the secondary instance during the creation of the instance. Although the identity domain administrator of a secondary instance may have the same user name as a user in the primary instance, they are different users who might have different privileges in each instance, and will have separate passwords. This administrator can switch between the primary and secondary instances to work in each instance. See Identify and Switch Instances for more information about how to switch instances.

The identity domain administrator of a secondary instance has superuser privileges of that instance and can use the Oracle Identity Cloud Service feature set of the instance. In the secondary instance, the identity domain administrator can:

• Manage users, groups, applications, system configuration, and security settings.

• Perform delegated administration by assigning users to different administrative roles.

• Enable and disable Multi-Factor Authentication (MFA), configure MFA settings, and configure authentication factors.

• Create self-registration profiles to manage different sets of users, approval policies, and applications.

Regarding secondary instances, there are no new administrator or user processes to learn. The process to perform any administrator or user task in a secondary instance is identical to the process for performing it in the primary instance.

**Important:** The identity domain administrator of a secondary instance can't create a secondary instance of Oracle Identity Cloud Service from their instance. There can't be a parent-child relationship between secondary instances. All secondary instances must be created from the cloud account, either by the cloud account administrator or by another administrator (provided the cloud account administrator gives them permissions to do so). In addition to the cloud account administrator creating the primary instance, this administrator or another administrator can create up to nine secondary instances.

The figure below shows an example of the relationship among various administrators of multiple instances.
In Example Corp, Mark Franklin is the cloud account administrator of the examplecorp cloud account, and is the owner of the primary Oracle Identity Cloud Service instance. He has superuser privileges for this cloud account. Mark wants to have separate Oracle Identity Cloud Service environments for development and production purposes. He creates a user account for Jerome Travers, Example Corp’s IT manager, and assigns the Identity Instance Creation cloud account role to him. This role gives Jerome the permissions to create and manage Oracle Identity Cloud Service secondary instances. By assigning the Identity Instance Creation role to Jerome, Mark delegates the creation of secondary instances to Jerome.

Jerome creates two secondary instances and assigns Angela Johnson, Example Corp’s development manager, to be the identity domain administrator of the development instance, and Lyle Robert, Example Corp’s production manager, to be the identity domain administrator of the production instance. Because they’re identity domain administrators, Angela and Lyle have superuser privileges for their respective secondary Oracle Identity Cloud Service instances. They can manage users, groups, applications, and configuration data in their instances. All work that happens in one instance is isolated from work performed in the other instance so there’s a complete separation of work in the development and production instances.
The diagram below shows the scenario in which Jerome Travers creates a secondary instance and assigns himself to be the identity domain administrator for that instance. Jerome now has access to two instances:

- The primary instance because Mark Franklin, the cloud account administrator, created an account for Jerome in that instance and assigned the **Identity Instance Creation** role to him.
- The secondary instance because Jerome is the identity domain administrator of that instance.

If Jerome signs in to Oracle Identity Cloud Service through the secondary instance, accesses the **My Services** dashboard, and clicks the **Identity Domain** menu in the upper-right corner, below the top menu bar, then two menu items appear: one for the primary instance and one for the secondary instance.

Jerome can use the **Identity Domain** menu to switch to the dashboard associated with the primary Identity Cloud Service instance. He can perform actions associated with any roles assigned to him for either the primary or secondary instance. Because
Mark assigned the **Identity Instance Creation** role to him for the primary instance, Jerome can create other secondary instances for the cloud account.

The following table lists the different steps that must be performed to set up secondary instances, the administrators involved for each instance, and what each administrator’s tasks are for a particular step.

Table 1-1  **Example of Administrative Responsibilities During a Typical Workflow of Setting Up Multiple Instances**

<table>
<thead>
<tr>
<th>Step Detail</th>
<th>Cloud Account Administrator</th>
<th>Administrator Assigned to the Identity Instance Creation Role</th>
<th>Secondary Instance 1 Administrator (for example, Development)</th>
<th>Secondary Instance 2 Administrator (for example, Production)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup the Oracle Cloud account.</td>
<td>• Receives the cloud account administrator and identity domain administrator roles for the primary instance.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
</tr>
<tr>
<td></td>
<td>• Signs in to Oracle Identity Cloud Service to reset their password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accesses the <strong>My Services</strong> dashboard from the Identity Cloud Service console.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create a user in the primary instance.</td>
<td>• Creates an account for the user who will create or manage secondary instances.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
</tr>
</tbody>
</table>
Table 1-1 (Cont.) Table 1-1 Example of Administrative Responsibilities During a Typical Workflow of Setting Up Multiple Instances

<table>
<thead>
<tr>
<th>Step Detail</th>
<th>Cloud Account Administrator</th>
<th>Administrator Assigned to the Identity Instance Creation Role</th>
<th>Secondary Instance 1 Administrator (for example, Development)</th>
<th>Secondary Instance 2 Administrator (for example, Production)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegate the ability to create or manage secondary instances.</td>
<td>• Assigns the <strong>Identity Instance Creation</strong> cloud account role to this user so that the user can create, modify, and remove secondary instances. See <a href="#">Before Creating a Secondary Instance</a> to learn more about how to assign this cloud account role.</td>
<td>• Receives a notification that contains information about how to sign in to the primary Oracle Identity Cloud Service instance of the Oracle Cloud account. • Uses the <a href="#">Access your Cloud Services</a> link in the notification to sign in with their user name and the temporary password that's generated by Oracle Identity Cloud Service. • Resets their password. • Clicks the <a href="#">Dashboard</a> link on the <a href="#">Guided Journey</a> page of the <a href="#">My Services</a> dashboard to create or manage a secondary instance.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
</tr>
<tr>
<td>Step Detail</td>
<td>Cloud Account Administrator</td>
<td>Administrator Assigned to the Identity Instance Creation Role</td>
<td>Secondary Instance 1 Administrator (for example, Development)</td>
<td>Secondary Instance 2 Administrator (for example, Production)</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Create a secondary instance (for example, Development).</td>
<td>No responsibilities for this administrator.</td>
<td>• Creates a secondary Development instance.</td>
<td>• Becomes an identity domain administrator of the secondary instance.</td>
<td>No responsibilities for this administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assigns the Secondary Instance 1 administrator to be the owner of this instance.</td>
<td>• Receives a notification email regarding this new administrator role as well as how to sign in to the secondary Oracle Identity Cloud Service instance of the Oracle Cloud account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Clicks the link to the right of the Admin Console URL field to access the Identity Cloud Service console for this instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Resets their password.</td>
<td></td>
</tr>
<tr>
<td>Step Detail</td>
<td>Cloud Account Administrator</td>
<td>Administrator Assigned to the Identity Instance Creation Role</td>
<td>Secondary Instance 1 Administrator (for example, Development)</td>
<td>Secondary Instance 2 Administrator (for example, Production)</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Create a secondary instance (for example, Production).</td>
<td>No responsibilities for this administrator.</td>
<td>• Creates a secondary Development instance.</td>
<td>No responsibilities for this administrator.</td>
<td>• Becomes an identity domain administrator of the secondary instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assigns the Secondary Instance 2 administrator to be the owner of this instance.</td>
<td></td>
<td>• Receives a notification email regarding this new administrator role as well as how to sign in to the secondary Oracle Identity Cloud Service instance of the Oracle Cloud account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Clicks the link to the right of the Admin Console URL field to access the Identity Cloud Service console for this instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Resets their password.</td>
</tr>
</tbody>
</table>
Table 1-1 (Cont.) Table 1-1 Example of Administrative Responsibilities During a Typical Workflow of Setting Up Multiple Instances

<table>
<thead>
<tr>
<th>Step Detail</th>
<th>Cloud Account Administrator</th>
<th>Administrator Assigned to the Identity Instance Creation Role</th>
<th>Secondary Instance 1 Administrator (for example, Development)</th>
<th>Secondary Instance 2 Administrator (for example, Production)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer the secondary instance.</td>
<td>No responsibilities for this administrator.</td>
<td>No responsibilities for this administrator.</td>
<td>• Uses the Identity Cloud Service console to create and manage more users, if needed, in this secondary instance, as well as to perform additional tasks as an identity domain administrator.</td>
<td>• Uses the Identity Cloud Service console to create and manage more users, if needed, in this secondary instance, as well as to perform additional tasks as an identity domain administrator.</td>
</tr>
</tbody>
</table>

Oracle Identity Cloud Service instances can also be created in data regions that are different from the data region that customers designate when they sign up for Oracle Cloud (the home data region). Before creating secondary instances in another data region, customers must extend their subscription to that region. They can then use the My Services Dashboard to create secondary instances for the region. See Extending Your Subscription to Another Data Region.

The figure below shows an example of the relationship among various administrators of multiple instances.
In Example Corp (examplecorp), Mark Franklin, the cloud account administrator, extends the company’s subscription to the Latin America (LAD) data region. Mark then creates a user account for Bruce Collins, Example Corp’s IT manager for LAD, and assigns the **Identity Instance Creation** role to him. This role gives Bruce permissions to create and manage Oracle Identity Cloud Service secondary instances.

Bruce creates the `latinamericaprod` secondary instance and assigns himself to be the identity domain administrator of that instance. He can use the Identity Cloud Service console to manage users, groups, applications, and configuration data in the instance.

To learn more about the Identity Cloud Service console, see Access Service Consoles.

### Before Creating a Secondary Instance

**Important:** If you're not a subscriber to the Universal Credits pricing model, then this Oracle Identity Cloud Service feature is available. However, if you're a subscriber to the Universal Credits pricing model, then this feature is temporarily unavailable. Please contact Oracle Support.

Before you create a secondary instance for Oracle Identity Cloud Service, ensure that:

- You've either set up an Oracle Cloud account or had an account created for you. See Create Users and Assign Roles in Getting Started with Oracle Cloud.
- You're either the cloud account administrator or you've been assigned to the **Identity Instance Creation** role so that you can create the secondary instance. See Learn About Cloud Account Roles in Getting Started with Oracle Cloud.
- You're in the primary instance of the data region for which you want to create a secondary instance. See Identify and Switch Instances.
- You're familiar with the pricing model for your instance. This pricing model represents the billing metric for the instance you're creating. See Understanding the User Per Month Pricing Model for more information about this pricing model.
Create a Secondary Instance

**Important:** If you’re not a subscriber to the Universal Credits pricing model, then this Oracle Identity Cloud Service feature is available. However, if you’re a subscriber to the Universal Credits pricing model, then this feature is temporarily unavailable. Please contact Oracle Support.

You create a secondary instance for Oracle Identity Cloud Service from the Oracle Cloud Infrastructure Classic Console.

To create this secondary instance, use the **Identity Domain** menu to select the primary instance of the data region for which you want to create the secondary instance. See **Identify and Switch Instances** for more information about using the **Identity Domain** menu.

Only cloud account administrators or administrators who have been assigned to the **Identity Instance Creation** cloud account role can create a secondary instance.

Each Oracle Identity Cloud Service instance has an instance name and a URL. The instance name is assigned to your instance for Oracle Identity Cloud Service when it's created. The name must be unique within the identity domain.

If you're a user who's assigned to be the administrator of the secondary instance, then use the URL in the notification email that's sent to you to access the instance. If you're a cloud account administrator, then you can access the URL from the Oracle Cloud Infrastructure Classic Console.

If you exceed the maximum number of instances that you can create, then you'll get an error when you click **Create Instance** from the console.

1. In the Oracle Cloud Infrastructure Classic Console, use the **Identity Domain** menu to select the primary instance of the data region for which you want to create a secondary instance, and then click **Create Instance**.
2. In the **Create Instance** dialog box, click the **All Services** tab.
3. In the **Identity Cloud** box, click **Create**. The **Create New Oracle Identity Cloud Service Instance** wizard opens. This wizard steps you through the process of creating an instance.
4. Complete the **Instance Details** page. Specify the following:
   a. **Name**: Specify a unique name for your instance. This name identifies your service within your identity domain. The instance name must start with a letter, and can have up to 25 lowercase letters and numbers. You can't use spaces and special characters. The name that you provide will appear on Oracle Identity Cloud Service's **Sign In** page for that instance.
   b. From the **Plan** list, select **Oracle Identity Cloud Service**.
   c. **License Type**: Specify the User per Month pricing model for your instance.
   d. In the **Initial Administrator Details** section, specify the administrator credentials for the instance that you’re creating. Enter the email address, user name, first name, and last name, as required, in the respective fields.

   To have the administrator access the Oracle Cloud Infrastructure Classic Console with their email address, select the **Use email as user name** check box, and then in the **Email** field, enter the email address for the administrator account.
To have the administrator access this console with their user name, don't select the **Use email address as user name** check box, and then, in the **User Name** field, enter the user name for the administrator.

If you're entering an existing administrator's login credentials, then ensure that the email address and user name are correct. Administrator details are populated automatically based on the logged-in user's details only if such information is available.

If you're assigning a user to be the administrator of this instance, and this user is already the administrator of either the primary instance or another secondary instance, then the user can switch between the instances to work in each instance. See **Identify and Switch Instances** for more information about how to switch instances.

5. Click **Create**.

6. In the **Confirmation** window, click **Create**.

The instance is created and the status of the instance is set to **Initialized**. Oracle Cloud sends a **Your new Oracle Identity Cloud Service instance in Oracle Cloud <cloudaccountname> is ready** email notification to the administrator of the instance when the instance is active and ready to use. `<cloudaccountname>` is a placeholder for the name of the Oracle Cloud account that was used to create the secondary instance. For example, if the user name of the cloud account is examplecorp, then the name of the notification will appear as **Your new Oracle Identity Cloud Service instance in Cloud Account examplecorp is ready**.

![Access Details for My Services](image)

The notification contains details about the user name and password for the administrator of the secondary instance as well as how this administrator can use this
information to access both the Oracle Cloud Infrastructure Classic Console (Access your Cloud Services) and the Identity Cloud Service console (Admin Console URL).

Use the Oracle Cloud Infrastructure Classic Console to access the Overview tab of the Service: Oracle Identity Cloud Service page to verify that the instance you created appears. See Modify a Secondary Instance to learn how to access this tab.

You can click the instance name (for an active instance) or you can click the Open Service Console link to access the Identity Cloud Service console. For more information on managing the service instance, see Verify That Your Services Are Ready and Manage Your Oracle Cloud Service in Getting Started with Oracle Cloud.

**Identify and Switch Instances**

**Important:** If you're not a subscriber to the Universal Credits pricing model, then this Oracle Identity Cloud Service feature is available. However, if you're a subscriber to the Universal Credits pricing model, then this feature is temporarily unavailable. Please contact Oracle Support.

After you create a secondary Oracle Identity Cloud Service instance, there are two instances: the primary instance and the secondary instance.

To ensure that you're accessing the secondary instance, and not the primary one, it's important that you learn how to distinguish when you're accessing the primary or secondary instance, and how to switch between them.

You can identify and switch instances from one of the following locations:

- **Sign In page:** If you're signing in to the secondary instance, then the name of the secondary instance appears in parenthesis after the name of the Oracle Cloud account. For example, if the name of the Oracle Cloud account is examplecorp and the name of the secondary instance is development, then examplecorp (development) appears on the Sign In page. If you're signing in to the primary instance of your home data region, then only the Oracle Cloud account name appears on the Sign In page (for this example, examplecorp). If you're signing in to the primary instance of another data region, then the name of the instance appears in parenthesis after the name of the Oracle Cloud account. For example, if the name of the primary instance is identityLAD, then examplecorp (identityLAD) appears on the Sign In page.

- **Oracle Cloud Infrastructure Classic Console:** If you have been assigned to the Identity Instance Creation cloud account role in the primary instance or you have been designated to be the identity domain administrator of the secondary instance, then you can access this console. To use the Oracle Cloud Infrastructure Classic Console to switch between instances, a user must sign in to the secondary instance.

If you have access to this console and you click the Identity Domain menu in the upper-right corner, below the top menu bar, then menu items appear. These menu items represent the primary and secondary instances that you have for all of your data regions. See Extending Your Subscription to Another Data Region.

The top-most menu item is the primary instance of your home data region (for example, examplecorp - North America). The primary instance of the home data region is represented by the name of the cloud account and the name of the data region. All other primary and secondary instances contain the name of the cloud account, the name of the data region, and the name of the instance.
In this example, Example Corp (examplecorp) has signed up for Oracle Cloud and designated North America as its home data region. Then the subscription has been extended to the Latin America (LAD) data region. Because North America is the home data region, the primary instance appears as examplecorp - North America. examplecorp - North America - development and examplecorp - North America - production are secondary instances of this data region.

For the LAD data region, examplecorp - LAD - identityLAD is the primary instance and examplecorp - LAD - latinamericaprod is the secondary instance.

One menu item that appears in the Identity Domain menu is labeled (traditional). For this example, this item is examplecorp - North America (traditional). This is associated with a traditional cloud account which doesn't apply if you're using multiple instances.

If you're a user who has been assigned to be the identity domain administrator of secondary instances, then you'll see the primary instance and those instances to which you've been assigned.

If you have signed in using a secondary instance then an Info box appears, alerting you that you're in a secondary instance.

Figure 1-1  Secondary Instance Info Notification

Although the Info box doesn't identify the name of the secondary instance, it's useful to confirm that you have signed in using a secondary instance of Identity Cloud Service.

- **Navigation Drawer**: In the Oracle Cloud Infrastructure Classic Console, expand the Navigation Drawer, and then expand Users. All of the data regions for which you have primary and secondary instances appear. See Extending Your Subscription to Another Data Region.
By default, the first data region that appears is your home data region. All other data regions for which you have primary and secondary instances appear below the home data region.

When you expand a data region, the first instance that appears is the primary instance. All secondary instances appear below the primary instance in the order that they were created.

For the home data region, the primary instance appears as identity (Primary). For all other data regions, the primary instance appears as identity\<\textless\text{data_region}\text{\rangle}. For example, if you have a primary instance for the LAD data region, then it would appear as identityLAD.

![Image](image.png)

For this example, Example Corp has subscribed to two data regions: one in North America and one in Latin America (LAD). Because the North America data region is the home data region, the primary instance appears as identity (Primary). development and production are secondary instances of the North America data region.

For the LAD data region, identityLAD is the primary instance and latinamerica\_prod is the secondary instance.

If you click the name of an instance, the User Management page appears for that instance. In the User Management page, click Identity Console in the upper-right corner and the Identity Cloud Service console opens.

- **Identity Cloud Service console:** The names of both the primary or secondary instance and the Oracle Cloud account that was used to create this instance appear in this console. To access this information, click the user icon in the upper-right corner of the console, and then select About from the drop-down menu. The Cloud Account Name and Instance Name fields display the names of the Oracle Cloud account and the instance.

**Important:** By default, there’s no single sign-on between Identity Cloud Service instances. If you switch between Identity Cloud Service instances, then you must sign in to each instance.
Modify a Secondary Instance

**Important:** If you're not a subscriber to the Universal Credits pricing model, then this Oracle Identity Cloud Service feature is available. However, if you're a subscriber to the Universal Credits pricing model, then this feature is temporarily unavailable. Please contact Oracle Support.

You may want to modify a secondary instance (for example, change the tier of its pricing model).

For the secondary instance, you may have selected the **Foundation** tier for the User per Month pricing model. However, you now want to use one of the **Standard** tiers so that you can integrate Oracle Identity Cloud Service with other Oracle Cloud services, including Oracle Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) services, and custom applications hosted on Oracle PaaS or Infrastructure-as-a-Service (IaaS), as well as leverage the identity management features and SSO for these services.

You can modify a secondary instance only if you created the instance or are the administrator of that instance.

1. In the Oracle Cloud Infrastructure Classic Console, locate the **Identity Cloud** tile.
2. Click the **Action** menu in the tile, and then select **View Details**. The **Overview** tab of the Service: Oracle Identity Cloud Service page appears. In this tab, the **Service Instances** pane lists all available instances.
3. To filter the list, select from the following type of instances:
   - **Active**: Lists all active and available instances.
   - **Inactive**: Lists all instances that don't have an **Active** status. For example, you might see instances with the following statuses: **Initialized, Initialization-in-progress, Canceled, Terminated**, or **Termination-in-progress**.
   - **All**: Lists all instances.
4. Locate the secondary instance that you want to modify.
5. Click the **Action** menu to the right of the **Open Service Console** link, and then select **Modify** from the **Action** list. You can modify the pricing model for the secondary instance.
6. In the **License Type** menu, select the pricing model that you want to change for your instance, and then click **Modify**.
7. In the **Confirmation** window, click **Modify**.

Oracle Cloud sends a **Your service instance has been updated** email notification to the administrator. In the notification, details appear about the modification to the secondary instance (for this example, the change to the pricing model).

Remove a Secondary Instance

**Important:** If you're not a subscriber to the Universal Credits pricing model, then this Oracle Identity Cloud Service feature is available. However, if you're a subscriber to
the Universal Credits pricing model, then this feature is temporarily unavailable. Please contact Oracle Support.

If you no longer need a secondary instance, then remove it.

You can remove a secondary instance only if you created the instance or are the administrator of that instance.

1. In the Oracle Cloud Infrastructure Classic Console, locate the Identity Cloud tile.

2. Click the Action menu in the tile, and then select View Details.

3. In the Service Instances pane of the Overview tab of the Service: Oracle Identity Cloud Service page, filter the list of instances. See Modify a Secondary Instance.

4. Locate the secondary instance that you want to remove.

5. Click the Action menu to the right of the Open Service Console link, and then select Delete from the Action list.

6. In the Delete Service Instance window, click Delete.

Oracle Cloud begins to remove the instance, and changes its the status to Termination in progress. After the instance is removed completely, Oracle Cloud updates the status of the service instance to Purged. Oracle Cloud sends a Your service instance has been terminated email notification to the administrator. In the notification, details appear about the instance, including the name of the instance that was removed and the Oracle Cloud account that was associated with it.

About Oracle Identity Cloud Service Concepts

Learn about the basic concepts behind the technologies used in Oracle Identity Cloud Service.

- Oracle Cloud Services
- Identity Domain
- SAML, OAuth, and OpenID Connect
- SCIM
- Other Key Concepts

Oracle Cloud Services

Learn about Software as a Service (SaaS), Data as a Service (DaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) services used in Oracle Cloud.

Oracle Cloud offers a host of cloud services.

Application services are classified into two categories:

- Software as a Service (SaaS): Provides a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.
- Data as a Service (DaaS): Provides data on demand to a user regardless of geographic or organizational separation of the provider and consumer.

Platform services are also classified into two categories:
• Platform as a Service (PaaS): Provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and deploying an application.

• Infrastructure as a Service (IaaS): Provides access to computing resources (that is, virtualized hardware and computing infrastructure) in Oracle Cloud across a public connection.

For a comprehensive list of the available Oracle Cloud SaaS, DaaS, PaaS, and IaaS services, go to https://www.oracle.com/cloud and from the Oracle Cloud menu, select that category of services that interests you. From the page that opens, you can find links to detailed information about each service.

Oracle Cloud securely integrates its different cloud services, customer applications, and cloud services from other vendors. For example; this integration let’s you,

• Embed Oracle Sales Cloud within your own application running on Oracle Java Cloud Service - SaaS Extension.

• Extend Oracle Fusion Customer Relationship Management Cloud Service with a custom application.

• Tie together an Oracle Cloud service with functionality from other sites, such as Salesforce.

• Use an Oracle Cloud service as the infrastructure for building your own applications.

Identity Domain

Learn about the basic concepts behind an Identity Domain in Oracle Identity Cloud Service.

An identity domain is a construct for managing users and roles, integration standards, external identities, secure application integration through Oracle Single Sign-On (SSO) configuration and OAuth administration. OAuth is an authorization protocol (a set of rules) that allows a third-party website or application to access a user's data without the user sharing login credentials. An identity domain controls the authentication and authorization of the users signing in to a cloud service in Oracle Cloud, and what cloud service features they can access.

An Oracle Cloud service account is a unique customer account that can have multiple cloud services of different service types. For example, you could have three different cloud services, such as Oracle Java Cloud Service, Oracle Database Cloud Service, and Oracle Cloud Infrastructure Compute Classic as part of a single Oracle Cloud service account.

Every Oracle Cloud service belongs to an identity domain. Multiple services can be associated with a single identity domain to share user definitions and authentication. Users in an identity domain can be granted different levels of access to each service associated with the domain to ensure a segregation of duties.
SAML, OAuth, and OpenID Connect

Learn about the basic concepts behind the SAML, OAuth, and OpenID Connect technologies used in Oracle Identity Cloud Service.

Security Assertion Markup Language (SAML) supports both authentication and authorization and is an open framework for sharing security information on the internet through XML documents. SAML includes three parts:

- **SAML Assertion**: How you define authentication and authorization information.
- **SAML Protocol**: How you ask (SAML Request) and get (SAML Response) the assertions you need.
- **SAML Bindings and Profiles**: How SAML assertions ride on (Bindings) and in (Profiles) industry-standard transport and messaging frameworks.

The OAuth 2.0 token service provided by the Oracle Cloud identity infrastructure provides secure access to the Representational State Transfer (REST) endpoints of cloud services by other cloud services and user applications.

OAuth 2.0 provides the following benefits:

- It increases security by eliminating the use of passwords in service-to-service REST interactions.
- It reduces the lifecycle costs by centralizing trust management between clients and servers. OAuth reduces the number of configuration steps to secure service-to-service communication.

Oracle Identity Cloud Service leverages the power of OpenID Connect and OAuth to deliver a highly-scalable, multi-tenant token service for securing programmatic access to custom applications by other custom applications, and for federated SSO and authorization integration with these applications:

- **Use OAuth 2.0** to define authorization in Oracle Identity Cloud Service for your custom applications. OAuth 2.0 has an authorization framework, commonly used for third-party authorization requests with consent. Custom applications can implement both two-legged and three-legged OAuth flows.

- **Use OpenID Connect** to externalize authentication to Oracle Identity Cloud Service for your custom applications. OpenID Connect has an authentication protocol that provides Federated SSO, leveraging the OAuth 2.0 authorization framework as a way to federate identities in the cloud. Custom applications participate in an OpenID Connect flow.

Using the OAuth 2.0 and OpenID Connect standards provides the following benefits:

- **Federated SSO** between the custom application and Oracle Identity Cloud Service. Resource owners (users accessing the custom application) need a single login to access Oracle Identity Cloud Service plus all applications integrated. Oracle Identity Cloud Service handles the authentication and credentials itself,
insulating custom applications. This capability is provided by OpenID Connect with OAuth 2.0.

- Authorization to perform operations on third-party servers with consent. Resource owners can decide at runtime whether the custom applications should have authorization to access data or perform tasks for them. This capability is provided by OAuth 2.0.

**SCIM**

Learn about the basic concepts behind the SCIM technology used in Oracle Identity Cloud Service.

With Oracle Identity Cloud Service REST APIs, you can use a System for Cross-Domain Identity Management (SCIM) to securely manage your Oracle Identity Cloud Service resources, including identities and configuration data. These APIs provide an alternative to using the web-based user interface when you want to use Oracle Identity Cloud Service for your own UI or for clients.

You can manage users, groups, and applications, perform identity functions and administrative tasks, and manage your identity domain settings.

Oracle Identity Cloud Service provides SCIM templates to help you integrate your applications for provisioning and synchronization. See Use the SCIM Interface to Integrate Oracle Identity Cloud Service with Custom Applications.

**Other Oracle Identity Cloud Service Key Concepts**

Learn about the basic concepts behind the technologies used in Oracle Identity Cloud Service.

- 2-Step Verification: An authentication method that requires users to use more than one way of verifying their identity, providing a second layer of security to their accounts.
- Access request: Allowing users to request group and application access from the Catalog, and view their access requests as well as the groups and applications to which they have access.
- Access token: A token that contains all the rights that a user has to access an application.
- Account recovery: This automated process is designed to help Oracle Identity Cloud Service users regain access to their accounts if they have trouble signing in, they're locked out, or they forget their passwords.
- Adaptive Security: This feature provides strong authentication capabilities for users, based on their behavior within Oracle Identity Cloud Service, and across multiple heterogeneous on-premises applications and cloud services. Adaptive Security is used to analyze a user’s risk profile within Oracle Identity Cloud Service, based on their historical behavior, such as too many unsuccessful login attempts and too many unsuccessful MFA attempts, and real-time device context, such as impossible travel between locations, and logins from unknown devices, unfamiliar locations, and suspicious IP addresses. With this enriched context and risk information, Adaptive Security risk profiles each user, and arrives at its own risk score and an overall consolidated risk level (High, Medium, Low) that can be used with Oracle Identity Cloud Service policies to enforce a remediation action, such as allowing or denying the user from accessing Oracle Identity Cloud Service.
and its protected applications and resources, requiring the user to provide a second factor to authenticate into Oracle Identity Cloud Service, and so on.

- Administrator role: A role that provides user accounts with administrative capabilities in Oracle Identity Cloud Service.

- Application: See Custom application and Oracle application.

- App Catalog application: An application that contains a preconfigured application template.

- Application role: An entitlement in an Oracle application.

- Application template: How a custom application is represented in Oracle Identity Cloud Service.

- Bridge: A link between a Microsoft Active Directory enterprise directory structure and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between Microsoft Active Directory and Oracle Identity Cloud Service.

- Bulk loading: Loading a large amount of user, group, or application data into Oracle Identity Cloud Service automatically.

- Bypass code: A second verification method for Oracle Identity Cloud Service users when they forget their phones, don’t have service, or can’t access their computers. Users can generate bypass codes after they enroll in 2-Step Verification, and then store the codes in a safe place.

- Confidential application: A custom application that’s accessed by multiple users, hosted in a secure and protected place (server), and uses OAuth 2.0.

- Cross-Origin Resource Sharing (CORS): Client applications that run on one identity domain can obtain data from another identity domain.

- Custom application: An application (such as a mobile application, a web page, a client application, or a server application) that you can integrate with Oracle Identity Cloud Service. By default, for security purposes, custom applications are trusted or confidential.

- Default settings: Oracle Identity Cloud Service settings that are applied to a customer's entire identity domain. These settings include the time zone, password recovery email, signing certificate settings, contact information, and language for the identity domain.

- Delegated administration: Providing user accounts with administrative capabilities in Oracle Identity Cloud Service.

- Delegated authentication: Enabling users to use their Microsoft Active Directory passwords to sign in to Oracle Identity Cloud Service to access resources and applications protected by Oracle Identity Cloud Service.

- Digital certificate: An electronic passport that allows a person, computer, or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may be referred to as a public key certificate.

- Federated SSO: Provides a higher level of security and control for an identity provider because a security token is used to authenticate the user against both the identity provider and Oracle Identity Cloud Service.
• **Group:** The link between user accounts and applications in Oracle Identity Cloud Service. Groups are designed to ease the administration of privileges that you grant to user accounts.

• **Identity provider:** This type of provider, also known as an Identity Assertion provider, provides identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service.

• **Identity provider policy:** Criteria that Oracle Identity Cloud Service uses to display specific identity providers for users to sign in to Oracle Identity Cloud Service when they are accessing particular apps.

• **Job:** A batch execution of importing or exporting users, groups, or application roles in Oracle Identity Cloud Service.

• **Mobile application:** A custom application that's hosted directly on the resource owner's browser, machine, or mobile device.

• **Multi-Factor Authentication (MFA):** A method of authentication that requires the use of more than one factor to verify a user's identity.

• **Network perimeter:** A defined list of IP addresses that Oracle Identity Cloud Service can evaluate to determine whether users who use these IP addresses can sign in to Oracle Identity Cloud Service.

• **Oracle Mobile Authenticator (OMA) app:** A mobile device app that users can use as a second verification method.

• **Oracle application:** A complete and modular enterprise application, engineered from the ground up to be cloud-ready and to coexist seamlessly in mixed environments.

• **Password policy:** A set of password-related criteria that you set in Oracle Identity Cloud Service for all users in an identity domain.

• **Password recovery email address:** A user's email address to which Oracle Identity Cloud Service password recovery notifications are sent. By default, a user's primary email address is also the user's password recovery email address. However, a user has the option of specifying a password recovery email address that is different than the primary email address.

• **Primary email address:** A user's email address to which all Oracle Identity Cloud Service notifications are sent.

• **Profile:** A collection of useful data about you in Oracle Identity Cloud Service. Your profile includes contact information, account information, and also settings that determine the time zone and language that displays for your account in the Identity Cloud Service console.

• **Provisioning:** Managing the lifecycle of user accounts in Software as a Service (SaaS) applications, such as creating and deleting accounts using Oracle Identity Cloud Service.

• **Provisioning Bridge:** A link between on-premises apps and Oracle Identity Cloud Service. The Provisioning Bridge can synchronize with these apps so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. As a result, the state of each record is synchronized between the apps and Oracle Identity Cloud Service.

• **Refresh token:** A secure mechanism to obtain a new access token when the current access token expires.
• Resource server application: A third-party custom application that provides services that a web application can consume on behalf of the user.

• SAML application: A custom application that's accessed by multiple users, hosted in a secure and protected place (server), and uses SAML 2.0.

• Security Questions: Questions presented to users as part of 2-Step Verification. See 2-Step Verification.

• Self-registration profile: A profile created by an administrator to manage different sets of users, approval policies, and applications in Oracle Identity Cloud Service.

• Service provider: A website such as Oracle Identity Cloud Service that hosts applications.

• Sign-on policy: Criteria that Oracle Identity Cloud Service uses to allow or deny access to apps that are assigned to users.

• Social Login: Accessing Oracle Identity Cloud Service using credentials from trusted public identity providers such as LinkedIn, Facebook, Twitter, Google, and Microsoft. Users can also log in to these providers to create an account in Oracle Identity Cloud Service if they don't have one.

• Synchronization: Controlling how operations such as creating and deleting accounts in SaaS applications are reflected in Oracle Identity Cloud Service.

• Tag: A key-value pair that is used to organize and identify an application.

• Trusted partner: Any application or organization, remote to Oracle Identity Cloud Service, that communicates with Oracle Identity Cloud Service.

• User account: How a user is represented in Oracle Identity Cloud Service. A user account enables the user to access the Oracle Cloud service to which they belong. In Oracle Identity Cloud Service, there is a one-to-one relationship between a user and a user account.

• User life cycle: The process flow of how a user account is created, managed, and deleted in Oracle Identity Cloud Service based on certain events or time factors.

About Oracle Identity Cloud Service Interfaces

The following summarizes the key interfaces to Oracle Identity Cloud Service:

• The service consoles: See Access Service Consoles.

• The client for the bridge: See Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service.

• Rest APIs: See REST API for Oracle Identity Cloud Service.

How to Begin with Oracle Identity Cloud Service Subscriptions

Here's how to get started with Oracle Identity Cloud Service subscriptions:

1. Purchase a nonmetered subscription. See Buying a Nonmetered Subscription to an Oracle Cloud Service in Getting Started with Oracle Cloud.

2. Set up your account or activate your order. See Setting Up an Oracle Cloud Services Account or Activating Your Order in Getting Started with Oracle Cloud.
3. Verify that Oracle Identity Cloud Service is ready to use. See Verifying That Metered Oracle Cloud Services Are Running or Verifying That a Service Is Running in Getting Started with Oracle Cloud.

4. Learn about user accounts, groups, applications, and application roles. See About Oracle Identity Cloud Service User Accounts and Groups and About Oracle Identity Cloud Service Applications and Application Roles.


6. Create accounts for your Oracle Identity Cloud Service users and groups. See Managing Oracle Identity Cloud Service Users and Managing Oracle Identity Cloud Service Groups.

7. Assign your users and groups to Oracle Identity Cloud Service applications and application roles. See Managing Oracle Identity Cloud Service Applications.

Supported Web Browsers

Oracle Identity Cloud Service supports the following web browsers:

<table>
<thead>
<tr>
<th>OS</th>
<th>Chrome</th>
<th>Firefox</th>
<th>Internet Explorer **</th>
<th>Microsoft Edge</th>
<th>Safari</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>N/A</td>
<td>Not Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>iOS</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>N/A</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Supported</td>
<td>Supported</td>
<td>N/A</td>
<td>N/A</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported (IE11 Only)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Note:**
Support for Microsoft Browsers will follow the same N-1 support policy that iOS provides. The most recent version plus one previous release. As of January 12th 2016, this means the most recent version of Microsoft Edge and IE11 only.

How to Access Oracle Identity Cloud Service

Access Oracle Identity Cloud Service through a service web console or the REST API.

Depending on how you signed up for Oracle Cloud, you'll be directed to either the Oracle Cloud Infrastructure Console or the Oracle Cloud Infrastructure Classic Console.

**Topics:**
- Access Oracle Identity Cloud Service from the Oracle Cloud Infrastructure Console
- Access Oracle Identity Cloud Service from the Oracle Cloud Infrastructure Classic Console
Access Oracle Identity Cloud Service from the Oracle Cloud Infrastructure Console

On most Oracle Cloud accounts, you access the Oracle Identity Cloud Service console from the Oracle Cloud Infrastructure Console.

1. Sign in to Oracle Cloud.
   If you received a welcome email, use it to identify the URL, your user name, and your temporary password. After signing in, you will be prompted to change your password.

2. From the Oracle Cloud Infrastructure Console, click the navigation menu in the top left corner, expand **Identity**, and then click **Federation**.

3. In the **Federation** page, click the **Oracle Identity Cloud Service Console** link.
   If multiple instances are listed, click the **Oracle Identity Cloud Service Console** link for the console instance you want to open.

Access Oracle Identity Cloud Service from the Oracle Cloud Infrastructure Classic Console

On some older Oracle Cloud accounts, you access the Oracle Identity Cloud Service console from the Oracle Cloud Infrastructure Classic Console.

1. Sign in to Oracle Cloud.
   If you received a welcome email, use it to identify the URL, your user name, and your temporary password. After signing in, you will be prompted to change your password.

2. From the Oracle Cloud Infrastructure Classic Console, click the navigation menu in the top left corner, and then click **Users**.
   Alternatively, mouse-over **Users** and then click the name of one of the Oracle Identity Cloud Service instances on the sub menu that opens.

3. In the **User Management** page, click **Identity Console** in the upper right corner.

Access Service Consoles

This overview describes the ways that administrators and users can use the service consoles in conjunction with Oracle Identity Cloud Service.

Use the following sections to learn about key elements for each service console.

Topics:
- Sign In Page
- My Profile Console
- Identity Cloud Service Console
- My Apps
Sign In Page

Learn how to sign in, set, and reset your password.

When your account has been added to Oracle Identity Cloud Service, you receive an activation email instructing you to activate your account. Click the activation link, and then set your password.

If you forget your own password and can't sign in to Oracle Identity Cloud Service, you can reset your password using your user name. See Recovering a Forgotten Password.

My Profile Console

Use this console to set up or modify your profile (for example, time zone and language preferences), manage your passwords, set your primary and recovery email addresses, and link your social login accounts if you are using social login.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Profile Details</td>
<td>Set up your profile information for the first time or modify your current profile information. See Set Up or Modify Your Profile.</td>
</tr>
<tr>
<td>Change My Password</td>
<td>Change your password to Oracle Identity Cloud Service. See Changing Your Password.</td>
</tr>
<tr>
<td>Email Options</td>
<td>Change your recovery and primary email addresses. See Set Your Email Options.</td>
</tr>
<tr>
<td>Security</td>
<td>Set a recovery email address, provide a mobile number, or select and answer security questions to help you regain access to your account if you have trouble signing in, you're locked out, or you forget your password. See Set Your Account Recovery Options.</td>
</tr>
<tr>
<td>My Access</td>
<td>View the groups and applications to which you have been granted access. See View Group and Application Access.</td>
</tr>
<tr>
<td>My Requests</td>
<td>View your requests for access to groups and applications. See View Group and Application Access Requests.</td>
</tr>
<tr>
<td>My Consents</td>
<td>View your terms of use and application consents. See Access Your Consents.</td>
</tr>
<tr>
<td>Link a Social Account</td>
<td>Link a social account to establish a connection between your social account and your Oracle Identity Cloud Service user account. See Link and Unlink Social Accounts.</td>
</tr>
</tbody>
</table>

Identity Cloud Service Console

Depending on your administrator type, use this console to manage users, groups, applications, administrative settings and security settings, customize the service, and run reports.
Oracle Identity Cloud Service provides you with a **Navigation Drawer** to maximize the real estate of the Identity Cloud Service console.

To display the **Navigation Drawer**, click the **Action menu** in the upper-left corner of the console. You'll see a listing of all folders and pages that compose the console.

Click a folder to see the pages associated with the folder. Then, click the menu item that represents the page that you want to display in the Identity Cloud Service console.

To hide the **Navigation Drawer**, click the **Action menu** again.

The following table describes the key elements shown in the Identity Cloud Service console.

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Use this introductory page for the Identity Cloud Service console to access the Oracle Identity Cloud Service documentation library, videos, tutorials, the dashboard, reports, and links that administrators use frequently.</td>
</tr>
<tr>
<td>Users</td>
<td>Create, manage, and remove user accounts. See <a href="#">Managing Oracle Identity Cloud Service Users.</a></td>
</tr>
<tr>
<td>Groups</td>
<td>Create, manage, and remove groups. See <a href="#">Managing Oracle Identity Cloud Service Groups.</a></td>
</tr>
<tr>
<td>Applications</td>
<td>Create, manage, and remove applications. See <a href="#">Managing Oracle Identity Cloud Service Applications.</a></td>
</tr>
<tr>
<td>Jobs</td>
<td>Review the overall status of all jobs, the details for a specific job, and download a job file. See <a href="#">Viewing Jobs and Job Details.</a></td>
</tr>
<tr>
<td>Reports</td>
<td>Run user, application, and diagnostic data reports. See <a href="#">Running Oracle Identity Cloud Service Reports.</a></td>
</tr>
<tr>
<td>Settings</td>
<td>Set up and manage default settings, trusted partner certificates, notifications, password policies, branding, bridges, diagnostics, session settings, and self-registration.</td>
</tr>
<tr>
<td>Default Settings</td>
<td>Specify whether users can set their own password recovery email address, the default tenant locale, and the default tenant contact information for an identity domain. See <a href="#">Change Default Settings.</a></td>
</tr>
<tr>
<td>User Settings</td>
<td>Specify whether the primary email address is required or optional to create a user account. See <a href="#">Manage User Settings in Oracle Identity Cloud Service.</a></td>
</tr>
<tr>
<td>Partner Settings</td>
<td>Add, manage, and use trusted partner certificates. See <a href="#">Manage Oracle Identity Cloud Service Trusted Partner Certificates.</a></td>
</tr>
<tr>
<td>Notifications</td>
<td>Customize and use notifications. See <a href="#">Customize Oracle Identity Cloud Service Notifications.</a></td>
</tr>
<tr>
<td>Password Policies</td>
<td>Set, test, modify, and evaluate password policies. See <a href="#">Managing Oracle Identity Cloud Service Password Policies.</a></td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Branding</strong></td>
<td>Customize the <a href="#">Sign In</a> page and brand the Identity Cloud Service console and notification templates by adding logos to them. See <a href="#">Customizing the Oracle Identity Cloud Service Interface</a>.</td>
</tr>
<tr>
<td><strong>Provisioning Bridges</strong></td>
<td>Create, manage, and remove Provisioning Bridges. See <a href="#">Manage Provisioning Bridges for Oracle Identity Cloud Service</a>.</td>
</tr>
<tr>
<td><strong>Directory Integrations</strong></td>
<td>Create, manage, and remove bridges. See <a href="#">Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service</a>.</td>
</tr>
<tr>
<td><strong>Diagnostics</strong></td>
<td>Set the diagnostic type to capture operational logs. See <a href="#">Run Oracle Identity Cloud Service Reports</a>.</td>
</tr>
<tr>
<td><strong>Session Settings</strong></td>
<td>Specify the session expiration and the logout URL for an identity domain. See <a href="#">Change Session Settings</a>.</td>
</tr>
<tr>
<td><strong>Self-Registration</strong></td>
<td>Create self-registration profiles to manage different sets of users, approval policies, and applications. See <a href="#">Manage Self-Registration Profiles in Oracle Identity Cloud Service</a>.</td>
</tr>
<tr>
<td><strong>Downloads</strong></td>
<td>Download software development kits (SDKs) to enable your mobile and Web applications to authenticate and integrate with Oracle Identity Cloud Service. Download applications, including the Oracle E-Business Suite (EBS) Asserter to integrate Oracle E-Business Suite with Oracle Identity Cloud Service, the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to integrate your Linux environment with Oracle Identity Cloud Service to perform user authentication with first-factor and second-factor authentication, the Secure Form Fill Client to configure Secure Form Fill for your applications, the Identity Cloud Service Device Fingerprint Utility to enable the <strong>Access for an unknown device</strong> event of Adaptive Security for a custom sign-in page, and the Provisioning Bridge client to install, start, and stop the bridge. The Provisioning Bridge provides a link between your on-premises apps and Oracle Identity Cloud Service. See <a href="#">Download Oracle Identity Cloud Service SDKs and Applications</a>.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Set up and manage delegated administration, identity providers, identity provider policies, sign-on policies, network perimeters, Multi-Factor Authentication (MFA), MFA settings, and authentication factors.</td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td>After you create or import user accounts, delegate administrative responsibilities for these accounts. See <a href="#">Add or Remove a User Account from an Administrator Role</a>.</td>
</tr>
<tr>
<td><strong>Adaptive Security</strong></td>
<td>Activate Adaptive Security, and add, manage, and use risk providers. See <a href="#">Manage Adaptive Security in Oracle Identity Cloud Service</a>.</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identity Providers</td>
<td>Add, manage, and use identity providers. See Manage Oracle Identity Cloud Service Identity Providers.</td>
</tr>
<tr>
<td>IDP Policies</td>
<td>Create, manage, and remove identity provider (IDP) policies. See Manage Oracle Identity Cloud Service Identity Provider Policies.</td>
</tr>
<tr>
<td>Network Perimeters</td>
<td>Define network perimeters. See Manage Oracle Identity Cloud Service Network Perimeters.</td>
</tr>
<tr>
<td>App Gateway</td>
<td>Use App Gateway to integrate web applications hosted either on a compute instance in a cloud infrastructure, or in an on-premises server with Oracle Identity Cloud Service for authentication purposes. See Manage Oracle Identity Cloud Service App Gateways.</td>
</tr>
<tr>
<td>Account Recovery</td>
<td>Configure factors that will help users regain access to their accounts if they have trouble signing in, they’re locked out, or they forget their passwords. See Manage Account Recovery in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>MFA</td>
<td>Enable and disable Multi-Factor Authentication (MFA), and configure MFA settings. See Manage Oracle Identity Cloud Service Multi-Factor Authentication Settings.</td>
</tr>
<tr>
<td>Factors</td>
<td>Configure authentication factors for MFA. See Manage Oracle Identity Cloud Service Multi-Factor Authentication Settings.</td>
</tr>
</tbody>
</table>

**My Apps**

On the **My Apps** page, you can access all apps assigned to you.

You can sort these apps by their names or by the dates when they were granted to you. For organizational purposes, you can designate preferred apps as favorites for future easy reference and access. See **Access My Apps** for more information about the **My Apps** page.

**Catalog**

Use this page to request access to groups of which you want to be a member and applications that you want to use.

See **Request Group and Application Access**.
2–Step Verification

Use this page to enroll in Multi–Factor Authentication (MFA) in Oracle Identity Cloud Service.

When you sign in to Oracle Identity Cloud Service, you’re prompted for your user name and password, which is the first factor. You’re then required to provide a second type of verification. This is called 2-Step Verification. The two factors work together to add an additional layer of security in Oracle Identity Cloud Service by using either additional information or a second device to verify your identity and complete the login process. See Manage 2–Step Verification from the My Profile Console for more information about the 2–Step Verification page.

About Oracle Identity Cloud Service User Accounts and Groups

This overview of user accounts and groups briefly explains what they are and how they are used.

A user account is an abstraction representing a way to be authenticated to access Oracle Identity Cloud Service. In Oracle Identity Cloud Service, the cardinality of relationship between user and account is one-to-one.

By default, all users can use their accounts to perform self-service capabilities in Oracle Identity Cloud Service. Users can update their profiles, reset their passwords, unlock their accounts, change their email preferences, and link social login accounts. As an Identity Domain Administrator, you may want to provide a user account with administrative capabilities in Oracle Identity Cloud Service. For example, in order to off-load some responsibilities, you may want to assign a user the User administrator role so that they can manage users, groups, and group memberships. To provide a user account with administrative capabilities, you assign administrator roles to user accounts. See Understanding Administrator Roles for more information about administrator roles and privileges that you can assign to user accounts.

As an administrator, you have easy and controlled privilege management through groups. Groups are the links between user accounts and applications in Oracle Identity Cloud Service. Groups are designed to facilitate the administration of privileges that you grant to user accounts. See Managing Oracle Identity Cloud Service Groups.

About Oracle Identity Cloud Service Applications and Application Roles

This overview briefly describes applications and application roles.

Oracle Identity Cloud Service provides you with a secure and centralized cloud service to manage the relationships that your users and groups have with your:

- **Cloud-based Oracle applications**: A complete and modular set of web-based enterprise applications, engineered to be cloud-ready and coexist seamlessly in mixed environments. You can use Oracle Cloud applications by accessing the UI
on your local web browser or through your mobile communications device connected to the Internet.

- **Custom applications**: Web applications that are written in a server-side language and can run on a server where the source code of the application isn't available to the public.

You can use Oracle Identity Cloud Service to grant users access to applications in two ways:

- Directly: Assigning users to applications.
- Indirectly: Assigning groups to applications. Users who are members of the groups are granted access to the applications.

In addition to granting users and groups access to Oracle applications, you can grant users and groups access to entitlements within applications. Each entitlement in an Oracle application is represented by an **Application Role**.

When a customer purchases or subscribes to any cloud services, the services are created in Oracle Identity Cloud Service as Applications. These services (Oracle Public Cloud Apps) have service consoles and the Application Roles control the authorization into these service consoles. Only PaaS services use Application Roles.

See [Managing Oracle Identity Cloud Service Applications](#).

**Typical Workflow for Using Oracle Identity Cloud Service**

Oracle Identity Cloud Service has five administrator roles and one user role. To start using Oracle Identity Cloud Service as an administrator or user, click the following links. Each link provides you with a guide of how to start using Oracle Identity Cloud Service as that administrator or user.

- **Identity Domain Administrator**
- **Security Administrator**
- **Application Administrator**
- **User Administrator**
- **User Manager**
- **Audit Administrator**
- **User**

**Note:**

See [Understanding Administrator Roles](#) to learn more about the privileges for each administrator or user role.

**Identity Domain Administrator**

An identity domain administrator has superuser privileges for an identity domain in Oracle Identity Cloud Service. All other Oracle Identity Cloud Service administrators have a subset of these privileges.
To start using Oracle Identity Cloud Service as an identity domain administrator, use the typical workflow below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the interface.</td>
<td>Customize the Sign In page or brand the Identity Cloud Service console and notification templates by adding logos to them.</td>
<td>Customizing the Oracle Identity Cloud Service Interface</td>
</tr>
<tr>
<td>Customize the default settings.</td>
<td>Customize the default settings for both the identity domain and the session between the Oracle Identity Cloud Service client and the server.</td>
<td>Configure User Settings</td>
</tr>
<tr>
<td>Manage user settings.</td>
<td>Specify whether the primary email address is required or optional to create a user account.</td>
<td>Change User Settings</td>
</tr>
<tr>
<td>Customize email notifications.</td>
<td>Customize email notifications for users and administrators.</td>
<td>Customize Oracle Identity Cloud Service Notifications</td>
</tr>
<tr>
<td>Customize the password policy.</td>
<td>Tailor the strength of the password policies.</td>
<td>Managing Oracle Identity Cloud Service Password Policies</td>
</tr>
</tbody>
</table>
| Configure Multi-Factor Authentication (MFA) | Enable MFA when you want to require your administrators and users to provide a second type of verification when they log in:  
  • Configure overall MFA policy settings such as which users are to use MFA and whether MFA is required.  
  • Configure the type of factors that you want to allow and specific policies for those factors. | Configure Authentication Factors                                |
| Configure account recovery.              | Configure factors that will help users regain access to their accounts if they have trouble signing in, they’re locked out, or they forget their passwords. | Manage Account Recovery in Oracle Identity Cloud Service |
| Onboard users and groups.                | Onboard users and groups by:  
  • Installing, configuring, and running bridges  
  • Importing users and groups  
  • Creating users and groups | Manage Provisioning Bridges for Oracle Identity Cloud Service  
Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service  
Managing Oracle Identity Cloud Service Users  
Managing Oracle Identity Cloud Service Groups |
<p>| Manage delegated authentication.          | Configure delegated authentication for bridges associated with Microsoft Active Directory domains. | Configure Delegated Authentication in Oracle Identity Cloud Service |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and manage custom applications.</td>
<td>Add and configure custom applications.</td>
<td>Managing Oracle Identity Cloud Service Applications</td>
</tr>
<tr>
<td>Assign users and groups to applications.</td>
<td>Assign users and groups to Oracle and custom applications.</td>
<td>Managing Oracle Identity Cloud Service Applications</td>
</tr>
<tr>
<td>Perform delegated administration.</td>
<td>After you create or import user accounts, you can delegate administrative responsibilities for these accounts.</td>
<td>Managing Oracle Identity Cloud Service Users</td>
</tr>
<tr>
<td>Add and manage identity providers.</td>
<td>Add and manage identity providers to provide identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Identity Providers</td>
</tr>
<tr>
<td>Manage identity provider policies.</td>
<td>Manage identity provider policies to restrict which identity providers appear on the Sign In page when users are accessing particular apps.</td>
<td>Manage Oracle Identity Cloud Service Identity Provider Policies</td>
</tr>
<tr>
<td>Define network perimeters.</td>
<td>Create network perimeters to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Network Perimeters</td>
</tr>
<tr>
<td>Manage sign-on policies.</td>
<td>Manage sign-on policies to define criteria that Oracle Identity Cloud Service uses to allow or deny access to users for apps that are assigned to them.</td>
<td>Manage Oracle Identity Cloud Service Sign-On Policies</td>
</tr>
<tr>
<td>Manage Adaptive Security and risk providers.</td>
<td>Activate Adaptive Security, and add, manage, and use risk providers to evaluate risk-based activity for Oracle Identity Cloud Service users, and generate a risk score for these users, based on this activity. This risk score is a number that varies from risk provider to risk provider, reflecting user threat.</td>
<td>Manage Adaptive Security in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Import trusted partner certificates.</td>
<td>Import certificates for trusted partners so that any application or organization, remote to Oracle Identity Cloud Service, can communicate with Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Trusted Partner Certificates</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Create Self-Registration Profiles</td>
<td>Add your customized header and footer logos, determine your allowed email domains, and add header, footer, success, and user consent text that will be used for self-registration.</td>
<td>Create Self-Registration Profiles</td>
</tr>
<tr>
<td>Run user and application reports</td>
<td>Run user and application reports to, for example, review user login attempts or user access to applications.</td>
<td>Running Oracle Identity Cloud Service Reports</td>
</tr>
<tr>
<td>Download SDKs and applications.</td>
<td>Download software development kits (SDKs) to enable your mobile and Web applications to authenticate and integrate with Oracle Identity Cloud Service. Download applications, including the Oracle E-Business Suite (EBS) Asserter to integrate Oracle E-Business Suite with Oracle Identity Cloud Service, the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to integrate your Linux environment with Oracle Identity Cloud Service to perform user authentication with first-factor and second-factor authentication, Identity Cloud Service App Gateway to integrate your application with Oracle Identity Cloud Service for authentication purposes, the Secure Form Fill Client to configure Secure Form Fill for your applications, the Identity Cloud Service Device Fingerprint Utility to enable the <strong>Access for an unknown device</strong> event of Adaptive Security for a custom sign-in page, and the Provisioning Bridge client to install, start, and stop the bridge. The Provisioning Bridge provides a link between your on-premises apps and Oracle Identity Cloud Service.</td>
<td>Download Oracle Identity Cloud Service SDKs and Applications</td>
</tr>
</tbody>
</table>

**Security Administrator**

A security administrator can manage Oracle Identity Cloud Service security settings for an identity domain in Oracle Identity Cloud Service.
Security administrators can customize the interface, default settings, notifications, and the password policy, configure Multi-Factor Authentication (MFA), and manage bridges, identity providers, and trusted partner certificates. See Understanding Administrator Roles.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the interface.</td>
<td>Customize the Sign In page or brand the Identity Cloud Service console and notification templates by adding logos to them.</td>
<td>Customizing the Oracle Identity Cloud Service Interface</td>
</tr>
<tr>
<td>Customize the default settings.</td>
<td>Customize the default settings for both the identity domain and the session between the Oracle Identity Cloud Service client and the server.</td>
<td>Change Oracle Identity Cloud Service Default Settings</td>
</tr>
<tr>
<td>Manage user settings.</td>
<td>Specify whether the primary email address is required or optional to create a user account.</td>
<td>Manage User Settings in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Customize email notifications.</td>
<td>Customize email notifications for users and administrators.</td>
<td>Customize Oracle Identity Cloud Service Notifications</td>
</tr>
<tr>
<td>Customize the password policy.</td>
<td>Tailor the strength of the password policies.</td>
<td>Managing Oracle Identity Cloud Service Password Policies</td>
</tr>
</tbody>
</table>
| Configure Multi-Factor Authentication (MFA) | Enable MFA when you want to require your administrators and users to provide a second type of verification when they log in:  
• Configure overall MFA policy settings such as which users are to use MFA and whether MFA is required.  
• Configure the type of factors that you want to allow and specific policies for those factors. | Configure Authentication Factors |
| Register App Gateway           | Register App Gateway to protect access to enterprise applications.          | Manage Oracle Identity Cloud Service App Gateways            |
| Configure account recovery.    | Configure factors that will help users regain access to their accounts if they have trouble signing in, they’re locked out, or they forget their passwords. | Manage Account Recovery in Oracle Identity Cloud Service     |
| Onboard users and groups.      | Onboard users and groups by installing, configuring, and running bridges.    | Manage Provisioning Bridges for Oracle Identity Cloud Service |

Chapter 1

Typical Workflow for Using Oracle Identity Cloud Service

1-50
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage delegated authentication.</td>
<td>Configure delegated authentication for bridges associated with Microsoft Active Directory domains.</td>
<td>Configure Delegated Authentication in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Add and manage identity providers.</td>
<td>Add and manage identity providers to provide identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Identity Providers</td>
</tr>
<tr>
<td>Manage identity provider policies.</td>
<td>Manage identity provider policies to restrict which identity providers appear on the <strong>Sign In</strong> page when users are accessing particular apps.</td>
<td>Manage Oracle Identity Cloud Service Identity Provider Policies</td>
</tr>
<tr>
<td>Define network perimeters.</td>
<td>Create network perimeters to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Network Perimeters</td>
</tr>
<tr>
<td>Manage sign-on policies.</td>
<td>Manage sign-on policies to define criteria that Oracle Identity Cloud Service uses to allow or deny access to users for apps that are assigned to them.</td>
<td>Manage Oracle Identity Cloud Service Sign-On Policies</td>
</tr>
<tr>
<td>Manage Adaptive Security and risk providers.</td>
<td>Activate Adaptive Security, and add, manage, and use risk providers to evaluate risk-based activity for Oracle Identity Cloud Service users, and generate a risk score for these users, based on this activity. This risk score is a number that varies from risk provider to risk provider, reflecting user threat.</td>
<td>Manage Adaptive Security in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Import trusted partner certificates.</td>
<td>Import certificates for trusted partners so that any application or organization, remote to Oracle Identity Cloud Service, can communicate with Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Trusted Partner Certificates</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Download SDKs and applications.</td>
<td>Download software development kits (SDKs) to enable your mobile and Web applications to authenticate and integrate with Oracle Identity Cloud Service. Download applications, including the Oracle E-Business Suite (EBS) Asserter to integrate Oracle E-Business Suite with Oracle Identity Cloud Service, the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to integrate your Linux environment with Oracle Identity Cloud Service to perform user authentication with first-factor and second-factor authentication, Identity Cloud Service App Gateway to integrate your application with Oracle Identity Cloud Service for authentication purposes, the Secure Form Fill Client to configure Secure Form Fill for your applications, the Identity Cloud Service Device Fingerprint Utility to enable the <strong>Access for an unknown device</strong> event of Adaptive Security for a custom sign-in page, and the Provisioning Bridge client to install, start, and stop the bridge. The Provisioning Bridge provides a link between your on-premises apps and Oracle Identity Cloud Service.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Manage identity provider policies.</td>
<td>Manage identity provider policies to restrict which identity providers appear on the Sign In page when users are accessing particular apps.</td>
<td>Manage Oracle Identity Cloud Service Identity Provider Policies</td>
</tr>
<tr>
<td>Define network perimeters.</td>
<td>Create network perimeters to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service.</td>
<td>Manage Oracle Identity Cloud Service Network Perimeters</td>
</tr>
<tr>
<td>Manage sign-on policies.</td>
<td>Manage sign-on policies to define criteria that Oracle Identity Cloud Service uses to allow or deny access to users for apps that are assigned to them.</td>
<td>Manage Oracle Identity Cloud Service Sign-On Policies</td>
</tr>
<tr>
<td>Run application reports.</td>
<td>Run operational or historical reports that capture data about Oracle Identity Cloud Service applications.</td>
<td>Running Oracle Identity Cloud Service Reports</td>
</tr>
</tbody>
</table>

### User Administrator

A user administrator can manage users, groups, and memberships for an identity domain in Oracle Identity Cloud Service.

A user administrator can onboard users and groups, assign users and groups to applications, and run user reports. See Understanding Administrator Roles.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboard users and groups.</td>
<td>Onboard users and groups by: • Configuring and running bridges • Importing users and groups • Creating users and groups</td>
<td>Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service Managing Oracle Identity Cloud Service Users Managing Oracle Identity Cloud Service Groups</td>
</tr>
<tr>
<td>Assign users and groups to applications.</td>
<td>Assign users and groups to Oracle and custom applications.</td>
<td>Managing Oracle Identity Cloud Service Applications</td>
</tr>
<tr>
<td>Run user reports.</td>
<td>Run operational or historical reports that capture data about Oracle Identity Cloud Service user accounts.</td>
<td>Running Oracle Identity Cloud Service Reports</td>
</tr>
</tbody>
</table>

### User Manager

A user manager can manage all users or users of selected groups in Oracle Identity Cloud Service.

User managers update, activate, deactivate, remove, and unlock user accounts. User managers can also reset passwords, reset authentication factors, and generate bypass codes for user accounts. See Understand Administrator Roles.
Audit Administrator

An audit administrator can run reports for an identity domain in Oracle Identity Cloud Service.

See Understanding Administrator Roles.

User

Users can update their profiles, reset their passwords, change their email preferences, view applications assigned to them, and link their social accounts to their Oracle Identity Cloud Service user accounts.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify your profile information.</td>
<td>Your profile is a collection of useful data about you. Your profile includes your contact information, account information, and settings that determine the time zone and language for your account in the Identity Cloud Service console.</td>
<td>Set Up or Modify Your Profile</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Change your password.</td>
<td>Edit your password, recover your forgotten password, or reset your expired password.</td>
<td>Change Your Password</td>
</tr>
<tr>
<td>Set your email options.</td>
<td>Modify both your primary email address and your password recovery email address.</td>
<td>Set Your Email Options</td>
</tr>
<tr>
<td>Set your account recovery options.</td>
<td>Set a recovery email address, provide a mobile number, or select and answer security questions to help you regain access to your account if you have trouble signing in, you’re locked out, or you forget your password.</td>
<td>Set Your Account Recovery Options</td>
</tr>
<tr>
<td>Link your social accounts.</td>
<td>Link your social accounts to Oracle Identity Cloud Service to access Oracle Identity Cloud Service using your social credentials.</td>
<td>Link and Unlink Social Accounts</td>
</tr>
<tr>
<td>Request access to groups and applications.</td>
<td>Request access to groups of which you want to be a member and applications that you want to use.</td>
<td>Request Group and Application Access</td>
</tr>
<tr>
<td>View your requests.</td>
<td>View your requests for access to groups and applications.</td>
<td>View Group and Application Access Requests</td>
</tr>
<tr>
<td>View your group and application access</td>
<td>View the groups and applications to which you have been granted access.</td>
<td>View Group and Application Access</td>
</tr>
<tr>
<td>View your applications.</td>
<td>View all applications that are assigned to you.</td>
<td>Access My Apps</td>
</tr>
</tbody>
</table>
| Set Up 2–Step Verification                | 2-Step Verification is an authentication method that requires you to use more than one way of verifying your identity. There are two ways to set up 2–Step Verification for your account:  
• During 2–Step Verification enrollment  
• Using the self-service console | Enroll in 2–Step Verification for Your Account  
Manage 2–Step Verification from the My Profile Console |
Understand Application Integration

In this chapter, you'll learn what application integration is, why you should integrate your applications with Oracle Identity Cloud Service, the types of application integrations, and how you can use the App Catalog, Microsoft Active Directory (AD) Bridge, Provisioning Bridge, and SCIM interface to integrate Oracle Identity Cloud Service with your Software-as-a-Service (SaaS), Microsoft Active Directory, enterprise LDAP, and custom applications.

Topics:

• What Is Application Integration?
• Why Should You Integrate Your Applications?
• What Are the Types of Application Integrations?

What Is Application Integration?

A typical large enterprise has thousands of applications, and these applications can be categorized into different buckets. There are Software-as-a-Service (SaaS) applications, homegrown applications, and on-premises applications. Customers are also building their applications in the cloud. The challenge with managing these different types of applications is that for each application, you must have administrators managing users, and administrators or developers protecting resources within the applications.

Application integration is providing one single place where customers can manage their users and the access they have to their company’s applications, as well as protect the resources associated with these applications. Oracle Identity Cloud Service provides a centralized location that customers can use to integrate all of their SaaS, homegrown, on-premises, and custom cloud applications.

Two key aspects of application integration are provisioning and synchronization. Provisioning allows you to use Oracle Identity Cloud Service to manage the lifecycle of user accounts in applications. This includes creating, modifying, disabling, enabling, and deleting user accounts and their profiles across applications.
For example, when you grant a user access to an application such as Google Suite, then an account is created for the user automatically in Google Suite. You can use Oracle Identity Cloud Service to add users to multiple applications and deprovision the users from these applications when conditions change for the users (for example, when they change roles or leave your organization).

Synchronization allows you to control how operations such as creating and deleting accounts in applications are reflected in Oracle Identity Cloud Service. This consists of bringing in user and group data from applications, and creating, modifying, or deleting the corresponding user accounts and groups in Oracle Identity Cloud Service.

Synchronization provides an inbound link between your applications and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with your applications so that any account data that's created, updated, or removed on the applications is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. So, if a user is deleted in one of your applications, then this change will be propagated into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between your applications and Oracle Identity Cloud Service.

**Why Should You Integrate Your Applications?**

Application integration reduces the time to develop new applications because you offload the business logic to secure applications to Oracle Identity Cloud Service. This logic includes securing your users, protecting the resources within the applications, and enabling users to access your applications through single sign-on (SSO).

Integrating your applications with Oracle Identity Cloud Service provides the user with a seamless experience. Because of SSO, the user doesn't have to remember different IDs and passwords for each application. When your applications are integrated with Oracle Identity Cloud Service, your administrative overhead is reduced greatly because you can manage the policies and users for your applications from one central place. From a compliance perspective, Oracle Identity Cloud Service provides you with a single location where you can manage the access that your users have to your applications.

As part of application integration, Oracle Identity Cloud Service is commonly used as either an identity provider or a service provider for applications. An identity provider, known as an Identity Assertion provider, provides identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service. A service provider is a website that hosts applications. You
can enable an identity provider and define one or more service providers. Your users can then access the applications hosted by the service providers directly from the identity provider.

For example, a website can allow users to log in to Oracle Identity Cloud Service with their Google credentials. Google acts as the identity provider and Oracle Identity Cloud Service functions as the service provider. Google verifies that the user is an authorized user and returns information to Oracle Identity Cloud Service (for example, the user name and the email address of the user, if the email address differs from the user name).

Some applications may require a user account to exist in their local identity store before the user can sign in to access these applications.

When users aren't created in Oracle Identity Cloud Service or imported into Oracle Identity Cloud Service from a flat file, they need to be synchronized from an authoritative source, such as an HR application or a corporate LDAP directory. For this scenario, the authoritative source and the application have to be integrated with Oracle Identity Cloud Service for provisioning and synchronization purposes.

What Are the Types of Application Integrations?

This section provides you with the following information to help you understand the types of application integrations:

**Topics:**

- **Which Integration Method to Use?**
- **Integrate Oracle Identity Cloud Service with Applications from the App Catalog**
- **Use Bridges to Integrate Oracle Identity Cloud Service with Microsoft Active Directory (AD) and an Enterprise LDAP**
- **Use the SCIM Interface to Integrate Oracle Identity Cloud Service with Custom Applications**

**Which Integration Method to Use?**

Use the following flowchart to learn which method to use to integrate your application with Oracle Identity Cloud Service.

The following scenarios will help you understand this flowchart for synchronization and provisioning purposes:
Scenarios for User Synchronization

One of the following scenarios may apply when synchronizing users and groups from authoritative sources:

An HR Application as an Authoritative Source

When a company hires an employee, an HR representative adds that employee’s information in the HR application directly. The HR application contains information about the user, such as the user’s first name, last name, job role, and job location. This information is used to create an account for the user and assign applications to the user. For this scenario, you want to synchronize your user account into Oracle Identity Cloud Service from the HR application.

Oracle Identity Cloud Service supports integration with the HR application via the App Catalog. If your application isn't listed in the App Catalog, then you can build your own connector or use the Generic SCIM App Template. This template facilitates the configuration of your custom application when the SCIM APIs are exposed. If your application doesn't expose the SCIM APIs, then you can develop a custom SCIM gateway to act as an interface between Oracle Identity Cloud Service and your application.

A Corporate LDAP as an Authoritative Source

Some customers store users and groups into an LDAP, such as Microsoft Active Directory (AD) or Oracle Internet Directory. These users and groups can authenticate into Oracle Identity Cloud Service via SSO. For this to occur, first, the users and groups must be synchronized from the LDAP into Oracle Identity Cloud Service. To do this, use the Microsoft Active Directory Bridge (for AD) or the Provisioning Bridge (for Oracle Internet Directory).

Scenario for User Provisioning

Oracle Identity Cloud Service enables you to use app templates to provision users to applications. In the App Catalog, you'll find a list of app templates that support provisioning. These templates enable you to integrate these applications with Oracle Identity Cloud Service quickly. If your application isn't listed in the App Catalog, then use the Generic SCIM App Template.

Now that you know how to use the flowchart to select a method to integrate your application with Oracle Identity Cloud Service for provisioning and synchronization purposes, let's learn about each integration type in greater detail.

Integrate Oracle Identity Cloud Service with Applications from the App Catalog

This section provides answers to the following questions to help you understand how to use the App Catalog to integrate Oracle Identity Cloud Service with Software-as-a-Service (SaaS) applications:

Topics:

- Why Integrate with SaaS Applications?
- What Is the App Catalog?
- What Are the Advantages of Using the App Catalog?
Why Integrate with SaaS Applications?

Over the past few years, customers are transitioning their access management system from an on-premises environment to a cloud-based one. This includes shifting their assets (such as their on-premises applications) into the cloud. Because of the proliferation of cloud-based SaaS applications in the market, Oracle Identity Cloud Service must be able to integrate with these applications. Oracle Identity Cloud Service has out-of-the-box integrations for thousands of SaaS applications. When a predefined integration isn't available for a SaaS application, Oracle Identity Cloud Service provides SAML and SCIM toolsets that will enable customers to integrate with it. By integrating your SaaS applications with Oracle Identity Cloud Service, you have one central place where you can not only manage your applications, but also the access that your users have to them.

What Is the App Catalog?

The App Catalog is a collection of partially configured application templates for thousands of SaaS applications, such as Amazon Web Services and Google Suite. Using the templates, you can define an application, configure SSO, and configure provisioning. Oracle creates and maintains the App Catalog for you, and provides step-by-step instructions that will help you to configure your applications.

What Are the Advantages of Using the App Catalog?

The App Catalog has out-of-the-box integrations for thousands of SaaS applications. When an application is available in the App Catalog, most of the metadata that Oracle Identity Cloud Service needs to integrate with the application already exists, so you don't have to define it. For most applications, it takes less than five minutes to configure them so that they can be integrated with Oracle Identity Cloud Service. All you have to do is go to the App Catalog, search for an application, create an instance of the application, and provide the connectivity details that Oracle Identity Cloud Service requires to communicate with it. When setting up applications, Oracle Identity Cloud Service features guided wizards that will help you configure them even further. This provides you with a consistent approach when using the App Catalog to integrate your applications with Oracle Identity Cloud Service.

Use Bridges to Integrate Oracle Identity Cloud Service with Microsoft Active Directory (AD) and an Enterprise LDAP

This section provides answers to the following questions to help you understand how to use bridges to integrate Oracle Identity Cloud Service with Microsoft Active Directory (AD) and an enterprise LDAP:

Topics:

- Why Integrate with Microsoft Active Directory (AD) and an Enterprise LDAP?
- What Are the Types of On-Premises Application Integrations?
Why Integrate with Microsoft Active Directory (AD) and an Enterprise LDAP?

Most customers have Microsoft Active Directory (AD) as their central directory service. These customers also use AD as their network directory. This directory is where all of their workstations are connected to and where they manage their users.

In addition to AD, customers use an enterprise LDAP to centralize all of their user identities. So, a customer uses AD to manage their employees, but in the centralized LDAP, the customer manages their partners, consumers, and any other users with which the customer has relationships.

For these reasons, it's imperative that Oracle Identity Cloud Service can integrate with both AD and an enterprise LDAP (for example, Oracle Internet Directory).

What Are the Types of On-Premises Application Integrations?

By using Oracle Identity Cloud Service, customers can control when they will migrate their directory-based applications to the cloud. In the interim, they can use one of the following:

- **AD Bridge:** This bridge provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Each minute, the bridge polls AD for any changes to these records and brings these changes into Oracle Identity Cloud Service. So, if a user is deleted in AD, then this change will be propagated into Oracle Identity Cloud Service. Because of this synchronization, the state of each record is synchronized between AD and Oracle Identity Cloud Service. After the user is synchronized from Microsoft Active Directory to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, then these changes are propagated to Microsoft Active Directory through the AD Bridge. See Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service.

- **Provisioning Bridge:** This bridge provides a link between your enterprise LDAP (such as Oracle Internet Directory) and Oracle Identity Cloud Service. Through synchronization, account data that is created and updated directly on the LDAP is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. As a result, any changes to these records will be transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between the LDAP and Oracle Identity Cloud Service. See Manage Provisioning Bridges for Oracle Identity Cloud Service.

Use the SCIM Interface to Integrate Oracle Identity Cloud Service with Custom Applications

This section provides answers to the following questions to help you understand how to use the SCIM interface to integrate Oracle Identity Cloud Service with custom applications:

**Topics:**

- **Why Integrate with Custom Applications?**
• What Is SCIM?
• Why Use SCIM?
• How Do You Use the Generic SCIM App Template?
• Does Your Custom Application Have a SCIM-based Interface?
• How Do You Develop a Custom SCIM Gateway?

Why Integrate with Custom Applications?

Let's say that you want to integrate your applications with Oracle Identity Cloud Service. Your applications are homegrown or aren't listed in the App Catalog, and an AD Bridge or Provisioning Bridge can't be used as a link between your applications and Oracle Identity Cloud Service.

A custom application is an application where the App Catalog or a bridge can't be used to integrate it with Oracle Identity Cloud Service. By integrating your custom applications with Oracle Identity Cloud Service, from one centralized cloud service, you can provide SSO capabilities for your applications, and provision and synchronize your users between the applications and Oracle Identity Cloud Service.

The App Catalog has thousands of applications that integrate with Oracle Identity Cloud Service. For most applications, Oracle Identity Cloud Service provides single sign-on (SSO) and user provisioning capabilities. User provisioning is not only giving users initial access to these applications, but also managing the complete lifecycle of the relationship that the users have with the applications.

What Is SCIM?

In the past, it was common that applications used to have their own user management APIs. Because the APIs for each application behave in a certain way, the developer had to understand the APIs specific to each application to build integrations for the applications.

To integrate your custom applications with Oracle Identity Cloud Service, Oracle recommends that you use the System for Cross-domain Identity Management (SCIM). SCIM provides developers with an abstraction layer. If APIs for the applications are exposed through SCIM, then developers don't have to learn the APIs associated with each application because the JSON format of the APIs is common across all applications.

In addition to SCIM being an open specification that standardizes user and group management across applications, it allows for the automation of user and group provisioning. You can provision and synchronize data for your users and groups across multiple applications.

With SCIM, you can define HTTP endpoints to create, read, update, and delete resources for entities such as users and groups. You can also use SCIM to extend the schemas for your company's users and groups. The SCIM specification defines a minimum set of attributes for the user schema, but this schema can be extended.

For example, suppose you need to provision the Employee ID custom attribute from the Oracle Identity Cloud Service user schema to your custom application. You can extend the default user schema, add this attribute, and map it between Oracle Identity Cloud Service and your application. The user schema in Oracle Identity Cloud Service
can now adhere to the attributes associated with your custom application's identity store.

The SCIM specification also defines security for any request that you make using HTTP endpoints. Security is defined by using a secure (HTTPS) protocol to establish communication between the endpoints and the applications with which you’re integrating, and requiring an authorization token that's used to access the request and perform the operations associated with it.

Use the following table to learn more about the SCIM specification:

<table>
<thead>
<tr>
<th>Item</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core schema</td>
<td><a href="https://tools.ietf.org/html/rfc7643">https://tools.ietf.org/html/rfc7643</a></td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
</tbody>
</table>

Why Use SCIM?

If you look at how integrations used to be built, developers had to understand the APIs exposed for each application. There was no consistency regarding how to represent an identity in these applications.

By using SCIM, there’s now a common standard of how you represent an identity in every application. Because all applications comply with the SCIM format, there’s a harmonious flow in terms of how these identities are represented. This makes it easier for an identity management cloud service such as Oracle Identity Cloud Service to integrate with these applications.

Having a common standard for representing identities in applications improves developers' work efficiency and productivity because developers don't have to spend time to learn the APIs for each application. From a corporate standpoint, the time it takes to develop an integration from an identity system to the application will be reduced significantly. You can now run automations for the integration because there’s a standard in terms of how you represent an identity and how you integrate with that identity.

By exposing your custom application's identity store with a SCIM-based interface, you avoid having to develop a custom connector between your application and Oracle Identity Cloud Service. This can be time-consuming, costly, and can lead to heavy maintenance in a future upgrade.

SCIM automates the user identity lifecycle management process and increases the security of data associated with your company's users and groups.

As your company grows, your users and groups increase. Through the day-to-day operations of your company, you may experience situations such as employee turnover or the memberships that your users have with your company's groups may change. Your company's user accounts, groups, and group memberships increase significantly.

Because SCIM is a standard, your company’s user and group data is stored in a consistent way and can be communicated as such across different apps (including your custom apps). You can automate the provisioning and deprovisioning process and have Oracle Identity Cloud Service function as a single point to manage
permissions and group memberships. By transferring your company's user and group data automatically, you mitigate the risk of inadvertent errors.

By implementing SCIM, you improve your company's security. Through SSO, your company's employees no longer have to sign on to each of their accounts individually. You can ensure security policy compliance for your users and their access to your company's applications.

When your employees are terminated or leave your company, you want your company's offboarding process to be consistent. This way, there's no chance that your company's administrators will forget to deprovision user accounts for applications that contain sensitive data. With SCIM, when users depart from your company, your administrators can terminate the accounts in Oracle Identity Cloud Service, and have peace of mind because these accounts will also be suspended or deleted in your SCIM-enabled apps.

How Do You Use the Generic SCIM App Template?

In the App Catalog, there are thousands of applications that integrate with Oracle Identity Cloud Service. You may have your applications running on your premises or in the cloud, or you may be building your applications in different infrastructure systems such as Amazon Web Services or Oracle Cloud Infrastructure.

Oracle Identity Cloud Service has to provide not only integrations with the applications that are listed in the App Catalog, but also tools so that you can build integrations for your custom applications without developing code.

With the Generic SCIM App Template, you can configure your custom applications so that the SCIM APIs are exposed, and you don't have to develop a single line of code. All that's required is to go to the App Catalog and search for a SCIM-managed app template. To use this template, you only have to provide your endpoint URL and the details that Oracle Identity Cloud Service requires to connect to your application, and then map the attributes between your application and Oracle Identity Cloud Service.

With the Generic SCIM App Template, you can provision or synchronize users between your custom applications and Oracle Identity Cloud Service.

In this diagram, the Generic SCIM App Template has been configured to enable Oracle Identity Cloud Service to communicate with a custom application that has a SCIM-based interface. This interface uses REST API endpoints to provision and synchronize users between Oracle Identity Cloud Service and the custom application.

Before You Begin

Before you begin to use the Generic SCIM App Template:
- Get access to an instance of Oracle Identity Cloud Service.
- Make sure that you have the appropriate permissions to register applications and to manage security components in the Identity Cloud Service console.
- Ensure that there’s HTTP(S) communication between Oracle Identity Cloud Service and the SCIM-based interface for your custom application.
- Make sure that you have a basic knowledge of the SCIM specification.

Assign Administrator Roles to Your User Account

Although you have access to an instance of Oracle Identity Cloud Service, you must be assigned to the following administrator roles in Oracle Identity Cloud Service to use the Generic SCIM App Template in the Identity Cloud Service console:

- Security administrator: To configure the security aspects of your Oracle Identity Cloud Service instance.
- Application administrator: To add a custom application and use the Generic SCIM App Template.

To assign these administrator roles to your user account:

1. Sign in to Oracle Identity Cloud Service with the credentials of your user account.
2. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Administrators.
3. Expand the node for the Security Administrator role.
4. Click Add, select the check box for your user account, and then click OK.
5. Repeat steps 3 and 4 to assign the application administrator role to your user account.

Does Your Custom Application Have a SCIM-based Interface?

In this section, you learn what to do, based on whether your custom application has a SCIM-based interface.

If your custom application has this interface, then you can configure the Generic SCIM App Template to provision Oracle Identity Cloud Service users with your application. See Configure the Generic SCIM App Template.

If your custom application doesn’t have this interface, then you can develop a custom SCIM gateway to act as the interface between Oracle Identity Cloud Service and your custom application. See How Do You Develop a Custom SCIM Gateway?

Configure the Generic SCIM App Template

In this section, you add an application using the Generic SCIM App Template, enable and configure connectivity for provisioning for your application, configure the application’s attribute mappings for provisioning, select the provisioning operations for your application, enable and configure synchronization for your application, and test your application to verify that users are provisioned to it.

Add an Application Using the Generic SCIM App Template

In this section, you use the Generic SCIM App Template to add an application.
1. In the Identity Cloud Service console, expand the Navigation Drawer, click Applications, click Add, and then select App Catalog.

2. In the Type of Integration section, click Provisioning, chose one of the following templates, and then click Add:
   - **GenericScim - Basic**: A Generic SCIM Template for SCIM interfaces that support basic authentication.
   - **GenericScim - Bearer Token**: A Generic SCIM Template for SCIM interfaces that support JWT tokens submitted as an authorization bearer.
   - **GenericScim - Client Credentials**: A Generic SCIM Template for SCIM interfaces that support client credentials for authentication.
   - **GenericScim - Resource Owner Password**: A Generic SCIM Template for SCIM interfaces that support the resource owner grant type.

3. In the Details pane of the corresponding template page, provide a name and description for your application, and then click Next.

4. In the Provisioning pane, click Finish. An instance of your application is created with five tabs: Details, Provisioning, Import, Users, and Groups.

   In the next section, you'll use the Provisioning tab to enable and configure connectivity for provisioning for your application.

Enable and Configure Connectivity for Provisioning for Your Application

In this section, you enable provisioning for your application and provide connectivity information for it. Oracle Identity Cloud Service uses this information to connect to your application's SCIM REST API endpoint for provisioning purposes.

1. Click the Provisioning tab.
2. Turn on the Enable Provisioning switch.
3. In the Confirmation window, click OK.
4. Use the following table to populate the fields of the Configure Connectivity section of the Provisioning tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Value Information</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The host name of your application's SCIM REST API endpoints. If the SCIM interface's URL is <a href="https://api.example.com/scimgate/Users">https://api.example.com/scimgate/Users</a>, then the host name is api.example.com.</td>
<td>This parameter appears in the UI for all Generic SCIM App Templates.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Value Information</td>
<td>Additional Information</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Base URI</strong></td>
<td>The base relative URL of your application's SCIM REST API. For example, if the SCIM interface's URL is <a href="https://api.example.com/scimgate/Users">https://api.example.com/scimgate/Users</a>, then the Base URI is /scimgate.</td>
<td>This parameter appears in the UI for all Generic SCIM App Templates.</td>
</tr>
<tr>
<td><strong>Administrator Username</strong></td>
<td>The administrator’s user name for your API authentication service. This value is sent as part of the body message of each request to your application's SCIM REST API. Format: Plain text.</td>
<td>This parameter appears in the UI for the <strong>GenericScim - Basic</strong> and <strong>GenericScim - Resource Owner Password</strong> templates.</td>
</tr>
<tr>
<td><strong>Administrator Password</strong></td>
<td>The administrator’s password for your API authentication service. This value is sent as part of the body message of each request to your application's SCIM REST API. Format: Plain text.</td>
<td>This parameter appears in the UI for the <strong>GenericScim - Basic</strong> and <strong>GenericScim - Resource Owner Password</strong> templates.</td>
</tr>
</tbody>
</table>
| **HTTP Operation Types** | By default, the template request uses the PATCH HTTP operation for any user's update operation. If your SCIM interface uses the PUT HTTP operation for user attribute updates, then use this field as per the example below.  
Example: __ACCOUNT__.Update=PUT | This parameter appears in the UI for all Generic SCIM App Templates. |
<p>| <strong>Access Token</strong>   | The value of the access token to be used by the template when communicating with your application's SCIM REST API. Format: Plain text. | This parameter appears in the UI for the <strong>GenericScim - Bearer Token</strong> template.       |
| <strong>Client Id</strong>      | The client ID for your API authentication service. Format: Plain text.                             | This parameter appears in the UI for the <strong>GenericScim - Client Credentials</strong> and <strong>GenericScim - Resource Owner Password</strong> templates. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Value Information</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Secret</td>
<td>The client secret for your API authentication service. Format: Plain text.</td>
<td>This parameter appears in the UI for the <code>GenericScim - Client Credentials</code> and <code>GenericScim - Resource Owner Password</code> templates.</td>
</tr>
<tr>
<td>Scope</td>
<td>The scope for your application. Example: <a href="https://www.example.com/auth/adm.direct.group">https://www.example.com/auth/adm.direct.group</a></td>
<td>This parameter appears in the UI for the <code>GenericScim - Client Credentials</code> and <code>GenericScim - Resource Owner Password</code> templates.</td>
</tr>
<tr>
<td>Authentication Server Url</td>
<td>The URL of your authentication service. Example: <a href="https://api.example.com/oauth2/v1/token">https://api.example.com/oauth2/v1/token</a></td>
<td>This parameter appears in the UI for the <code>GenericScim - Client Credentials</code> and <code>GenericScim - Resource Owner Password</code> templates.</td>
</tr>
<tr>
<td>Custom Authentication Headers</td>
<td>Used to send additional static header values to your API authentication service. Example: Basic authorization base64encodedusername:password</td>
<td>This parameter appears in the UI for the <code>GenericScim - Client Credentials</code> and <code>GenericScim - Resource Owner Password</code> templates.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>How long (in milliseconds) Oracle Identity Cloud Service will wait to establish communication with your application's SCIM REST API. Format: Plain text.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Socket Timeout</td>
<td>How long (in milliseconds) Oracle Identity Cloud Service will wait to receive data from your application's SCIM REST API. Format: Plain text.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number of your application's SCIM REST API endpoints. The default port number for this parameter is 443. For example, if the URL is <a href="https://api.example.com:6355/scimgate/Users">https://api.example.com:6355/scimgate/Users</a>, then set the port number value to 6355.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Value Information</td>
<td>Additional Information</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>If your application's SCIM REST API endpoints don’t require SSL, then set the value of this parameter to false.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service’s REST APIs.</td>
</tr>
<tr>
<td>JSON Resource Tag</td>
<td>The name of the attribute used in JSON messages when your application's SCIM REST API returns multiple resources. The default value is Resources. For example, if the response message of the user for the GET operation is:</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service’s REST APIs.</td>
</tr>
<tr>
<td>UID Attributes</td>
<td>The mapping between the <strong>UID</strong> (guid) internal attribute and your application's SCIM attribute for user and group object classes.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service’s REST APIs.</td>
</tr>
<tr>
<td>Name Attributes</td>
<td>The mapping between the <strong>NAME</strong> internal attribute and your application's SCIM attribute for user and group object classes.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service’s REST APIs.</td>
</tr>
<tr>
<td>Status Attributes</td>
<td>The mapping between the <strong>ENABLE</strong> (status) internal attribute and your application's SCIM attribute for the user object class.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service’s REST APIs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Value Information</td>
<td>Additional Information</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Attributes</td>
<td>Your application's SCIM REST API attribute that corresponds to the user's password. This is used for masking the password attribute in the log files. Default value: Users=password</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Date Attributes</td>
<td>The list of date attributes available for your application's SCIM REST API. Example: Users=meta.lastModifiedDate,joiningDate</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Date Format</td>
<td>The date-and-time format of the date attributes available for your application's SCIM REST API. Example: MMM d, yyyy h:mm:ss a z</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Content Type</td>
<td>The content-type header that your application's SCIM REST API expects Oracle Identity Cloud Service to send as a header HTTP request. Default value: application/scim+json</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Accept Type</td>
<td>The content-type header that is expected as an HTTP response from your application's SCIM REST API. Default value: application/scim+json</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Custom Headers</td>
<td>Used to send additional static header values to the SCIM REST API endpoints of your application. Format: &lt;headerName1&gt;=&lt;value&gt;, &lt;headerName2&gt;=&lt;value&gt;</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>SCIM Version</td>
<td>The version of your application's SCIM REST API. Default value: 13. The range for this attribute varies from 1 to 19.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Value Information</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OClass Mapping</td>
<td>Used to map an attribute of one object class to an attribute of another object class. For example, if the groups attribute of the <strong>ACCOUNT</strong> object class must be mapped to the <strong>GROUP</strong> object class, then enter <strong>ACCOUNT</strong>.groups=<strong>GROUP</strong>.</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Default Batch Size</td>
<td>The default page or batch size for the GET operation. Default value: 200</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
<tr>
<td>Managed Object Classes</td>
<td>The classification type of the schemas that your application must manage. Default value: [&quot;Users&quot;, &quot;Groups&quot;]</td>
<td>You can't update the value for this parameter in the UI. To update this parameter value, use Oracle Identity Cloud Service's REST APIs.</td>
</tr>
</tbody>
</table>

5. After populating the fields accordingly, click **Test Connectivity** to verify whether Oracle Identity Cloud Service can communicate with your application's SCIM REST API endpoints.

   If a successful connection can be established, then a **Connection successful**. message appears.

   If you receive an error message, check the values that you provided, and then click **Test Connectivity** again. If the problem persists, then contact your system administrator.

   Before testing, you can save the application and use Oracle Identity Cloud Service REST APIs to update the parameter values that don't appear in the UI. After updating the parameter values, open the application again using the Identity Cloud Service console, and then click **Test Connectivity**.

Configure Attribute Mappings for Provisioning

You can change the default attributes mapped between Oracle Identity Cloud Service and your application's SCIM REST API.

1. In the **Provisioning** tab of your application page, scroll to the **Configure Attribute Mapping** section, and then click **Attribute Mapping**. The Attribute Mapping window appears, and shows the default attribute mappings.

2. In the **Attribute Mapping** window, add, modify, or remove attribute mappings, according to your application's SCIM user schema.

3. Click **OK**.

Select Provisioning Operations

You can select which provisioning operations are supported by your application's SCIM REST APIs.
1. In the Provisioning tab of your application page, scroll to the Select Provisioning Operations section.

2. Select the following operations:
   - Authoritative Sync: If you enable this operation, then your application will become an authoritative source for Oracle Identity Cloud Service. Users in the application will be synchronized into Oracle Identity Cloud Service. If you select this operation, then the other provisioning operations will be deactivated.
   - Create Account: If a user is assigned to your application in Oracle Identity Cloud Service, then an account will be created for the user in the application.
   - Update Account: If an administrator edits the values of the provisioning form for a user who is assigned to your application, then these changes will be propagated to the application.
   - De-activate Account: If an administrator activates or deactivates a user who is assigned to your application, then this change will be propagated to the application.
   - Delete Account: If a user is removed from your application in Oracle Identity Cloud Service, then the user's account will be removed from the application.

Enable and Configure Synchronization for Your Application

By enabling and configuring synchronization for your application, Oracle Identity Cloud Service can synchronize user accounts from your application and match these accounts to corresponding Oracle Identity Cloud Service users.

1. Turn on the Enable Synchronization switch.

2. If you want Oracle Identity Cloud Service to communicate with your application’s SCIM REST API to synchronize groups from the application into Oracle Identity Cloud Service as application roles, then click Refresh Application Data. Otherwise, go to the next step.

3. Use the following table to populate the fields of the Configure Synchronization section of the Provisioning tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Value Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Identifier</td>
<td>The Oracle Identity Cloud Service user attribute that matches user accounts synchronized from the application with users in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>Application Identifier</td>
<td>The user attribute of your application's SCIM REST API that matches user accounts synchronized from the application with users in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Value Information</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>When exact match is found</td>
<td>Use the values in this menu to control whether Oracle Identity Cloud Service or an application administrator confirms any user accounts that are synchronized from the application into Oracle Identity Cloud Service. Values are:  • <strong>Link and confirm</strong>: Link the synchronized user accounts to corresponding Oracle Identity Cloud Service users automatically.  • <strong>Link but do no confirm</strong>: Link the synchronized user accounts to corresponding Oracle Identity Cloud Service users, but application administrators need to confirm the linking operation in the Import tab manually.</td>
</tr>
<tr>
<td>Max. number of creates</td>
<td>The value that you enter in this field represents the maximum number of user accounts that are created in Oracle Identity Cloud Service from the application. If you don't want to limit how many user accounts are created, then leave this field blank.</td>
</tr>
<tr>
<td>Max. number of deletes</td>
<td>The value that you enter in this field represents the maximum number of user accounts that are deleted in Oracle Identity Cloud Service after these accounts are deleted from the application. If you don't want to limit how many user accounts are deleted, then leave this field blank.</td>
</tr>
<tr>
<td>Synchronization schedule</td>
<td>Specify how often (in hours, days, or weeks) synchronization happens between the application and Oracle Identity Cloud Service automatically. If you want to synchronize the user accounts manually, then select Never.</td>
</tr>
</tbody>
</table>

4. Click **Finish**.

**Test the Provisioning Operations You Selected**

After you use the Generic SCIM App Template to configure your application, you must test the provisioning operations you selected to verify that they are operable.

1. In the **Applications** page, select and activate your application, and then click it to open the **Details** tab.
2. Click the **Users** tab, and then click **Assign**.
3. In the **Assign Users** window, choose a user, and then click **Assign**.
4. In the **Assign Application** window, populate any form fields needed to provision a user account to your application, and then click **Save**. Oracle Identity Cloud
Service starts the provisioning operation to create a user account in your application.

5. Verify that the user account has been created in your application.

6. In the **Users** tab, deactivate the user, activate the user again, and remove the user from your application. Each change you make is reflected in the user account for your application.

7. Click the **Import** tab, and then click **Import**.

Oracle Identity Cloud Service communicates with your application's SCIM REST API to get a list of all user accounts. Oracle Identity Cloud Service tries to match each user account with an existing user in Oracle Identity Cloud Service. If a user exists, then the user is assigned to your application. If the user doesn't exist, then you can perform one of the following actions manually:

- **Assign Existing User**: Assign the user account to any user in Oracle Identity Cloud Service.

- **Create New User and Link**: Add a new user to Oracle Identity Cloud Service, and then assign the user account to this newly created user.

**How Do You Develop a Custom SCIM Gateway?**

If your custom application doesn't provide a SCIM-based interface, then you can develop a custom SCIM gateway to act as the interface between Oracle Identity Cloud Service and your custom application. This gateway exposes your application's identity store as SCIM-based REST APIs, and then you can use the Generic SCIM App Template to integrate Oracle Identity Cloud Service with your application for provisioning or synchronization purposes.

Before developing your custom SCIM gateway, if you're a new developer who isn't familiar with the SCIM standard, then you must first understand the SCIM protocol. Then, see which identity attributes are available for your custom application and model them as SCIM-based attributes. Next, utilize open-standard libraries to expose your custom application's APIs as SCIM APIs. Last, familiarize yourself with the create, read, update, and delete (CRUD) operations that you want your custom SCIM gateway to perform.

**Supported Operations**

**User** is a type of resource in the SCIM specification. To manage this resource, the SCIM gateway must expose REST API endpoints to enable operations such as creating, searching for, updating, and deleting users. The HTTP request for the operation that you want to perform and the HTTP response from that operation must be in a **JSON** format.

You can implement the following user operations:

<table>
<thead>
<tr>
<th>User Operation</th>
<th>Description</th>
<th>HTTP Operation</th>
<th>HTTP Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a User</td>
<td>Create a user account in your custom application.</td>
<td><strong>POST</strong></td>
<td><a href="https://app.example.com/scimgate/Users">https://app.example.com/scimgate/Users</a></td>
</tr>
<tr>
<td>User Operation</td>
<td>Description</td>
<td>HTTP Operation</td>
<td>HTTP Endpoint</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Search Users</td>
<td>Obtain a list of all users with their attributes that are in your custom application.</td>
<td>GET</td>
<td><a href="https://app.example.com/scimgate/Users">https://app.example.com/scimgate/Users</a></td>
</tr>
<tr>
<td>Search a User</td>
<td>Retrieve information about a specific user and their attributes in your custom application.</td>
<td>GET</td>
<td><a href="https://app.example.com/scimgate/Users/">https://app.example.com/scimgate/Users/</a>&lt;id&gt;</td>
</tr>
<tr>
<td>Update a User Attribute</td>
<td>Update an attribute value of a user account in your custom application.</td>
<td>PUT</td>
<td><a href="https://app.example.com/scimgate/Users/">https://app.example.com/scimgate/Users/</a>&lt;id&gt;</td>
</tr>
<tr>
<td>Delete a User</td>
<td>Remove a user account from your custom application.</td>
<td>DELETE</td>
<td><a href="https://app.example.com/scimgate/Users/">https://app.example.com/scimgate/Users/</a>&lt;id&gt;</td>
</tr>
</tbody>
</table>

How Do You Secure the Custom SCIM Gateway?

Because you don't want unauthorized users or clients to access your custom SCIM gateway, you must secure it. To do this, use an authorization token to protect the HTTP(S) endpoints of your gateway. This token will validate the user or client to allow them to make appropriate HTTP calls to the gateway endpoints. If the token isn't present or is invalid, then the endpoints will return a 401 HTTP response code because Oracle Identity Cloud Service isn't authorized to access the endpoints.

Oracle Identity Cloud Service uses the administrator's user name and password, which are configured when you register your custom application, to request an access token from the custom SCIM gateway. Oracle Identity Cloud Service can then use this token to access the gateway endpoints as an authorization bearer header.

Sample Implementation of a Custom SCIM Gateway

Oracle provides a sample Node.js application that conforms to SCIM specifications, and which you can use to develop a custom SCIM gateway to integrate it with your custom application.

This custom gateway exposes HTTP endpoints to enable operations such as creating, searching for, updating, and deleting users. The custom gateway stores information about the users locally in the db.json file. This file has the JSON format.
The sample application uses express and body-parser packages. The server.js file implements a route for users' endpoints:

```
"...
var express = require('express')
var app = express()
var bodyParser = require('body-parser');
app.use(bodyParser.json());
var config = require('./config.js');
...
```

The routes/users.js file defines the SCIM REST API endpoints, and maps each endpoint to the corresponding JavaScript function:

```
"...
//Get operation for /Users endpoint
app.get('/scimgate/Users', users.findAll);

//Get operation for /Users/:id endpoint
app.get('/scimgate/Users/:id', users.findOne);

//Put operation for /Users endpoint
app.post('/scimgate/Users', users.create);

//Put operation for /Users/:id endpoint
app.put('/scimgate/Users/:id', users.update);

//Delete operation for /Users endpoint
app.delete('/scimgate/Users/:id', users.delete);
...
```

The user.controller.js file implements JavaScript functions to create, read, update, and delete users in the local user store, represented by the userdb.json file:

```
"...
exports.findAll = function(req, res){
  console.log('Entering findAll function.');
  ...
};

exports.findOne = function(req, res) {
  console.log('Entering findOne function.');
  ...
};

exports.create = function(req, res){
  console.log('Entering create function.');
  ...
};

exports.update = function(req, res){
  console.log('Entering update function.');
  ...
};
```

Chapter 2
What Are the Types of Application Integrations?
The `userdb.json` file contains an array of users, and the structure of each user entry follows the SCIM specification standard, using a subset of the user attributes:

```json
{
  "resources": [
    {
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "id": "1",
      "externalId": "1",
      "userName": "user1@example.com",
      "name": {
        "formatted": "User 1 Name",
        "familyName": "Name",
        "givenName": "User 1"
      },
      "displayName": "User 1 DisplayName",
      "active": true,
      "password": "User1Password",
      "emails": [
        {
          "value": "user1@example.com",
          "type": "work",
          "primary": true
        }
      ]
    }
  ]
}
```

To authorize the client to make HTTP requests, the sample SCIM gateway application makes use of two environment variables that you must set before running the application: `ADMINUSER` and `ADMINPASS`. These variables represent the administrator's user name and password for your API authentication service. You provide values for these variables by setting up the `run.sh` shell script for Unix or Mac environments, or the `run.bat` batch script for Windows environments.

Oracle Identity Cloud Service sends these administrative credentials in the form of an authorization header for all requests to authenticate the administrator's credentials, and then accesses the custom SCIM gateway using the `basic` grant type.

You can modify the sample application's source code and implement other types of authentication methods to match your requirements.
Configure and Run the Custom SCIM Gateway Sample Application

In this section, you configure and run the custom SCIM gateway sample application to work with the `GenericScim - Basic` template.

1. Edit the `run` script file in the `root` folder of the sample SCIM gateway application, update the `ADMINUSER` and `ADMINPASS` values, and then save the file.

   If you're running the sample application in a Unix or Mac environment, then use the `run.sh` script. If you're using Windows, then use `run.bat`.

2. Open a command prompt or terminal, navigate to the `root` folder of the sample application, execute the `run` script by typing the name of the file, and then press Enter to start the sample application. You'll see log information that will help you to understand what the sample application is doing.

   Make sure the hostname of this sample application is reachable through the Internet so that Oracle Identity Cloud Service can contact the application.

Register the Custom SCIM Gateway Application

In this section, you register the custom SCIM gateway sample application with Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Applications, click Add, and then select App Catalog.

2. In the Type of Integration section, click Provisioning, locate the `GenericScim - Basic` template, and then click Add.

3. In the Details pane of the `GenericScim - Basic` page, enter `SCIM Gateway Application` for both the name and description of your application, and then click Next.

4. In the Provisioning pane, turn on the Enable Provisioning switch.

5. In the Confirmation window, click OK.

6. Use the following table to populate the fields of the Configure Connectivity section of the Provisioning tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Enter the host name of your application.</td>
</tr>
<tr>
<td>Base URI</td>
<td>/scimgate</td>
</tr>
<tr>
<td>Administrator Username</td>
<td>admin</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Enter the administrator's password you have set in the run script of the sample application.</td>
</tr>
<tr>
<td>HTTP Operation Types</td>
<td><strong>ACCOUNT</strong>.Update=PUT</td>
</tr>
</tbody>
</table>

For more information about the fields of the Configure Connectivity section, see the table in Enable and Configure Connectivity for Provisioning for Your Application.
7. Click **Finish** to save the application.

If you deploy and run the sample application in a non-HTTPS server or a server which doesn't contain a valid certificate, then you may need to use Oracle Identity Cloud Service’s REST API to change the `SSLEnabled` parameter to `false`. If the server doesn't listen to the default HTTP(s) port number, then change the `Port` parameter to the corresponding port number your application runs. After you update these parameters you can test connectivity between the application and Oracle Identity Cloud Service, and then activate the application.

**Use REST APIs to Update the Custom SCIM Gateway Application**

In this section, you use Oracle Identity Cloud Service REST APIs to update the `port`, and `sslEnabled` parameters of the custom SCIM gateway application.

1. Use a client credential application in Oracle Identity Cloud Service to acquire an access token. If a client credential application hasn’t been created in your environment, then add one.

2. Use the access token as an authorization bearer to execute a `GET` request to the following endpoint:

   ```
   https://yourtenant.identity.oraclecloud.com/admin/v1/Apps?filter=displayName eq "SCIM Gateway Application"
   ```

   The JSON response contains an ID value for this application.

3. Use the ID value and the access token from the previous steps to execute a `PATCH` request to the following endpoint:

   ```
   https://yourtenant.identity.oraclecloud.com/admin/v1/Apps/ºIDº
   ```

   Replace the ID value with the ID value of your application, set the `Content-type` header to `application/json`, and provide the following content for the body:

   ```json
   {
   "schemas": [
   "urn:ietf:params:scim:api:messages:2.0:PatchOp"
   ],
   "Operations": [
   {
   "op": "replace",
   "value": [ "false"]
   },
   {
   "op": "replace",
   "value": [ "6355"]
   }
   ]
   }
   ```

4. In the Identity Cloud Service console, expand the Navigation Drawer, click **Applications**, and then select **SCIM Gateway Application**.
5. In the **Provisioning** pane, click **Test Connectivity** to verify that a connection can be established between Oracle Identity Cloud Service and your custom SCIM gateway application.

6. Click **Finish**, and then click **Activate** to activate the application.

**Test Your Custom SCIM Gateway Sample Application**

Test your custom SCIM gateway sample application by provisioning Oracle Identity Cloud Service users with it.

1. In the **Applications** page, select your application, and then click it to open the **Users** tab.

2. In the **Users** tab, click **Assign**.

3. In the **Assign Users** window, choose a user, and then click **Assign**.

4. In the **Assign Application** window, populate the **Username**, **Full Name**, **Family Name**, **Given Name**, **Display Name**, and **Primary Email** form fields with values, and then click **Save**.

5. In the **Assign Users** window, click **OK**.

Oracle Identity Cloud Service creates a user account in the **userdb.json** file of your application.

6. Open the **userdb.json** file and verify that a user account has been created. Then, close the file.

7. In the **Users** tab, click the **Action** menu to the right of the user, and then select **Deactivate**.

8. After one minute, open the **userdb.json** file and verify that the corresponding user account has a `false` value for the `active` attribute. Then, close the file.

9. In the **Users** tab, click the **Action** menu to the right of the user, and then select **Activate**.

10. After one minute, open the **userdb.json** file and verify that the corresponding user account has a `true` value for the `active` attribute. Then, close the file.

11. In the **Users** tab, select the user, and then click **Revoke**.

12. In the **Confirmation** window, click **OK**.

13. After the **Confirmation** window closes, open the **userdb.json** file and verify that the corresponding user account has been removed. Then, close the file.
Part II
Perform User Tasks

Learn how to perform important end user tasks that you must do right away, and others that you will return to later.

Chapters

• Configure User Settings
• Managing 2-Step Verification
• Use the Oracle Mobile Authenticator App
Configure User Settings

Learn how to configure user settings in Oracle Identity Cloud Service.

Topics:
- Typical Workflow for Configuring User Settings
- Change Your Password
- Recover Your Account
- Set Up or Modify Your Profile
- Set Your Email Options
- Set Your Security Options
- Understanding Social Login
- Accessing My Apps
- Managing Group and Application Access
- Access Your Consents
- #unique_157

**Typical Workflow for Configuring User Settings**

Here are the tasks that administrators and users can do to configure their user settings, manage their Oracle Identity Cloud Service profile information, and manage applications to which they have been granted access.

You can access the Performing self-service tasks infographic to see how to update your password, reset or recover your password, update your email options, and unlock your account in Oracle Identity Cloud Service.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Your Password.</td>
<td>Administrators and users can change their password.</td>
<td>Change Your Password</td>
</tr>
<tr>
<td>Manage Profile Information.</td>
<td>Administrators and users can set up their profile, set their password recovery email address, set their primary email address, configure their account recovery factors, set up and manage their 2–Step Verification methods, and edit their profile information.</td>
<td>Set Up or Modify Your Profile Set Your Email Options Set Your Security Options Manage 2–Step Verification from the My Profile Console</td>
</tr>
<tr>
<td>Access and Organize Applications</td>
<td>Administrators and users can access and organize the applications to which they have been granted access.</td>
<td>Access My Apps</td>
</tr>
</tbody>
</table>
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlink your social account from your Oracle Identity Cloud Service user account.</td>
<td>When you use a social identity provider to sign in to Oracle Identity Cloud Service, your social account is linked to your Oracle Identity Cloud Service user account automatically. If you don't want to sign in to Oracle Identity Cloud Service using that social account, then unlink it.</td>
<td>Unlink Social Accounts</td>
</tr>
<tr>
<td>Access your consents</td>
<td>Users can list and revoke their consents.</td>
<td>Access Your Consents</td>
</tr>
<tr>
<td>Generate Access Token</td>
<td>Users can generate personal access token to be used to invoke Oracle Identity Cloud Service REST API or resources protected by Oracle Identity Cloud Service.</td>
<td>#unique_158</td>
</tr>
</tbody>
</table>

## Change Your Password

Passwords are valid only for the period specified by the password policy defined by your administrator. When your password expires, you must update your password to access Oracle Identity Cloud Service.

1. In the **My Profile** console, click **Change My Password**.
2. In the **Old Password** field, enter your current password.
3. In the **New Password** field, enter a new password.

**Tip:**

If you're using your Oracle Identity Cloud Service password to sign in, then use the **Password Criteria** pane to confirm that your new password conforms to the password policy set by your administrator. If your password conforms to the policy, then each criterion displays a green check mark.

If you're using your Microsoft Active Directory password to sign in to Oracle Identity Cloud Service, then your password policy criteria is defined and maintained by your Microsoft Active Directory administrator. Contact your administrator for more information about this criteria.

4. In the **Confirm New Password** field, reenter your new password.
5. Click **Submit**.

You receive an email verification that your password was updated correctly.
Recover Your Account

If you have trouble signing in to Oracle Identity Cloud Service, you're locked out, or you forget your password, then you can reset your password to recover your account.

There are three factors that you can set to regain access to your account. You can specify an alternate (recovery) email address, provide a mobile number, or select and answer security questions to verify your identity.

1. In the Oracle Identity Cloud Service login page, click the **Click here** link.
2. In the **Forgot Your Password?** page, enter your user name, and then click **Next**.
3. Select the **Recovery Email**, **Mobile Number**, or **Security Questions** account recovery method.
   a. If you select **Recovery Email**, then a **Password Reset** notification is sent to the recovery email address associated with your account. Follow the instructions in the notification to reset your password.
   b. If you select **Mobile Number**, then a passcode is sent to the mobile number associated with your account. Enter the passcode, and then click **Verify** to reset your password.
   c. If you select **Security Questions**, then one of the security questions that you set appears. Provide the answer to this security question, and then click **Verify** to reset your password.

**Important:**
The factors that are available for you to select are dependent upon the selections you made when you set your account recovery options. For example, if you didn't set your mobile number as an account recovery factor, then you can't use this factor to recover your account. It won't appear in the **Forgot Your Password?** page.

If **Recovery Email** is the only account recovery method that you set, then you won't be prompted to select a method. Instead, the **Password Reset** notification is sent to the recovery email address associated with your account.

If you haven't set any account recovery options, then the **Password Reset** notification is sent to your primary email address.

Set Up or Modify Your Profile

If you are logging in to Oracle Identity Cloud Service for the first time, set up your profile information. If you have already set up your profile, you can modify your profile information.

Your profile is a collection of useful data about you. Your profile includes contact information, account information, and also settings that determine the time zone and language that displays for your account in the Identity Cloud Service console.
1. In the My Profile console, click My Profile Details and update any information as necessary. For example, you can change the time zone and language that displays for your account.

2. Click Save.

Set Your Email Options

You can change the primary email address that was set up for you when your account was created.

The primary email address is the email address to which all your notifications are sent. Your administrator has already set your primary email address.

1. In the My Profile console, click Email Options.
2. To the right of the Primary Email field, click Change.
3. In the Reauthentication dialog box, enter your password, and then click OK.
4. In the Primary Email field, enter a new email address.
5. Click Save & Verify.
6. In the verify your email address dialog box, verify your new email address, and then click Send.

A verification email is sent to your new email address. To verify your email address, follow the instructions in the email. Also, an update email notification is sent to your old email address.

Note:

In addition to your primary email address, you can set an alternate (recovery) email address that you can use to help you recover your account. See Set Your Account Recovery Options.

Set Your Security Options

From the My Profile console, you can set your options for account recovery and 2-Step Verification for security purposes.

To set your security options, see one of the following topics:

- Set Your Account Recovery Options
- Manage 2-Step Verification From the My Profile Console

Set Your Account Recovery Options

If you didn’t set your account recovery options the first time you signed in to Oracle Identity Cloud Service, then you can do so from the Security tab of the My Profile console. This way, if you have trouble signing in, you’re locked out, or you forget your password, then you can regain access to your account.
You can access the Manage Account Recovery in Oracle Identity Cloud Service infographic to see how to set your account recovery options when you sign in to Oracle Identity Cloud Service for the first time.

There are three account recovery factors that you can set:

- **Recovery email**: By default, your primary email address has been set as the email address that Oracle Identity Cloud Service will use to help you recover your account. If you have to regain access, then Oracle Identity Cloud Service will send a notification to this email address. Follow the instructions in the notification to recover your account. Instead of your primary email address, you can specify an alternate (recovery) email address to regain access.

- **Mobile number**: You can provide a mobile number that Oracle Identity Cloud Service will use to help you recover your account. This way, if you have to regain access, then Oracle Identity Cloud Service will send a one-time passcode in a text message to this mobile number. You enter this passcode to recover your account.

- **Security questions**: You can select and answer security questions, and provide hints for answers to these questions, to verify your identity. If you have to recover your account, then you must answer these questions correctly to regain access.

**Important:**

The account recovery factors that are available for you to set are dependent upon the selections your identity domain administrator or security administrator made when they set up account recovery for your identity domain. For example, if your administrator deactivated mobile number as an account recovery factor, then you can’t use this factor to recover your account. It won’t appear in the Security tab of the My Profile console. See Configure Account Recovery.

Because you want to be able to regain access to your account, you must set at least one account recovery factor.

---

## Set a Recovery Email Address as an Account Recovery Factor

By default, your primary email address has been set as the email address that Oracle Identity Cloud Service will use to help you recover your account. If you have to regain access, then Oracle Identity Cloud Service will send a notification to this email address. Follow the instructions in the notification to recover your account. Instead of your primary email address, you can specify an alternate (recovery) email address to regain access.

1. In the My Profile console, click **Security**.
2. In the **Recovery Email** pane, click the **Action** menu ⚙️.
3. Select **Edit**.
4. In the **Reauthentication** dialog box, enter your password for security purposes, and then click **OK**.
5. In the **Recovery Email Address** dialog box, enter a different email address to use to recover your account, and then click **OK**.
Oracle Identity Cloud Service sends a verification notification to this email address.

**Tip:**

If you didn't receive the notification, then in the **Recovery Options** page, click **Resend Email**. Oracle Identity Cloud Service will resend the notification to the email address you provided in step 5.

6. In your Inbox, open the verification notification, and then click the **Email Verification** link.

7. In the **Email Verified** page, click the **Click here to continue** link.

8. In the **Recovery Email** pane of the **Recovery Options** page, verify that you see the recovery email address that you provided in step 5.

**Set Your Mobile Number as an Account Recovery Factor**

You can provide a mobile number that Oracle Identity Cloud Service will use to help you recover your account. This way, if you have to regain access, then Oracle Identity Cloud Service will send a one-time passcode in a text message to this mobile number. You enter this passcode to recover your account.

1. In the **My Profile** console, click **Security**.

2. In the **Mobile Number** pane, click **Configure**.

**Note:**

If you don't see a **Configure** button in this pane, then you have already set your mobile number as an account recovery factor.

3. In the **Mobile Number** field of the **Mobile Number** dialog box, select a country code for your mobile number, enter the mobile number to use to recover your account, and then click **Send Passcode**.

Oracle Identity Cloud Service sends a passcode in a text message to this mobile number.

**Note:**

Don’t enter any non-numeric characters for your mobile number. For example, if your mobile number is **212-555-1212**, then enter **2125551212**.

4. Enter the passcode in the text field that appears below the **Mobile Number** field, and then click **Verify**.

**Note:**

If you didn't receive the passcode, then click **Resend**. Oracle Identity Cloud Service will resend the passcode to your mobile number.
Set Security Questions as an Account Recovery Factor

You can select and answer security questions, and provide hints for answers to these questions, to verify your identity. If you have to recover your account, then you must answer these questions correctly to regain access.

1. In the My Profile console, click Security.
2. In the Security Questions pane, click Configure.

**Note:**

If you don’t see a Configure button in this pane, then you have already set security questions as an account recovery factor.

3. In the Security Questions dialog box, select your security questions, provide answers and optional answer hints, and then click Save.

**Tip:**

After you provide an answer to a security question, click Reveal. Your answer will appear in clear text, and you can verify that you entered it correctly.

Modify Your Recovery Email Address

You can change the email address that Oracle Identity Cloud Service will use to help you recover your account if you have to regain access.

To modify your recovery email address, follow the instructions in Set a Recovery Email Address as an Account Recovery Factor.

Modify Your Mobile Number

You can change the mobile number that Oracle Identity Cloud Service will use to help you recover your account if you have to regain access.

1. In the My Profile console, click Security.
2. In the Mobile Number pane, click the Action menu.

**Note:**

If you don’t see in this pane, then you have not set your mobile number as an account recovery factor.

3. Select Edit.
4. In the **Mobile Number** field of the **Mobile Number** dialog box, select a different country code for your mobile number or enter the updated mobile number to use to recover your account, and then click **Send Passcode**.

Oracle Identity Cloud Service sends a passcode in a text message to this mobile number.

5. Enter the passcode in the text field that appears below the **Mobile Number** field, and then click **Verify**.

![Tip]

If you didn’t receive the passcode, then click **Resend**. Oracle Identity Cloud Service will resend the passcode to your mobile number.

---

**Modify Your Security Questions**

You can change the security questions, answers, and hints that Oracle Identity Cloud Service will use to help you recover your account if you have to regain access.

1. In the My Profile console, click **Security**.

2. In the **Security Questions** pane, click the **Action** menu.

![Note]

If you don’t see in this pane, then you have not set security questions as an account recovery factor.

3. Select **Edit**.

4. In the **Security Questions** dialog box, select different security questions, provide other answers and optional answer hints, and then click **Save**.

![Tip]

After you provide an answer to a security question, click **Reveal**. Your answer will appear in clear text, and you can verify that you entered it correctly.

---

**Remove Your Mobile Number as an Account Recovery Factor**

If you no longer want to use your mobile number to recover your account if you have to regain access, then you can remove it as an account recovery factor.

1. In the My Profile console, click **Security**.

2. In the **Mobile Number** pane, click the **Action** menu.
3. Select Remove.
4. In the Confirmation dialog box, click OK.

Remove Security Questions As an Account Recovery Factor

If you no longer want to use security questions to recover your account if you have to regain access, then you can remove them as an account recovery factor.

1. In the My Profile console, click Security.
2. In the Security Questions pane, click the Action menu.

3. Select Remove.
4. In the Confirmation dialog box, click OK.

Understand Social Login

Users can access Oracle Identity Cloud Service using their credentials from trusted public identity providers. After logging into an identity provider, users have the option to create an account in Oracle Identity Cloud Service if they don't have one.

Read the following use cases to understand social login using Oracle Identity Cloud Service.

• Use Case: Log in Using Social Login
• Use Case: Link Social Accounts
• Use Case: Unlink Social Accounts

Use Case: Log in Using Social Login

Read a use case for logging in using social login with Oracle Identity Cloud Service.

Beatrix Kiddo is an end user who needs access Oracle Identity Cloud Service. At the login page, she sees a list of identity providers, including social providers applicable to her. She selects Microsoft and is presented with the Microsoft login form. She completes the steps to log in to Microsoft.

If she doesn't have an Oracle Identity Cloud Service account, she is asked if she would like to register now and create one or if she would like to cancel registration:
• If she chooses to cancel registration, her login attempt is canceled.
• If she chooses to register, then she is shown a registration page with her profile information auto populated.

Note:
The auto populated information varies depending upon the data being captured from the social identity provider.

She provides all required registration information. Her account is created successfully, and she receives an email so that she can activate her account.

Use Case: Link Social Accounts

Read a use case for linking social accounts with Oracle Identity Cloud Service.

Linking social accounts is the process of associating a public identity provider user account with an existing Oracle Identity Cloud Service user account. If multiple social accounts are linked to a user account in Oracle Identity Cloud Service, then the user can access Oracle Identity Cloud Service by logging in with any of the linked social accounts.

To understand how users link social accounts in Oracle Identity Cloud Service, read this use case.

Beatrix Kiddo is an end user for ABC Corporation and an Oracle Identity Cloud Service customer. Beatrix logs in to Oracle Identity Cloud Service using a social account, accesses her user profile, and then accesses the Social Accounts tab. On the Social Accounts tab, she sees the social account that she used the first time to login into Oracle Identity Cloud Service. When she signs in using a social account, that account is automatically linked to her Oracle Identity Cloud Service account.

If she wants to link another social account, she clicks Link a Social Account and completes the steps necessary to log in to the social account. She can now log in using either of those social accounts.

Use Case: Unlink Social Accounts

Read a use case for unlinking social accounts with Oracle Identity Cloud Service.

Unlinking social accounts is the process of disassociating a public identity provider user account with an existing Oracle Identity Cloud Service user account.

To understand how users unlink social accounts in Oracle Identity Cloud Service, read this use case.

Beatrix Kiddo is an end user for ABC Corporation and an Oracle Identity Cloud Service customer. Beatrix logs in to Oracle Identity Cloud Service using a social account provided for her on the Oracle Identity Cloud Service login page. When she does this, her existing Oracle Identity Cloud Service user account is associated with her public identity provider user account.

Beatrix doesn't want to use one of her social accounts anymore. She wants to unlink this social account. When she does, her Oracle Identity Cloud Service account is no longer linked to that social account.
Link and Unlink Social Accounts

When you use a social identity provider to sign in to Oracle Identity Cloud Service, your social account is linked to your Oracle Identity Cloud Service user account automatically. If you don't want to sign in to Oracle Identity Cloud Service using that social account, then unlink it.

If your social account is unlinked, then you can link it to establish a connection between your social account and your Oracle Identity Cloud Service user account. As a result, you can use your social credentials to access Oracle Identity Cloud Service.

If a social identity provider is created and activated, then you'll see the **Social Accounts** tab. Otherwise, this tab won't appear.

1. In the My Profile console, click **Social Accounts**, and then click **Link a Social Account**.

2. In the **Link a Social Account** dialog box, click the **Action** menu, and then click **Link**.

   A login page with the social account that you chose displays.

3. Complete the steps necessary to log in to your social account.

   You're redirected to Oracle Identity Cloud Service.

4. In the My Profile console, click **Social Accounts**, and then verify that the social account you linked appears.

5. (Optional) To unlink a social account, click the **Action** menu, and then click **Unlink**.

Access My Apps

Use the **My Apps** page to access and organize applications.

Applications that show in the **My Apps** page are applications to which the administrator has granted you access. Access can be granted to you as an individual user or to a group to which you belong. You are directed to the **My Apps** page after you activate your account and each time you log in thereafter.

1. Click your avatar and then choose **My Apps**.

2. Search for applications by entering a string that begins the application name.

3. Set your favorites.

4. Sort applications by **Name** and **Recently Granted**.

5. To access an application, click the application tile or the application name to be taken to the home page of the application. Bookmark application homepages so that you can access the applications directly.

Use Form Fill Applications

Store your application credentials using form fill apps so that you have one click access to the websites you use most.

Complete the following prerequisites before using form fill apps,
• Open the **My Apps** page using a Google Chrome or Mozilla Firefox browser.

**Note:**

Internet Explorer and Edge is not supported.

• Install the Oracle Secure Form Fill Plugin. If one or more apps require the plug-in, a message appears at the top of the page with an option to install it. Click **Install Plugin** and follow the instructions. Without the plug-in installed, apps that require the plug-in are locked.

1. After installing the Oracle Secure Form Fill Plugin, refresh the **My Apps** page.
2. Open a form fill app.
3. Install the secure form fill plug in, you have not already done installed it, and then refresh your browser.

**Note:**

If you are using Google Chrome, you are prompted to go to the Extensions on Google Chrome and install the Oracle Secure Form Fill Plugin.

If you are using Mozilla Firefox, instead of downloading the Secure Form Fill Mozilla Firefox plug-in from the Mozilla Store, install the Secure Form Fill Mozilla Firefox plug-in from the My Apps page.

Internet Explorer and Edge are not supported.

4. Enter your application credentials, and then click **Login**.

The application launches and signs you into the website. Ensure that you log out of the website when finished.

If your user name or password changes for an application, click the gear icon to update your login credentials. You can also retrieve login information such as your application password.

### Manage Group and Application Access

After you request group and application access from the Catalog page you can view your access and requests from the My Profile page.

**Topics**

• **Requesting Application and Group Access**

• **Viewing Group and Application Access**

• **Viewing Group and Application Access Requests**
Request Group and Application Access

Request access to groups to which you want to be a member and to applications to which you want use. If you do not see the group or application on the Catalog page, the administrator has not allowed the group or application to be requested. To make the group or application accessible, contact your administrator.

1. Click your user name, and then select Catalog from the drop-down menu.
2. In the Catalog page, select either Groups or Applications.
3. Click the plus (+) sign for the group or application to which you want access.
4. In the Add Access dialog box, enter the reason for the request, and then click OK.

Two emails are sent to you.

- The first email verifies your request. To go to the My Requests tab and verify that your request has been submitted, click the My Requests link in the email.
- The second email verifies your access. To go to the My Access tab and verify that your access has been granted, click the My Access link in the email.

View Group and Application Access

1. In the My Profile console, click the My Access tab.
2. To view your group or application access, click the Groups or Applications. The groups and applications that you have access to are listed.

View Group and Application Access Requests

To view your requests for group and application access, in the My Profile console, click the My Requests tab. Your group and application access requests are listed.

For each request, the following information is displayed:

- The name of the group or application.
- The justification you entered while requesting for the group or application
- The date and time when you submitted the request
- A check mark with each request to denote that you have been granted access to the group or application.

Access Your Consents

For some applications, you must agree to the terms of use so that you can access them. Also, application resources may require consent so that client applications can access these resources. You can view and revoke the terms of use and consents of applications you have agreed upon.

The My Consents page of the My Profile console lists two types of applications:
• Applications you have agreed to the terms of use.
• Applications you have consented access to resources.

The Terms of Use Consents section in the My Consents page of the My Profile console is associated with consents that you agreed to upon accessing applications protected by Oracle Identity Cloud Service.

The Application Consents section of this page refers to OAuth consents that you allowed applications to access, for resource scopes that require consent.

1. In the My Profile console, click My Consents.

   The page shows the list of applications that you have agreed to the terms of use, and the list of applications you have allowed consent.

2. For both the Terms of Use Consents and Application Consents sections, perform the following:

   • Open the Terms of Use consent: Click one of the application names. The Terms of Use page opens and displays the statement of the consent the user agreed upon for the application.

   • Revoke: Select the check box in front of the application name, and then click Revoke.

     Alternatively, you can click the action menu option of the application, and then click Revoke.

     In the Confirmation window, click OK to confirm you want to revoke the terms of use consent.
Manage 2-Step Verification

Learn how to configure 2-Step Verification for your account.

- Enroll in 2-Step Verification for Your Account
- Add Backup Verification Methods
- Trust a Device
- Set a Default Verification Method
- Manage 2-Step Verification from the My Profile Console

Typical Workflow for Managing 2-Step Verification

There are two ways to set up 2-Step Verification for your account, during 2-Step Verification enrollment or using the 2-Step Verification page from the Oracle Identity Cloud Service self-service console. Use the 2-Step Verification page to perform tasks such as enabling and disabling 2-Step Verification, setting up authentication methods, trusting a device, and generating bypass codes.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enroll in 2-Step Verification for Your Account</td>
<td>Learn how to enroll in 2-Step Verification during 2-Step Verification enrollment and the authentication methods available to you.</td>
<td>Enroll in 2-Step Verification for Your Account</td>
</tr>
<tr>
<td>Add Backup Verification Methods</td>
<td>Learn how to add backup verification methods for your account when you enroll in 2-Step Verification.</td>
<td>Add Backup Verification Methods</td>
</tr>
<tr>
<td>Trust a Device</td>
<td>Learn how to trust a device when you enroll in 2-Step Verification.</td>
<td>Trust a Device</td>
</tr>
<tr>
<td>Set a Default Verification Method</td>
<td>Learn how to set a default verification method when you enroll in 2-Step Verification.</td>
<td>Set a Default Verification Method</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding a 2-Step Verification Method</td>
<td>Learn how to add 2-Step Verification methods on the 2-Step Verification page and the authentication methods that are available to you.</td>
<td>Adding a 2-Step Verification Method from the Self-Service Console</td>
</tr>
<tr>
<td>Removing a 2-Step Verification Method</td>
<td>Learn how to remove 2-Step Verification methods on the 2-Step Verification page.</td>
<td>Removing a 2-Step Verification Method</td>
</tr>
</tbody>
</table>
Enroll in 2–Step Verification for Your Account

2-Step Verification is an authentication method that requires you to use more than one way of verifying your identity, providing a second layer of security to your accounts.

After you enter your user name and password at the login page, you use a second verification method, such as a passcode that is sent as an SMS to your mobile device. This prevents anyone but you from logging in, even if they know your password. There are two ways to set up 2-Step Verification for your account, during 2-Step Verification enrollment or using the My Profile console. This section covers the steps to set up authentication methods during enrollment, and also the steps required to use those methods to verify your identity during log in.

The following 2–Step Verification methods are supported:

- **Text Message (SMS)**
  - Set Up a Mobile Number as an Authentication Method
  - Use a Mobile Number as an Authentication Method

- **Mobile App OTP and Notifications**
  - Set Up the Oracle Mobile Authenticator App as an Authentication Method
  - Use the Oracle Mobile Authenticator App as an Authentication Method
  - Set Up a Third-Party Authenticator App as an Authentication Method
  - Use a Third-Party Authenticator App as an Authentication Method

- **Security Questions**
  - Set Up Security Questions as an Authentication Method
  - Use Security Questions as an Authentication Method

- **Email**
  - Set Up Email as an Authentication Method
  - Use Email as an Authentication Method
Set Up a Mobile Number As An Authentication Method

Enroll your mobile number as a 2–Step Verification method.

When Multi-Factor Authentication (MFA) is enabled, the first time that you log in, the Enable 2-Step Verification flow appears after you enter your user name and password.

1. On the Enable 2-Step Verification introduction page, click **Enable**.
   
The authentication methods available to you appear on the **Select a Method** page.

2. Click **Mobile Number**.

3. Enter the mobile number where you want to receive the passcode, and then click **Send**.
   
   Oracle Identity Cloud Service sends a passcode by SMS to your mobile device.

4. Enter the passcode into the **Passcode** box, and then click **Verify**. The **Successfully Enrolled** page appears.
   
   If you do not receive a text, click **Resend**.

5. Click **Done**.
   
   To set up an additional method during enrollment, select another method from the bottom of the page, and then walk through the enrollment process for that method. Alternatively, you can set up additional methods later using the **Security** tab in the Oracle Identity Cloud Service My Profile console.

Use a Mobile Number as an Authentication Method

After you enroll your mobile device as a 2–Step Verification method, use it to provide a second method of verification when you log in.

1. Enter your user name and password in an MFA-protected environment.
   
   The 2-Step Verification page appears, and then you are prompted for your second verification method.
   
   A text message that contains a passcode is sent to the mobile number that you entered.

2. Enter that passcode into the **Passcode** box on the 2-Step Verification page, and then click **Verify**.
   
   If you didn’t receive the passcode, click **Resend Passcode**.

3. Optional. If you can’t receive a text, for example, you don’t have your phone with you, click **Use backup verification method** to use an alternative method to verify your identity.

---

**Note:**

You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven’t set up more than one verification method, you can call the help desk and have a bypass code generated for you.
4. Optional. You can also select **Use backup verification method** to change your default verification method.
   a. Click **Use backup verification method**. All 2–Step Verification methods that you are enrolled in appear in the **Backup Verification Method** section.
   b. Select a different verification method. You are then prompted to enter the required verification for that method.
   c. Enter the required verification.
   d. Select the **Make this my default method** check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.

5. Optional. Select the **Trust this computer for _ days** check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.

**Set Up the Oracle Mobile Authenticator App as an Authentication Method**

Enroll the Oracle Mobile Authenticator (OMA) app as a 2–Step Verification method.

When Multi-Factor Authentication (MFA) is enabled, the first time that you log in, the Enable 2-Step Verification flow appears after you enter your user name and password.

1. On the Enable 2-Step Verification introduction page, click **Enable**.
   The authentication methods available to you appear on the **Select a Method** page.

2. Click **Mobile App**.
   You are prompted to download the Oracle Mobile Authenticator app from the app store.

3. After you install the OMA app, you need to link it to an account. You can add an account three ways:
   a. **Scan the Quick Response (QR) code**
   b. **Enter the key manually**
   c. **Use the enrollment URL**
   After you add the account using one of these methods, OMA app enrollment is complete.

**Use the Oracle Mobile Authenticator App as an Authentication Method**

After you enroll the Oracle Mobile Authenticator (OMA) app as a 2–Step Verification method, use it to provide a second method of verification to securely log in to applications.

1. Enter your user name and password in an MFA-protected environment.
   The **2-Step Verification** page appears, and then you are prompted for your second verification method.
2. Which authentication method that appears depends on the MFA method that your administrator enabled:

If your administrator enabled both Mobile App OTP and Mobile App Notification, Mobile App Notification is the default method pushed to your phone for authentication.

a. Mobile App OTP

To avoid clock skew, which is the time difference between the server and your device, make sure that your device clock is synchronized. The maximum allowed time difference is 90 seconds.

- You are prompted to enter the passcode that is generated by the OMA app on your mobile device.
- Tap the OMA app on your device to launch it.
- Tap the account for which you want to generate a new OTP. An OTP for the account appears, and the countdown begins until a new OTP is automatically generated.
- Enter or paste that passcode into the Passcode box on the 2-Step Verification page, and then click Verify.

b. Mobile App Notification

- You are prompted to open and respond to the notification that was sent to the OMA app on your mobile device.
- Open the notification in the OMA app, and then tap Allow.

3. Optional. If you are unable to use the OMA app, for example, you don’t have your phone with you, click Use backup verification method to use an alternative method to verify your identity.

Note:
You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven’t set up more than one verification method, you can call the help desk and have a bypass code generated for you.

4. Optional. You can also select Use backup verification method to change your default verification method.

a. Click Use backup verification method. All 2–Step Verification methods that you are enrolled in appear in the Backup Verification Method section.

b. Select a different verification method. You are then prompted to enter the required verification for that method.

c. Enter the required verification.

d. Select the Make this my default method check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.

5. Optional. Select the Trust this computer for _ days check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.
Set Up a Third-Party Authenticator App as an Authentication Method

Enroll a third-party authenticator app as a 2–Step Verification method.

When Multi-Factor Authentication (MFA) is enabled, the first time that you log in, the Enable 2-Step Verification flow appears after you enter your user name and password.

1. On the Enable 2-Step Verification introduction page, click **Enable**. The authentication methods available to you appear on the **Select a Method** page.
2. Click **Mobile App**, and then select the **Scan offline QR** code check box.
3. Scan the offline version of the Quick Response (QR) code that appears for use with third-party authenticators. If you can't scan the QR code, you are also given the option the enter the key manually. You can use either option with the third-party authenticator app. We recommend using the Oracle Mobile Authenticator as it supports notifications and many important security features.
4. After set up is complete on the Authenticator app, a one-time passcode (OTP) appears for your account in the third-party authenticator app. Enter that OTP on the **Enable 2-Step Verification** page, and then click **Verify**. The **Successfully Enrolled** page appears.
5. Click **Done**.

To set up an additional method during enrollment, select another method from the bottom of the page, and then walk through the enrollment process for that method. Alternatively, you can set up additional methods later using the **Security** tab in the Oracle Identity Cloud Service My Profile console.

Use a Third-Party Authenticator App as an Authentication Method

After you enroll a third-party authenticator app as a 2–Step Verification method, use it to provide a second method of verification when you log in.

1. Enter your user name and password in an MFA-protected environment. The **2-Step Verification** page appears, and then you are prompted for your second verification method. You are prompted to enter the passcode that is generated by the third-party authenticator app on your mobile device.
2. Enter that passcode into the **Passcode** box on the 2-Step Verification page, and then click **Verify**.
3. Optional. If you are unable to use the App, for example, you don’t have your phone with you,click **Use backup verification method** to use an alternative method to verify your identity.
You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven't set up more than one verification method, you can call the help desk and have a bypass code generated for you.

4. Optional. You can also select **Use backup verification method** to change your default verification method.
   a. Click **Use backup verification method**. All 2–Step Verification methods that you are enrolled in appear in the **Backup Verification Method** section.
   b. Select a different verification method. You are then prompted to enter the required verification for that method.
   c. Enter the required verification.
   d. Select the **Make this my default method** check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.

5. Optional. Select the **Trust this computer for _ days** check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.

### Set Up Security Questions as an Authentication Method

Enroll in the security questions 2–Step Verification method.

When Multi-Factor Authentication (MFA) is enabled, the first time that you log in, the Enable 2-Step Verification flow appears after you enter your user name and password.

1. On the Enable 2-Step Verification introduction page, click **Enable**.
   The authentication methods available to you appear on the **Select a Method** page.

2. Click **Security Questions**.
   The number of security questions that you are required to answer appear.

3. Select the questions, and then provide your answers.

4. Optional. Enter answer hints. The answer and the hint can't be the same.
   The hint appears as a tooltip when you are using security questions as your second authentication method.

5. Click **Save**.
   The **Successfully Enrolled** page appears.

6. Click **Done**.
   To set up an additional method during enrollment, select another method from the bottom of the page, and then walk through the enrollment process for that method. Alternatively, you can set up additional methods later using the **Security** tab in the Oracle Identity Cloud Service My Profile console.
Use Security Questions as an Authentication Method

After you enroll in the security questions 2-Step Verification method, use it to provide a second method of verification when you log in.

1. Enter your user name and password in an MFA-protected environment. The 2-Step Verification page appears, and then you are prompted for your second verification method.

2. Enter the answers to your security questions, and then click Verify.

3. Optional. If you forgot your answers, click Use backup verification method to use an alternative method to verify your identity.

   Note:
   You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven’t set up more than one verification method, you can call the help desk and have a bypass code generated for you.

4. Optional. You can also select Use backup verification method to change your default verification method.

   a. Click Use backup verification method. All 2-Step Verification methods that you are enrolled in appear in the Backup Verification Method section.

   b. Select a different verification method. You are then prompted to enter the required verification for that method.

   c. Enter the required verification.

   d. Select the Make this my default method check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.

5. Optional. Select the Trust this computer for _ days check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.

Set Up Email as an Authentication Method

Enroll your email as your 2-Step Verification method.

When Multi-Factor Authentication (MFA) is enabled, the first time that you log in, the Enable 2-Step Verification flow appears after you enter your user name and password.

1. On the Enable 2-Step Verification introduction page, click Enable. The authentication methods available to you appear on the Select a Method page.

2. Click Email.
   Oracle Identity Cloud Service sends a one-time passcode to your primary email address.
3. Enter the passcode into the **Passcode** box, and then click **Verify**. The **Successfully Enrolled** page appears.
   If you do not receive an email, click **Resend email**.

4. Click **Done**.
   To set up an additional method during enrollment, select another method from the bottom of the page, and then walk through the enrollment process for that method. Alternatively, you can set up additional methods later using the **Security** tab in the Oracle Identity Cloud Service My Profile console.

**Use Email as an Authentication Method**

After you enroll your primary email as a 2–Step Verification method, use it to provide a second method of verification when you log in.

1. Enter your user name and password in an MFA-protected environment.
   The **2-Step Verification** page appears, and then you are prompted for your second verification method.
   If email is your default 2–Step Verification method, an email that contains a passcode is sent to your primary email address. If email isn’t your default 2–Step Verification method, you can click **Use backup verification method** and select **Email** from the list of backup methods.
   After you enroll in email as a 2–Step Verification method, if you change your primary email address and the change is verified, Oracle Identity Cloud Service automatically sends the passcode to the updated address. There is no need to re-enroll.

2. Enter that passcode into the **Passcode** box on the 2-Step Verification page, and then click **Verify**.
   If you didn’t receive the email, click **Resend email**.

3. Optional. If you can’t receive an email, click **Use backup verification method** to use an alternative method to verify your identity.

   **Note:**
   You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven’t set up more than one verification method, you can call the help desk and have a bypass code generated for you.

4. Optional. You can also select **Use backup verification method** to change your default verification method.
   a. Click **Use backup verification method**. All 2–Step Verification methods that you are enrolled in appear in the **Backup Verification Method** section.
   b. Select a different verification method. You are then prompted to enter the required verification for that method.
   c. Enter the required verification.
   d. Select the **Make this my default method** check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.
5. Optional. Select the **Trust this computer for ___ days** check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.

### Add Backup Verification Methods

When you need to log in and provide a second verification method, backup verification methods come in handy if you have left your device at home, for example.

To set up an additional method during Multi-Factor Authentication (MFA) enrollment, on the **Successfully Enrolled** page of the 2-Step Verification flow, select another method from the bottom of the page. You then walk through the enrollment process for that method. Alternatively, you can set up additional methods using the **2-Step Verification** page in the Oracle Identity Cloud Service self-service console.

### Trust a Device

When you access an app for the first time using your 2-Step Verification method from your computer or a device, you have the option to flag your computer or device as trusted. Trusted devices don’t require you to provide a second method of authentication each time that you log in (for a defined time period that is set by your administrator).

This feature is similar to the “remember my computer” option that you often see during authentication on many web sites. When you log in and provide your second verification method, select the **Trust this computer for ___ days** check box. That device is then listed in the **Trusted Devices** section of the **Security** tab in the Oracle Identity Cloud Service My Profile console. See **Manage 2-Step Verification Using the Self-Service Console**.

If you choose not to trust the computer, you are prompted for 2-Step Verification each time that you log in from that device. You have the opportunity each time that you log in to trust the computer or device.

### Set a Default Verification Method

When you enable 2-Step Verification you can set a 2-Step Verification method as your default.

You can change your default verification method the first time that you log in to an MFA protected environment, or you can use the **Security** page in the **My Profile** console of Oracle Identity Cloud Service.

1. Enter your user name and password in an MFA-protected environment. On the Enable 2-Step Verification introduction page, click **Enable**. Or, from the **Security** page in the **My Profile** console, click **Enable**.

2. Select one of your previously set up account recovery methods as your default by clicking **Set as Default** next to the method.

   You are prompted to provide the appropriate verification, such as an OTP or answer security questions.

3. To enroll in a new 2-Step Verification method and set that method as your default, click the button for that method.
You are prompted to walk through the enrollment steps for that method.

4. Click **Done**.

To change your default verification method after enrolling:

- **Change Your Default Verification Method During Login**
- **Change Your Default Verification Method Using the My Profile Console**

### Change Your Default Verification Method During Login

You can change your default verification method when you log in.

1. Enter your user name and password in an MFA-protected environment.
   
   The **2-Step Verification** page appears, and then you are prompted for your second verification method.

2. Click **Use backup verification method**. All 2–Step Verification methods that you are enrolled in appear in the **Backup Verification Method** section.

3. Select a different verification method. You are then prompted to enter the required verification for that method.

4. Enter the required verification.

5. Select the **Make this my default method** check box to set this 2-Step Verification method as your default. The next time that you log in, you are prompted to verify your identity using this method of verification.

### Manage 2–Step Verification from the My Profile Console

If you skipped enrolling in 2-Step Verification when you signed in to Oracle Identity Cloud Service, then you can do so from the **Security** tab of the **My Profile** console.

2-Step Verification is an authentication method that requires you to use more than one way of verifying your identity, providing a second layer of security to your accounts. After you enter your user name and password at the login page, you use a second verification method, such as a passcode that is sent as an SMS to your mobile device. This prevents anyone but you from logging in, even if they know your password. There are two ways to set up 2-Step Verification for your account, during 2-Step Verification enrollment or using the My Profile console.

There are many 2-Step Verification methods that you can set up. The methods that are available to you for set up are selected by your identity domain administrator or security administrator.

- **Mobile App**: Use a mobile app to generate a time-based passcode (OTP). A prompt appears for you to enter the passcode that you obtain from the mobile app. Or, a login request is sent to the mobile app and you tap **Allow** to authenticate.

- **Mobile Number**: Send a passcode as a text message (SMS) to your phone that you then enter on the page.

- **Security Questions**: Answer security questions.

- **Email**: Send an OTP to your primary email address that you then enter on the page.
• **Bypass Code**: Generate a bypass code and store it for later use. You can also contact an administrator to obtain a bypass code for access.

The following topics provide more information on managing your 2-Step Verification methods from the **Security** page.

- Add a 2–Step Verification Method from the My Profile Console
- Rename a 2–Step Verification Method
- Remove a 2–Step Verification Method
- Manage Security Questions
- Generate a Bypass Code
- Use a Bypass Code
- Remove a Trusted Device
- Set a Default Verification Method
- Change Your Default Verification Method Using the My Profile Console

### Add a 2–Step Verification Method from the My Profile Console

Use the 2–Step Verification page in Oracle Identity Cloud Service to add a verification method for your account.

These steps assume that you are already enrolled in 2-Step Verification and want to add an additional method.

1. Access the My Profile console by clicking your initials in the upper-right corner, and then select **My Profile** from the drop-down list.

2. Click **Security**. If you see **Enable** in the **2-Step Verification** section of the page, you aren’t currently enrolled in 2–Step Verification. Click **Enable** to get started.

3. Locate the method that you want to add, and in the pane for that method, click **Configure**.

4. Walk through the enrollment wizard to add the method. These are the same steps that you perform when you set up an authentication method during enrollment.

### Remove a 2–Step Verification Method

Use the **2–Step Verification** section of the **Security** page in Oracle Identity Cloud Service to remove a verification method from your account.

1. Access the My Profile console by clicking your initials in the upper-right corner, and then select **My Profile** from the drop-down list.

2. Click **Security**. If you see **Enable** in the **2-Step Verification** section of the page, you aren’t currently enrolled in 2–Step Verification. Click **Enable** to get started.

3. Locate the method pane for the method that you want to remove, and then click the **Action** menu 🕒.

4. Select **Remove**, and then at the confirmation dialog box, click **OK**.
Rename a 2–Step Verification Method

Use the 2–Step Verification section of the Security page in Oracle Identity Cloud Service to rename a verification method associated with your account, for example, when you add another mobile number, and you want each name to be more descriptive.

1. Access the My Profile console by clicking your initials in the upper-right corner, and then select My Profile from the drop-down list.
2. Click Security. If you see Enable in the 2-Step Verification section of the page, you aren’t currently enrolled in 2–Step Verification. Click Enable to get started.
3. Click the Action menu for the method that you want to rename.
4. Select Rename, enter a new name for the method, and then click Save.

Manage Security Questions

Use the 2–Step Verification section of the Security page in Oracle Identity Cloud Service to set up and manage security questions that are associated with your account.

1. Access the My Profile console by clicking your initials in the upper-right corner, and then select My Profile from the drop-down list.
2. Click Security. If you see Enable in the 2-Step Verification section of the page, you aren’t currently enrolled in 2–Step Verification. Click Enable to get started.
3. Locate the Security Questions pane and click Configure.
   The Security Questions dialog box appears.
4. To set up your security questions:
   a. Select the questions, and then provide your answers.
   b. Optional. Enter answer hints. The answer and the hint can’t be the same.
      The hint appears as a tooltip when you are using security questions as your second authentication method.
   c. Click Save.
5. To manage existing security questions, make your changes, and then click Save.

Generate a Bypass Code

A bypass code is useful as a second verification method when you forgot your phone, don’t have service, or can’t access your computer. You can generate bypass codes after you enroll in 2-Step Verification, and then store the codes in a safe place.

Use the Security tab in Oracle Identity Cloud Service to generate bypass codes for your account.

1. Access the My Profile console by clicking your initials in the upper-right corner, and then select My Profile from the drop-down list.
2. Click Security. If you see Enable in the 2-Step Verification section of the page, you aren’t currently enrolled in 2–Step Verification. Click Enable to get started.
3. Locate the **Bypass Codes** section, and then click **Generate**.

4. At the **Confirmation** window, copy your bypass code, and then store it in a safe place for use the next time that you need a backup verification method.

5. Click **Done**.

   A bypass code pane displays the number of uses allowed. Your bypass code doesn't expire, but you can only use it once.

6. (Optional) Click **Reveal** to view and copy your bypass code.

7. (Optional) Click the **Action** menu in the bypass code pane, click **Email**, and then click **OK** in the **Confirmation** window to send the bypass code to your email.

### Use a Bypass Code

After you generate bypass codes, you can use them as a second method of verification when you forget your phone, don't have service, or can't access your computer.

1. Enter your user name and password in an MFA-protected environment. The **2-Step Verification** page appears, and then you are prompted for your second verification method.

2. If you can't use your usual second verification method (for example, because you don't have your phone or you have no Internet connectivity), click **Use backup verification method** to use an alternative method to verify your identity.

3. In the **Backup Verification Methods** section of the page, click **Use a bypass code**.

   **Note:**
   
   You must have previously set up more than one verification method, such as using a bypass code that you previously generated and stored in a safe place. If you haven't set up more than one verification method, you can call the help desk and have a bypass code generated for you.

4. You are prompted to either enter your bypass code or contact the help desk to have an administrator generate a bypass code for you. Enter your code in the **Bypass code** box, and then click **Verify**.

5. Optional. Select the **Trust this computer for _ days** check box (if enabled by your administrator) to skip providing a second method of authentication for the number of days indicated when you log in from the same device. The number of days is defined by your administrator.

### Remove a Trusted Device

Use the **2–Step Verification** section of the **Security** page in Oracle Identity Cloud Service to remove a trusted device that is associated with your account.

Devices are trusted when you select the **Trust this device for _ days** check box during log in.
1. Access the My Profile console by clicking your initials in the upper-right corner, and then select My Profile from the drop-down list.

2. Click Security. If you see Enable in the 2-Step Verification section of the page, you aren’t currently enrolled in 2–Step Verification. Click Enable to get started.

3. Locate the Trusted Devices section.

4. Click the Action menu for the trusted device that you want to remove.

5. At the confirmation dialog box, click OK. The next time that you log in from that device, you are prompted for a second verification method to log in.

Set a Default Verification Method

When you enable 2-Step Verification you can set a 2-Step Verification method as your default.

You can change your default verification method the first time that you log in to an MFA protected environment, or you can use the Security page in the My Profile console of Oracle Identity Cloud Service.

1. Enter your user name and password in an MFA-protected environment. On the Enable 2-Step Verification introduction page, click Enable. Or, from the Security page in the My Profile console, click Enable.

2. Select one of your previously set up account recovery methods as your default by clicking Set as Default next to the method.

   You are prompted to provide the appropriate verification, such as an OTP or answer security questions.

3. To enroll in a new 2-Step Verification method and set that method as your default, click the button for that method.

   You are prompted to walk through the enrollment steps for that method.

4. Click Done.

   To change your default verification method after enrolling:
   • Change Your Default Verification Method During Login
   • Change Your Default Verification Method Using the My Profile Console

Change Your Default Verification Method Using the My Profile Console

You can change your default verification method using the My Profile console if you are enrolled in more than one method.

1. Click Security. If you see Enable in the 2-Step Verification section of the page, you aren’t currently enrolled in 2–Step Verification. Click Enable to get started.

   A check mark on the method pane indicates your current default verification method.

2. Click the 2-Step Verification Action menu and select Change Default.
The Change Default window displays the 2–Step Verification methods that you are enrolled in.

3. Select the method that you want to use as your default verification method.

4. Click Done.

The check mark appears on the method pane that you just set as your default.
Use the Oracle Mobile Authenticator App

Topics

• Typical Workflow for Managing the Oracle Mobile Authenticator App
• Use the Oracle Mobile Authenticator App

Typical Workflow for Managing the Oracle Mobile Authenticator App

Use the Oracle Mobile Authenticator (OMA) App to perform tasks such as adding an account to the OMA App and then using the OMA App as a second verification method with Oracle Identity Cloud Service.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the OMA App</td>
<td>Learn how to add an account to the OMA App by scanning the QR code, entering the key manually, or using the enrollment URL</td>
<td>Add an Account to the OMA App by Scanning the QR Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add an Account to the OMA App by Entering the Key Manually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add an Account to the OMA App by Using the Enrollment URL</td>
</tr>
<tr>
<td>Manage the Oracle Mobile</td>
<td>Learn how to switch between grid and list views, edit and delete accounts, manage your PIN, and view notification history.</td>
<td>Manage the OMA App</td>
</tr>
<tr>
<td>Authenticator App</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use the Oracle Mobile Authenticator App

The Oracle Mobile Authenticator (OMA) app is a mobile device app that you can use as a second verification method by tapping Allow on the login request notification sent to your phone or by using the one-time passcode (OTP) that the app generates.

A mobile authenticator app uses either OTP or push notifications to prove that the user has possession of the mobile device. Only the mobile authenticator app that is in possession of the user’s secret key can generate a valid OTP. You can download the Oracle Mobile Authenticator app from the app store.

<table>
<thead>
<tr>
<th>OMA App Version</th>
<th>Mobile Platform Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 4.0+</td>
<td>iOS 7.1+</td>
</tr>
</tbody>
</table>
Add an Account to the OMA App by Scanning the QR Code

After you install the Oracle Mobile Authenticator (OMA) app, you can link the App to an account by scanning the quick response (QR) code.

1. Open the OMA app on your phone, and then tap Add Account.
2. Scan the QR code that displays on the Enable 2-Step Verification page. After setup is complete, the Successfully Enrolled page appears.
   If you are scanning the offline QR code:
   a. After setup is complete, the OMA app displays a one-time passcode (OTP) for your account.
   b. Click Verify.
      The Successfully Enrolled page appears.
3. Click Done.

Add an Account to the OMA App by Entering the Key Manually

After you install the Oracle Mobile Authenticator (OMA) app on your device, you can link the App to an account by entering the key manually.

1. On the Enable 2-Step Verification page, select the Scan offline QR code check box, and then click Enter key manually.
   The enrollment instructions on the page switch to configuring the OMA app manually.
2. Open the OMA app on your phone, and then tap Add Account.
3. Tap Enter Key Manually.
4. Select Oracle as the Account Type, and then enter your user name as the Account, which is typically your email address.
5. On the Enable 2-Step Verification page, enter the key that displays, and then tap Save.
6. After setup is complete, the OMA app displays a one-time passcode (OTP) for your account. Enter that OTP on the Enable 2-Step Verification page.
7. Click **Verify**.
   The **Successfully Enrolled** page appears.

8. Click **Done**.

**Add an Account to the OMA App Using the Enrollment URL**

After you install the Oracle Mobile Authenticator (OMA) app, you can link the App to an account by tapping the enrollment URL.

You must perform these steps from your mobile device using a supported mobile browser: iOS – Safari, Android and Windows – Any mobile browser.

1. On the **Enable 2-Step Verification** page from your mobile device, tap **Configure the App using this URL**. A window displays two options for using the enrollment URL:
   a. Tap the enrollment URL to open the OMA app on your device and start the configuration process. For iOS devices, you must use the Safari browser to launch the enrollment URL.
   b. Enter your email address, and then click **Send** to send the enrollment URL to your email address. Make sure to open the email on your device, and then tap the enrollment URL.

   The **Successfully Enrolled** page appears.

2. Tap **Done**.

**Manage the Oracle Mobile Authenticator App**

The Oracle Mobile Authenticator (OMA) app makes it easy for you to customize how you view your accounts, manage your PIN, and manage notifications.

**Topics**

- Switch Between Grid View and List View in the OMA App
- Manually Check for Pending Notifications
- Edit Accounts in the OMA App
- Reorder Accounts in the OMA App
- Delete an Account in the OMA App
- Enable OMA App Protection
- Change Your OMA App PIN
- Disable OMA App PIN Protection
- Manage Notification History in the OMA App

**Switch Between Grid View and List View**

You can change how you view your list of accounts in the Oracle Mobile Authenticator (OMA) app.

1. Launch the OMA app, and then tap the menu icon in the upper-left corner.
2. Tap **Grid View** or **List View** to toggle between the two views.
For Windows phones, in the lower-right corner, tap the grid or list icon to toggle between the two views.

**Manually Check for Pending Notifications**

Oracle Mobile Authenticator (OMA) app automatically checks for authentication requests, but you can also manually check for your pending notifications.

How to check for pending notifications depends on which view you are using in the OMA app:

1. While in List View, pull down on the account list to check for any pending notifications for all accounts in the list. If there is a pending notification, it automatically appears. Tap **Allow** or **Deny**.

2. While in Grid View, pull down on an account tile to check for pending notifications for that account. If there is a pending notification, it automatically appears. Tap **Allow** or **Deny**.

The number of notifications that require your attention also appear on the bell icon in the upper-right corner. Tap the bell icon to access the **Notification History** screen, tap a pending notification, and then tap **Allow** or **Deny**.

**Edit Accounts in the OMA App**

You can edit your accounts in the Oracle Mobile Authenticator (OMA) app. The steps to edit an account in the OMA app vary between the supported operating systems.

- **iOS**: While in List View, swipe left on the account tile that you want to edit. While in Grid View, swipe up. Tap **Edit**, make your changes in the **Edit Account** screen, and then tap **SAVE**.

  **Note:**

  To edit an account when using VoiceOver mode, you must be in Grid View. The Edit option isn’t available in List View when using VoiceOver mode.

- **Android**: While in List View, long tap the account that you want to edit. While in Grid View, tap the account, and then long tap it when it appears in detail view. Tap the pencil icon that appears in the upper-right corner, make your changes in the **Edit Account** screen, and then tap **SAVE**.

- **Windows**: Tap and hold the account tile that you want to edit. A menu appears. Tap **Edit** and make your changes in the **Edit Account** screen, and then tap **Save**.

**Sync an Account**

You can sync your accounts in the Oracle Mobile Authenticator (OMA) app. The steps to sync your accounts in the OMA app vary between the supported operating systems.

- **iOS**: While in List View, swipe left on the account tile that you want to sync. While in Grid View, swipe up. Tap **Edit** and in the Edit Account screen, tap **Sync**.
Account to update the account with the latest policies and to refresh the shared secret.

**Note:**

To edit an account when using VoiceOver mode, you must be in Grid View. The Edit option isn’t available in List View when using VoiceOver mode.

- **Android:** While in List View, long tap the account that you want to sync. While in Grid View, tap the account, and then long tap it when it appears in detail view. Tap the pencil icon that appears in the upper-right corner, and the in the Edit Account screen, tap **Sync Account** to update the account with the latest policies and to refresh the shared secret.

- **Windows:** Tap **Sync Account** to update the account with the latest policies and to refresh the shared secret. Tap **Edit** and in the Edit Account screen, tap **Sync Account** to update the account with the latest policies and to refresh the shared secret.

### Reorder Accounts in the OMA App

You can change the order in which you view accounts in the Oracle Mobile Authenticator (OMA) app.

The steps to reorder your accounts in the OMA app vary between the supported operating systems.

- **iOS:** While in List View, long tap the account to enter editing mode, and then hold the reorder icon on the right to drag. Tap **Done** when you finish. While in Grid View, long tap the account tile, and then drag (supported in iOS9 and up).

- **Android:** Tap and hold the account tile, and then drag it.

- **Windows:** While in List View, long tap the account tile. From the menu that appears, tap **Reorder**, and then drag.

### Delete an Account in the OMA App

You can delete accounts in the Oracle Mobile Authenticator (OMA) app.

The steps to delete an account in the OMA app vary between the supported operating systems.

- **iOS:** While in List View, swipe left on the account tile that you want to delete. While in Grid View, swipe up. Tap **Delete**.

**Note:**

To delete an account when using VoiceOver mode, you must be in Grid View. The Delete option is not available in List View when using VoiceOver mode.
- **Android**: Tap and hold the account tile that you want to delete, tap the trash can icon that appears in the upper-right corner, and then in the Delete Account window, tap **Delete Account**.
- **Windows**: Tap and hold the account tile that you want to delete. A menu appears. Tap **Delete**, and then tap **Delete Account** in the window that appears.

## Enable App Protection

Add an additional level of security to the Oracle Mobile Authenticator (OMA) app by using an app PIN, by using biometrics such as Touch ID or Fingerprint, and by using Screen Protection to protect the app.

App PIN protection requires a PIN to unlock the OMA app before you can generate a one-time passcode (OTP) or approve a notification. Biometric protection requires Touch ID or Fingerprint verification to unlock the App before you can generate an OTP or approve a notification. Screen Protection, enabled by default, prevents OMA App content from being captured by screen recording.

The OMA app doesn’t support biometrics using a Windows device, and Touch ID with the OMA app is only supported with iOS version 8 and higher.

1. **To enable an app PIN:**
   
   Your application may require you to set up a PIN when you enroll.
   
   a. Launch the OMA app, and then tap the menu icon in the upper-left corner.
   
   b. Tap **App Protection**.
   
   c. Tap to enable PIN or Touch ID protection for the OMA app.
   
   d. Enter your PIN at the prompt, enter it again to verify, and then tap **OK**. The next time that you access the OMA app, you are prompted to enter your PIN.

2. **To enable Biometrics:**
   
   When you initially enable Touch ID or Fingerprint, you are prompted to set your PIN if you haven’t. If you have set your PIN, you are prompted to enter your PIN first before enabling Touch ID or Fingerprint.
   
   a. Launch the OMA app, and then tap the menu icon in the upper-left corner.
   
   b. Tap **App Protection**.
   
   c. Tap to enable Touch ID protection for the OMA app.
   
   d. Enter your PIN at the prompt.
   
   e. Enter your PIN again to verify and tap **OK**.

   The next time that you open the App, you are prompted to use your fingerprint to gain access to the OMA app.

3. **To disable Screen Protection:**
   
   Screen Protection prevents OMA App content from being captured by screen recording (iOS only), AirPlay (iOS only), or Screen Mirroring and is enabled by default. Screen protection is available in iOS version 11 and higher.
   
   a. Launch the OMA app, and then tap the menu icon in the upper-left corner.
   
   b. Tap **App Protection**.
   
   c. Tap to disable Screen Protection for the App.
Change Your OMA App PIN

Change your PIN in the Oracle Mobile Authenticator (OMA) app.

1. Launch the OMA app, and then tap the menu icon in the upper-left corner.
2. Tap App Protection, and then tap Change PIN.
3. Enter the current PIN, the new PIN, confirm the new PIN, and then tap Done.

Disable OMA App PIN Protection

You can disable PIN protection for the Oracle Mobile Authenticator (OMA) app.

Your application may be configured to not allow you to disable PIN protection.

1. Launch the OMA app, and then tap the menu icon in the upper-left corner.
2. Tap App Protection and slide to disable PIN protection for the OMA app.
3. Enter your PIN and tap Done.

Manage Notification History in the OMA App

You can access and view details about your notification history in the Oracle Mobile Authenticator (OMA) app.

1. Launch the OMA app and tap the bell icon in the upper-right corner to launch the Notifications page. Alternatively, you can tap the menu icon in the upper-left corner and tap Notifications. The Notification History page displays all notifications for the account.

   For the iOS platform, pending notifications that are currently in the Notification center of your device don’t appear in the OMA app when you manually launch the OMA app.

2. The Pending tab displays notifications for login requests that require you to either allow or deny the request. Tap a notification to view login request details.

3. The History tab displays notifications for login requests that you've already addressed. To clear the history, tap Clear in the upper-right corner of the History tab and tap Clear again at the prompt.
Part III

Perform Identity Administration

Learn how to perform important administrative functions that you must do right away, and others that you will return to later.

Chapters

• Manage Oracle Identity Cloud Service Users
• Manage Oracle Identity Cloud Service Groups
• Manage Oracle Identity Cloud Service Applications
• Manage Oracle Identity Cloud Service Jobs
• Run Oracle Identity Cloud Service Reports
Manage Oracle Identity Cloud Service Users

This section describes how to manage Oracle Identity Cloud Service users. This includes but not limited to creating user accounts, assigning groups to user accounts, importing user accounts, and multiple factor authentication for user accounts.

Topics:

• Typical Workflow for Managing Oracle Identity Cloud Service Users
• Understand the User Life Cycle
• Understand Administrator Roles
• Create User Accounts
• View Details About User Accounts
• Edit Attribute Values for the User Account
• Assign Groups to the User Account
• Remove Groups from the User Account
• Assign Applications to the User Account
• Remove Applications from the User Account
• Activate User Accounts
• Deactivate User Accounts
• Import User Accounts
• Export User Accounts
• Generate Bypass Codes for User Accounts
• Reset Authentication Factors for User Accounts
• Unlock User Accounts
• Add or Remove a User Account from an Administrator Role
• Generate Personal Access Tokens
• Send Invitations to Users to Activate Their Accounts
• Reset Passwords for User Accounts
• Remove User Accounts
# Typical Workflow for Managing Oracle Identity Cloud Service Users

With the user management feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing user accounts.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the user life cycle.</td>
<td>You can learn about the process flow of how a user account is created, managed, and deleted in Oracle Identity Cloud Service.</td>
<td>Understand the User Life Cycle</td>
</tr>
<tr>
<td>Understand administrator roles.</td>
<td>You can learn about administrator roles that you can assign to Oracle Identity Cloud Service users.</td>
<td>Understand Administrator Roles</td>
</tr>
<tr>
<td>Create user accounts.</td>
<td>You can create user accounts using the Users page.</td>
<td>Create User Accounts</td>
</tr>
<tr>
<td>View details about user accounts.</td>
<td>You can view details about user accounts using the Users page.</td>
<td>View Details About User Accounts</td>
</tr>
<tr>
<td>Modify user accounts.</td>
<td>You can modify user accounts using the Users page.</td>
<td>Edit Attribute Values for the User Account, Assign Groups to the User Account, Remove Groups from the User Account, Assign Applications to the User Account, Remove Applications from the User Account</td>
</tr>
<tr>
<td>Activate and deactivate user accounts.</td>
<td>You can activate and deactivate user accounts using the Users page.</td>
<td>Activate User Accounts, Deactivate User Accounts</td>
</tr>
<tr>
<td>Import and export user accounts.</td>
<td>You can import and export user accounts using the Users page.</td>
<td>Import User Accounts, Export User Accounts</td>
</tr>
<tr>
<td>Generate bypass codes for user accounts.</td>
<td>You can generate bypass codes for user accounts using the Users page.</td>
<td>Generate Bypass Codes for User Accounts</td>
</tr>
<tr>
<td>Reset authentication factors for user accounts.</td>
<td>You can reset authentication factors for user accounts using the Users page.</td>
<td>Reset Authentication Factors for User Accounts</td>
</tr>
<tr>
<td>Unlock user accounts.</td>
<td>You can unlock user accounts using the Users page.</td>
<td>Unlock User Accounts</td>
</tr>
<tr>
<td>Delegate administrative responsibilities for user accounts.</td>
<td>You can delegate administrative responsibilities to user accounts using the Administrators page.</td>
<td>Add or Remove a User Account from an Administrator Role</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Generate personal access tokens.</td>
<td>Generate tokens that client applications can use to access an API or a resource application within a limited period of time.</td>
<td>Generate Personal Access Tokens</td>
</tr>
<tr>
<td>Send invitations to users to activate their accounts.</td>
<td>You can send invitations to users to activate their user accounts using the Users page.</td>
<td>Send Invitations to Users to Activate Their Accounts</td>
</tr>
<tr>
<td>Reset passwords for user accounts.</td>
<td>You can reset passwords for user accounts using the Users page.</td>
<td>Reset Passwords for User Accounts</td>
</tr>
<tr>
<td>Remove user accounts.</td>
<td>You can remove user accounts using the Users page.</td>
<td>Remove User Accounts</td>
</tr>
</tbody>
</table>

You can create, manage, and remove user accounts by:

- The Identity Cloud Service console
- SCIM-based APIs

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

# Understand the User Life Cycle

**User life cycle** is a term to describe the process flow of how a user account is created, managed, and deleted in Oracle Identity Cloud Service based on certain events or time factors.

A user account goes through various stages in the life cycle. The stages are non-existent, deactivated, activated, and deleted.
You can define business requirements for each transition of the user life cycle. Use the sample scenarios listed in the following table to establish the link between user life cycle transitions and business objectives.

<table>
<thead>
<tr>
<th>Current State</th>
<th>Operation</th>
<th>Sample Scenario</th>
<th>Process Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-existent</td>
<td>Create</td>
<td>Human resources (HR) enters user profile information for a new hire.</td>
<td>If the new hire's start date isn't a future date, then the user account is introduced into Oracle Identity Cloud Service with an <strong>Activated</strong> status. If the new hire's start date is a future date, then the user account is created in Oracle Identity Cloud Service, and is then deactivated.</td>
</tr>
<tr>
<td>Current State</td>
<td>Operation</td>
<td>Sample Scenario</td>
<td>Process Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Deactivated</td>
<td>Activate</td>
<td>The user’s start date is in effect.</td>
<td>The user account is activated in Oracle Identity Cloud Service, and the user can now log in and use this Oracle Cloud service. The user can access all groups, applications, and administration role privileges assigned to the user account.</td>
</tr>
<tr>
<td>Activated</td>
<td>Modify</td>
<td>The user is promoted to a new position. HR changes the job title of the user.</td>
<td>New groups, applications, and administration roles are assigned to the user account. Old irrelevant groups, applications, and administration roles are removed from the user account.</td>
</tr>
<tr>
<td>Activated</td>
<td>Deactivate</td>
<td>The user takes a one-year sabbatical from the company. HR manually deactivates the user account on the last working day of the user. The user rejoins the company after some period. HR activates the user account.</td>
<td>The user account is deactivated in Oracle Identity Cloud Service, and the user can no longer log in and use this Oracle Cloud service. The user account can be activated again.</td>
</tr>
<tr>
<td>Activated</td>
<td>Delete</td>
<td>The user retires from the company. HR manually deletes the user account on the last working day of the user.</td>
<td>The user account is removed from Oracle Identity Cloud Service. All groups, applications, and administration role privileges assigned to the user account are revoked as part of the workflow. If you remove (delete) the user, the audit data of the user remains in the system. To manually (and immediately) purge the audit data of the deleted user, see Purge Audit Data for the Deleted User.</td>
</tr>
</tbody>
</table>

The following concepts are integral to user lifecycle management:
• User Account: A user account represents a user in Oracle Identity Cloud Service, and enables the user to access the Oracle Cloud service to which they belong. In Oracle Identity Cloud Service, there is a one-to-one relationship between a user and a user account. By default, all users can use their accounts to perform self-service capabilities in Oracle Identity Cloud Service. Users can update their profiles, reset their passwords, unlock their accounts, and change their email preferences.

• Administrator Role: You may want to provide a user account with administrative capabilities in Oracle Identity Cloud Service. To do this, you assign administrator roles to user accounts. See Understand Administrator Roles.

• Group: Oracle Identity Cloud Service provides easy and controlled privilege management through groups. Groups are the links between user accounts and applications in Oracle Identity Cloud Service. Groups are designed to ease the administration of privileges that you grant to user accounts or other groups. See Manage Oracle Identity Cloud Service Groups.

• Application: Oracle applications are a complete and modular set of enterprise applications, engineered from the ground up to be cloud-ready and to coexist seamlessly in mixed environments.

You can use Oracle Identity Cloud Service to grant access to Oracle applications in two ways:

– Directly: Assigning users to the applications

– Indirectly: Assigning groups to the applications. Any users who are members of the groups are granted access to the applications.

In addition to granting users and groups access to Oracle applications, you can grant users and groups access to entitlements within applications. For example, you use Oracle Identity Cloud Service to grant John Doe and Jane Doe access to Oracle Java Cloud Service. You want John Doe to have administrator privileges for Oracle Java Cloud Service, but Jane Doe to have user privileges only.

Each entitlement in an Oracle application is represented by an application role. So by assigning John Doe to the application administrator role of Oracle Java Cloud Service, he can not only access this Oracle Cloud service, but he can also function as an administrator within it.

See Manage Oracle Identity Cloud Service Applications for more information about how you can use Oracle Identity Cloud Service to grant and revoke access rights for users and groups to applications and application roles.

**Understand Administrator Roles**

In the following topic, you learn about Oracle Identity Cloud Service administrator roles and the privileges associated with each role.

In your organization, you might want administrators to have different rights of access to various tasks and resources in Oracle Identity Cloud Service. For example, the identity domain administrator has superuser privileges for an Oracle Identity Cloud Service identity domain. This administrator may want to delegate some of their responsibilities to other users to carry out the tasks associated with these responsibilities, such as managing system configuration and security settings, applications, users, groups, group memberships, and so on. To do this, the administrator assigns these users to other Oracle Identity Cloud Service administrator
roles. Users who are assigned to these roles will be able to perform specific tasks that are associated with the roles.

The following table lists the Oracle Identity Cloud Service administrator roles that you can assign to users and describes the privileges for each administrator role. See Add or Remove a User Account from an Administrator Role.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity domain administrator</td>
<td>Has superuser privileges for an identity domain in Oracle Identity Cloud Service. Identity domain administrators can:</td>
</tr>
<tr>
<td></td>
<td>• Manage users, groups, applications, system configuration, and security settings</td>
</tr>
<tr>
<td></td>
<td>• Perform delegated administration by assigning users to different administrative roles</td>
</tr>
<tr>
<td></td>
<td>• Enable and disable Multi-Factor Authentication (MFA), configure MFA settings, and configure authentication factors</td>
</tr>
<tr>
<td></td>
<td>• Create self-registration profiles to manage different sets of users, approval policies, and applications</td>
</tr>
<tr>
<td>Security administrator</td>
<td>Manage Oracle Identity Cloud Service system configuration and security settings for an identity domain in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td></td>
<td>Security administrators can customize the interface, default settings, notifications, and the password policy, configure Multi-Factor Authentication (MFA), and manage the Microsoft Active Directory (AD) Bridge, Provisioning Bridge, identity providers, and trusted partner certificates.</td>
</tr>
<tr>
<td>Application administrator</td>
<td>Manage Oracle Identity Cloud Service applications. Application administrators can create, update, activate, deactivate, and delete applications. Application administrators can also grant and revoke access to applications for groups and users.</td>
</tr>
<tr>
<td>User administrator</td>
<td>Manage users, groups, and group memberships for an identity domain in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>User manager</td>
<td>Manage all users or users of selected groups in Oracle Identity Cloud Service. User managers can update, activate, deactivate, remove, and unlock user accounts. User managers can also reset passwords, reset authentication factors, and generate bypass codes for user accounts.</td>
</tr>
<tr>
<td>Audit administrator</td>
<td>Run reports for an identity domain in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>User</td>
<td>Perform self-service capabilities in Oracle Identity Cloud Service. Users can update their profiles, reset their passwords, change their email preferences, link their social accounts to Oracle Identity Cloud Service, request access to groups and applications, view their access requests, access groups and applications assigned to them, and enroll in Multi-Factor Authentication (MFA).</td>
</tr>
</tbody>
</table>

**Note:** By default, all Oracle Identity Cloud Service users are granted the User role. You can assign a user to the additional administrator roles that appear in this table.

**Note:**

See Typical Workflow for Using Oracle Identity Cloud Service to learn more about the tasks that users who belong to each administrator and user role can perform in Oracle Identity Cloud Service.
Create User Accounts

You can create user accounts only if you are granted access to the identity domain administrator or user administrator role in the Administrators page of the Identity Cloud Service console.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Users, and then click Add.

2. In the First Name and Last Name fields of the Add User window, enter the user’s first and last name.

3. To have the user log in to Oracle Identity Cloud Service with their email address:
   a. Leave the Use the email address as the user name check box selected.
   b. In the User Name / Email field, enter the email address for the user account.

   OR

4. To have the user log in to Oracle Identity Cloud Service with their user name:
   a. Clear the Use the email address as the user name check box.
   b. In the User Name field, enter the user name that the user is to use to log in to the Identity Cloud Service console.

   Note:
The value that you enter into the User Name field can be either a valid email address or a non-email string. If it's a non-email string, then the following characters are allowed:

   • a-z
   • A-Z
   • 0-9
   • Special characters !@#$%^&*()_+=-{}[]|:";'<>?,
   • White space

   c. In the Email field, enter the email address for the user account.

   Note:
If you turned off the Allow primary email address as optional switch in the User Settings page, then you must provide an email address in the Email field to create the user account.

If you turned this switch on, then you can create the account without entering an email address in the Email field.

5. To assign the user account to a group, click Next. Otherwise, click Finish.

6. In the Add User window, select the check box for each group that you want to assign to the user account. Click Finish.
View Details About User Accounts

With the Users page, you can see profile information for a user account, any groups or apps to which the account is assigned, and risk data collected for the account.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.

2. Click the user account about which you want to view additional information.

Tip:

To search for users, in the search field, enter all or part of the beginning of the user name, first name, or last name that you want to locate, and then press Enter. To fine-tune your search, click the search field again, and then select a status (Active, Inactive, or Locked).

3. Click Details to see additional profile information that you can edit, such as:

<table>
<thead>
<tr>
<th>Profile Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user's primary email address</td>
<td>This email address is the user's email address to which Oracle Identity Cloud Service will send notifications. See Understanding the Types of Notifications.</td>
</tr>
<tr>
<td>The user's password recovery email address</td>
<td>If the user forgets their password, then Oracle Identity Cloud Service will send notifications to this email address.</td>
</tr>
<tr>
<td>If the user account is a federated single sign-on (SSO) account</td>
<td>With a federated account, a user can interact with Oracle Identity Cloud Service through an identity provider, using a website that's external to Oracle Identity Cloud Service. See Adding an Identity Provider.</td>
</tr>
<tr>
<td>The user's country, time zone, and preferred language</td>
<td>If these attribute values for the user are different from attribute values that you set for the identity domain, then you can modify them. See Set Up or Modify Your Profile.</td>
</tr>
</tbody>
</table>

4. Click Groups to see a list of any groups assigned to the user account.

You can assign groups to the user account or remove groups from the user account.

5. Click Access to see a list of any applications assigned to the user account.

You can assign applications to the user account or remove applications from the user account.

Note:

The Active icon for each application on the Access tab represents the active status of the user account and not the application status. The status remains active as long as the user account is active, regardless of whether the application is active or inactive.
6. Click **Security** to see risk data collected for the user, including whether the user is enrolled in Multi-Factor Authentication (MFA).

---

**Note:**

If you don't see the **Security** tab, then activate Adaptive Security or at least one risk provider. See [Activate Adaptive Security](#) and [Activate a Risk Provider](#). Also, see [Understand Risk Providers](#) to learn more about risk ranges, risk providers, and risk scores associated with user accounts because you must be familiar with these concepts to understand the panes of the **Security** tab.

---

7. In the **User Risk Scores** pane, click the default risk provider to view the risk incidents and details associated with this risk provider for the user account.

---

**Note:**

If you don't see the default risk provider, then activate it. See [Activate a Risk Provider](#).

---

Two panes appear below the default risk provider: **Risk Incidents** and **Details**.

- The **Risk Incidents** pane displays a graph that illustrates user-threat risk scores and risk scores after remediation for a selected time interval. The risk scores are displayed as per the risk score ranges.

- The **Details** pane displays incidents associated with actions that a user is performing in Oracle Identity Cloud Service.

There are three incidents (or events) that Oracle Identity Cloud Service uses to lower the risk score of the user:

- **Time-based risk-score re-evaluation**: The user's risk score has been lowered because Oracle Identity Cloud Service detected that the user hasn't committed risky activity over a period of time. The score is reduced periodically as long as there are no threat events.

- **Successful user password reset**: The user reset their Oracle Identity Cloud Service password.

- **Successful user login**: The user signed in to Oracle Identity Cloud Service.

---

**Note:**

If the default risk provider is deactivated, then the user's risk score won't be lowered.

---

The following risky actions (or threats) are monitored by Oracle Identity Cloud Service:

- **Access from an unfamiliar location**: The user accessed Oracle Identity Cloud Service from a location that hasn’t been previously used to access
the service, and which exceeds the distance specified between the user’s current access location and the user’s previous access location.

– **Access from an unknown device:** The user accessed Oracle Identity Cloud Service from a device that hasn't been previously used to access the service.

– **Access from suspicious IP addresses:** The IP address from where the user is accessing Oracle Identity Cloud Service is flagged as suspicious by the integrated IP reputation provider.
Tip:

Expand the **Access from suspicious IP addresses** event and click the **Information** icon to the right of the IP address to see why the integrated IP reputation provider blacklisted it. Reasons include:

* Spam Sources: The IP address is tunnelling spam messages through proxy, anomalous SMTP activities, or forum spam activities.
* Windows Exploits: The IP address is offering or distributing malware, shell code, rootkits, worms, or viruses.
* Web Attacks: The IP address is involved in attacks such as cross-site scripting, iFrame injection, SQL injection, cross-domain injection, or domain password brute force.
* Botnets: The IP address is seen in Botnet C&C channels and infected zombie machines are controlled by the bot master.
* Scanners: The IP address is seen in reconnaissance such as probes, host scans, domain scans, and password brute force.
* Denial of Service: The IP address is noticed in DOS, DDOS, anomalous SYN flood, and anomalous traffic detection.
* Phishing: The IP address is hosting phishing sites and other kinds of fraud activities such as Ad Click Fraud or Gaming Fraud.
* Proxy: The IP address is providing proxy and anonymization services. This also includes TOR anonymizer IP addresses.
* Mobile Threats: The IP address is associated with malicious and unwanted mobile applications.
* Package: This IP address is associated with information about all other reasons.
* TOR Proxy: The IP address acts as an exit node for the TOR Network. The exit node is at the last point along the proxy chain and makes a direct connection to the originator’s intended destination.
* Reputation: This IP address is associated with other IP addresses (for example, through common ownership, having the same subnet, and so on). This IP address is classified as high risk because of documented threat activity.

- **Impossible travel between locations:** Oracle Identity Cloud Service obtained the user’s current access location, using the IP address, calculated the distance between this location and the user’s immediately preceding access location, and determined that this distance cannot be covered at the speed specified in the threshold.

- **Too many unsuccessful login attempts:** The user exceeded the number of unsuccessful login attempts into Oracle Identity Cloud Service.
allowed, based on the value specified for the Account lock threshold attribute of the password policy. See Modify the Custom Password Policy.

– **Too many unsuccessful MFA attempts:** The user exceeded the number of unsuccessful login attempts into Oracle Identity Cloud Service allowed, based on the value specified for the Max Unsuccessful MFA attempts attribute of MFA. See Configure Multi-Factor Authentication Settings.

**Note:**
If the default risk provider is deactivated, then the user’s risk score won’t be increased.

8. In the **Risk Incidents** pane, filter the data that appears in this graph by completing one of the following options:

   a. To view risk score ranges that represent user-threat risk scores and risk scores after remediation for the current day, week, or month, or since the user signed in to Oracle Identity Cloud Service for the first time, from the drop-down menu, select **1 Day, 1 Week, 1 Month**, or **All**.

   b. To specify a custom date-and-time range to view risk-related user activity for the user account, click the left **Calendar** icon to specify the start date and time, and the right **Calendar** icon to set the end date and time.

9. In the **Details** pane, click an incident (either a threat or an event) to learn more about it.

### Edit Attribute Values for the User Account

After viewing details about a user account, you can modify the account by editing attribute values for the user account.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.

2. Click the user account that you want to modify.

3. Click **Details**.

4. Modify an attribute value for the user account by:

   a. Entering a value in the attribute field (for example, the **City** field).

   b. Turning on or off a switch (for example, the **Federated** switch).

   c. Selecting a value from the drop-down list (for example, a Microsoft Active Directory (AD) domain from the **Authenticated By** list).

**Important:**
You can't edit attribute values for your user account. To do this, access the **My Profile Details** tab of the My Profile console. See Set Up or Modify Your Profile.
A new feature of Oracle Identity Cloud Service is delegated authentication. Delegated authentication allows identity domain administrators and security administrators to specify whether users can use their Oracle Identity Cloud Service or AD passwords to sign in to Oracle Identity Cloud Service to access resources protected by Oracle Identity Cloud Service, such as the My Profile console, Identity Cloud Service console, and apps assigned to the user.

For example, suppose you configured delegated authentication for an AD Bridge in Oracle Identity Cloud Service so that a user can use their AD password to authenticate into Oracle Identity Cloud Service. Or, perhaps the user’s account can be synchronized between AD and Oracle Identity Cloud Service from more than one bridge.

From the **Authenticated By** list, you can select which AD domain contains the user’s credentials to sign in to Oracle Identity Cloud Service. Or, select **Oracle Identity Cloud Service** to have the user sign in with their Oracle Identity Cloud Service password.

If you don’t see a value in the **Authenticated By** list, click **View Authentication Source**. If you configured delegated authentication for this user account, then the AD Bridge associated with the user’s AD domain appears. Otherwise, **Oracle Identity Cloud Service** is displayed.

After editing attribute values for the user account, click **Update User**.

### Assign Groups to the User Account

After viewing details about a user account, you can modify the account by assigning groups to the user account.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.
2. Click the user account that you want to modify.
3. Click **Groups**.
4. Click **Assign**. To search for groups to assign to the user account, in the search field, enter all or part of the beginning of the group names or descriptions that you want to locate, and then press **Enter**.
5. In the **Assign Groups** window, select the check box for each group that you want to assign to the user account.
6. Click **OK**.
Remove Groups from the User Account

After viewing details about a user account, you can modify the account by removing groups from the user account.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.
2. Click the user account that you want to modify.
3. Click **Groups**.

**Tip:**

To search for groups to remove from the user account, in the search field, enter all or part of the beginning of the group names or descriptions that you want to locate, and then press **Enter**.

4. Select the check box for each group that you want to remove from the user account.
5. Click **Revoke**.
6. In the **Confirmation** window, click **OK**.

Assign Applications to the User Account

After viewing details about a user account, you can modify the account by assigning applications to it.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.
2. Click the user account that you want to modify.
3. Click **Access**.
4. Click **Assign**.
5. In the **Assign Applications** window, click **Assign** for each application that you want to assign to the user account.

**Note:**

The Active icon for each application on the Access tab represents the active status of the user account and not the application status. The status remains active as long as the user account is active, regardless of whether the application is active or inactive.

6. Click **OK**.
Remove Applications from the User Account

After viewing details about a user account, you can modify the account by removing applications from it.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Click the user account that you want to modify.
3. Click Access.
4. Select the check box for each application that you want to remove from the user account.
5. Click Revoke.
6. In the Confirmation window, click OK.

Activate User Accounts

Activating a user account reinstates the access rights of the user account for Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Select the check box for each deactivated user account that you want to activate, or to activate all deactivated user accounts, search for accounts with a status of Inactive. Then, select the Select All check box.
3. Click Activate.
4. In the Confirmation window, click OK.
Deactivate User Accounts

Deactivating a user account temporarily disables the access rights that the user account has to Oracle Identity Cloud Service.

Deactivated users are not be able to login until you reactivate the user account. Group memberships and application roles remain intact and are available once the user account is reactivated.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Select the check box for each activated user account that you want to deactivate.

   Tip:
   To deactivate all activated user accounts, search for accounts with a status of Active. Then, select the Select All check box.

3. Click Deactivate.
4. In the Confirmation window, click OK.

Import User Accounts

If you are an identity domain administrator or a user administrator, you can batch import user accounts using a comma-separated values (CSV) file.

Before you can import user accounts, first create a CSV file that is properly formatted for the import process. To create and prepare a file for import, follow these steps.

1. Use these sample files as a starting point.
2. Extract the compressed file and then open the Users.csv file.
3. Review and then delete any demo data in the Users.csv file.

   Tip:
   To familiarize yourself with the import process, consider importing just the demo data. You can then delete the unwanted demo data from Oracle Identity Cloud Service before you begin importing production data.

4. Create an import file using the Users.csv file. The Users.csv file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table.

   Note:
   The maximum number of rows in the user import file must not exceed 100,000 and the import file size must not exceed 52 MB.
At a minimum, the file must have these exact column headings and the fields in these columns must be unique.

- User ID
- Last Name
- First Name
- Work Email

For each account, you create a new row (line) and enter data into each column (field). Each row equals one record.

The IDs of the users that you want to import into Oracle Identity Cloud Service must contain at least three characters. The names of the groups that you want to import into Oracle Identity Cloud Service must contain at least five characters.

The telephone numbers of the users that you want to import must meet the requirements of the RFC 3966 specification.

When importing users, the attribute Recovery cannot be specified as one of valid values for Primary Email Type. The valid values for Primary Email Type are home, work, or other.

If you are uploading a CSV file with modified email addresses, make sure to include the Primary Email Type attribute in the template's header to trigger the change. For each user with a modified email address, add an appropriate value (either home, work, or other) in the Primary Email Type column.

To create a CSV file, you can use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.

5. Save your file in a CSV format.
   a. Open the CSV file with a text editor, such as Notepad.
   b. Save the file with UTF-8 for encoding.

   **Note:**
   If you do not save the file in a CSV format with UTF-8 encoding, the import fails. Saving the file in UTF-8 format ensures that non-English characters display properly.

To import user accounts:

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Click Import.
3. In the Import Users dialog box, click Browse to locate and select the CSV file that contains the user accounts to import.

   **Note:**
   Click Download sample file in the dialog box to download a sample file.
4. Verify that the path and name of the CSV file that you selected appear in the Select a file to import field.

5. Click Import.

   If a user account is missing a required value, such as the user’s first name, last name, or user name, then Oracle Identity Cloud Service can’t import it. If Oracle Identity Cloud Service can’t import a user account, then it evaluates the next account in the CSV file.

6. After Oracle Identity Cloud Service evaluates all user accounts, review the job results.

   • If the job can be processed immediately, then a dialog box appears with the Job ID link for your import job. Click the link and review the details that appear on the Jobs page.

   • If the job cannot be processed immediately, then a message appears with a Schedule ID in it. Copy that Schedule ID, and use it to search for the job on the Jobs page. The job will appear when processing completes. Go to Step 7.

   **Tip:**

   Oracle Identity Cloud Service assigns a job ID to each file that’s imported or exported, for auditing purposes.

7. On the Jobs page, locate the job that you want to view, and then click View Details.

   A table displays the first names, last names, email addresses, user names, and statuses of the user accounts that you imported into Oracle Identity Cloud Service.

   **Note:**

   If a user account can be imported into Oracle Identity Cloud Service, then a Creation Succeeded or Update Succeeded link appears for the status, depending on whether you imported a new account or modification to an existing account. To see granular details about the account, click the link.

   If a user account can’t be imported, then a Creation Failed or Update Failed link appears for the status. To see information about why the account or modification can’t be imported into Oracle Identity Cloud Service, click the link.

8. Review the details that appear on the Jobs page.

   This page shows how many accounts you imported, how many accounts imported successfully, and how many accounts can’t be imported because of a system error.

---

# Export User Accounts

Using the Oracle Identity Cloud Service admin console, you can export the user accounts for the following attributes only: User Name, Work Email, Home Email,
Primary Email Type, Honorific Prefix, First Name, Middle Name, Last Name, and Honorific Suffix.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.

2. To export all user accounts, click Export, and then select Export All.

   OR

   To export only some user accounts, select the check box for each user account that you want to export. Click Export, and then select Export Selected.

   Tip:

   The number that appears within parentheses to the right of Export All is how many user accounts are created in Oracle Identity Cloud Service. The number within parentheses to the right of Export Selected is how many user accounts you selected to export.

3. In the Confirmation window, click OK.

4. After Oracle Identity Cloud Service creates the export file, you need to review the results.

   • If the job can be processed immediately, then a dialog box appears with the Job ID link for your import job. Click the link and review the details that appear on the Jobs page.

   • If the job cannot be processed immediately, then a message appears with a Schedule ID in it. Copy that Schedule ID, and use it to search for the job on the Jobs page. The job will appear when processing completes.

5. On the Jobs page, locate the job that you want to view, and then click View Details.

   A page shows how many user accounts you exported, how many accounts Oracle Identity Cloud Service exported successfully, and how many accounts can't be exported because of a system error.

6. Click Download.

7. Save your file in a UTF-8 format. Saving the file in UTF-8 format ensures that non-English characters display properly.

8. (Optional) In addition to saving the file in UTF-8 format, if you are using Microsoft Excel to open and save the file, perform the additional steps to ensure that non-English characters display properly.

   a. In Microsoft Excel, open a new workbook, click the Data tab, and then choose From Text.

   b. On the Import Text File window, choose your CSV file, and then click Import.

   c. For Original data type, select Delimited, for File origin, select 65001: Unicode (UTF-8), and then click Next.

   d. For Delimiters, select Comma, deselect all other options, and then click Next.

   e. For Column data format, select General, and then click Finish.

   f. Click OK.
g. Save the file.

Generate Bypass Codes for User Accounts

You can increase security for user accounts by using Multi-Factor Authentication (MFA) capabilities provided by Oracle Identity Cloud Service. MFA adds an extra layer of identity verification to the login process by requiring a user to provide a second verification method, such as a one-time passcode (OTP) for the device associated with the user’s account, notification, short message service (SMS), also known as a text message, or security questions.

The ability to generate a bypass code is available to the user after the user enrolls in 2-Step Verification. The user can generate a bypass code and store it for later use or request that an administrator generate a bypass code for the user. For example, when a user has forgotten their phone, doesn't have cell service, or can't access their computer, at the 2-Step Verification page, the user can contact the help desk to have an administrator generate a bypass code.

As a result, the user can use this bypass code as a one-time 2-Step Verification method to log in to Oracle Identity Cloud Service.

In addition, the administrator can set when the bypass code expires, and how often the bypass code can be used for the user account.

Note:
The user must already be enrolled in MFA to use a bypass code or request that one be generated for the user.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Click the user account for which you want to generate a bypass code.
3. Click the Action menu, and then select Generate Bypass Code.
4. In the Bypass Code expires after region of the Generate Bypass Code window, set when the bypass code expires.
   a. Set the time (in days, hours, and minutes) that the bypass code will expire. After this time elapses, the user can't use the bypass code.
   b. If you don't want the bypass code to expire, then click Never Expires.
5. In the Bypass Code can be used region of the Generate Bypass Code window, specify how often the bypass code can be used.
   a. If the bypass code can be used only one time, then click Once.
   b. If the bypass code can be used for a finite number of times, then click the button to the left of the text box. Enter a number in the text box that represents how many times the bypass code can be used.
   c. If the bypass code can be used for an unlimited number of times, then click Unlimited.
6. Click OK.
7. In the **Bypass Code** window, click **Email**. A notification is sent to the user. This notification contains the bypass code that the user uses as a one-time 2-Step Verification method to log in to Oracle Identity Cloud Service.

### Reset Authentication Factors for User Accounts

Reset all verification factors for users enrolled in Multi-Factor Authentication (MFA) if a user’s device can't be used to provide a second factor for authentication. Resetting all verification factors removes any existing factors in which the user is enrolled.

Resetting all verification factors removes any existing factors in which the user is enrolled. The next time the user logs in, the user is prompted to enroll in 2–Step Verification and account recovery.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.
2. Click the user account for which you want to reset authentication factors.
3. Click the **Action** menu, and then select **Reset Factors**.
4. In the **Confirmation** window, click **OK**.

### Unlock User Accounts

After a consecutive number of unsuccessful login attempts to Oracle Identity Cloud Service, a user account is locked. The user receives a notification that contains a link that the user can click to reset their password and unlock their account. An administrator can unlock accounts without requiring a password reset.

If a user's account is locked, and the user or an administrator doesn't unlock the account, then Oracle Identity Cloud Service will unlock it automatically. An administrator can set this time period ranging between 5 minutes and 24 hours. See **Modify the Custom Password Policy**.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.
2. Click the user account that you want to unlock.
3. Click the **Action** menu, and then select **Unlock User**.
4. In the **Confirmation** window, click **OK**.

**Tip:**

To display all user accounts that are locked, click the search field and select the **Locked** status.
Add or Remove a User Account from an Administrator Role

After you create or import user accounts in Oracle Identity Cloud Service, you can delegate administrative responsibilities for these accounts.

By default, all users can perform self-service capabilities in Oracle Identity Cloud Service, such as updating their profiles, resetting their passwords, and changing their email preferences. You may want to provide a user account with administrative capabilities. For example, you may want a user to manage applications in Oracle Identity Cloud Service. So, you would assign the user account to the application administrator role.

A user account can be assigned to more than one administrator role. The user account inherits the privileges for each administrator role assigned to the account. If a user account is assigned to both the application administrator role and the user administrator role, then the user can manage applications, users, groups, and group memberships in Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Administrators.

2. Expand the node for the administrator role for which you want to add or remove a user account, and then perform one of the following:

   - To add a user account to an administrator role, click Add, select the check box for each user account that you want to add, and then click OK.
     
     If you're adding users to the user manager role, then after selecting the check box for each user that you're adding to this role, you must also select one of the following options:
     
     - **Manage all users**: These users can manage all users in the Oracle Identity Cloud Service identity domain.
     
     - **Manage selected groups of users**: These users can manage only those users who belong to the groups that you select. After selecting this option, enter or select the groups to be managed by these users.

     After making this selection, click OK. If you want to modify either the users who are assigned to the user manager role or the groups that these users can manage, then click the Action menu , and select Edit from the drop-down menu that appears.

   - To remove a user account from an administrator role, select the user account that you want to remove, click Remove, and then in the Confirmation window, click OK.

Generate Personal Access Tokens

An access token is an authorization that's used by a client application to access an API or a resource application within a limited period of time.

The time-bound access tokens inform the resource application that the client is authorized to access the application and perform specific actions specified by the scope that's granted.
You can download access tokens only if an identity domain administrator assigns administrator roles or resource applications to your user account.

To generate personal access tokens:

1. Access Oracle Identity Cloud Service console, click the avatar icon on the top-right corner, and then click **My Access Tokens**.

2. You can download an access token in the following ways:
   - Select **Invokes Identity Cloud Service APIs** to specify the available administrator roles that are assigned to you. The APIs from the specified administrator roles will be included in the token.
   - Select **Invokes other APIs** to select confidential applications that are assigned to the user account.
     a. Click **Select an Application** to add a configured confidential resource application. On the **Select an Application** window, the list of assigned confidential applications displays.
     b. Click applications to select them, and then click **Add**. The **My Access Tokens** page lists the added applications.

3. In the **Token Expires in (Mins)** field, select or enter how long (in minutes) the access token you’re generating can be used before it expires. You can choose to keep the default number or specify between 1 and 527,040.

4. Click **Download Token**. The access token is generated and downloaded to your local machine as a **tokens.tok** file.

---

**Send Invitations to Users to Activate Their Accounts**

After a user account is created in Oracle Identity Cloud Service, a Welcome invitation is sent to the user, requesting that the user activate the account. The new user account must be activated before it can be used.

If the user account isn't activated after a designated amount of time, then the Oracle Identity Cloud Service administrator can send another invitation to the user to activate the account.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.

2. Select the check box for each user account to which you want to send an invitation.

   **Tip:**

   To send invitations to all user accounts, select the **Select All** check box.

3. Click **More**, and then select **Resend Invitation**.

4. In the **Confirmation** window, click **OK**.
Reset Passwords for User Accounts

You can use Oracle Identity Cloud Service to reset the password for a user account. When you request a password change, Oracle Identity Cloud Service sends a notification to the user so that the user can provide a new password for the account.

You can reset a password for a single account, for multiple accounts, or for all accounts in the identity domain.

You can't reset the passwords for deactivated user accounts. To activate all deactivated user accounts, search for accounts with a status of Inactive. Then select the Select All check box.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Select the check box for each user account for which you want to reset the password.

Tip:
To reset the passwords for all user accounts, do not select any check boxes, and go to Step 3.

3. Click More, and then perform one of the following choices.
   - If you selected either a single or multiple user accounts:
     a. Select Reset Password.
     b. In the Confirmation window, click OK.
   - If you didn’t select any user accounts (because you want to reset the passwords for all accounts):
     a. Select Reset All Passwords.
     b. In the Confirmation window, click OK.

Remove User Accounts

You can remove user accounts who no longer need access to the service. You can remove either a single user account or multiple accounts.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Select the check box for each user account that you want to remove.
3. Click More, and then click Remove.
4. In the Confirmation window, click OK.
Note:

If you remove (delete) a user, the audit data of the user remains in the system.
Manage Oracle Identity Cloud Service Groups

Learn how to manage Oracle Identity Cloud Service groups.

Topics

• Typical Workflow for Managing Oracle Identity Cloud Service Groups
• Understand Groups
• Create Groups
• View Details About Groups
• Edit Attribute Values for the Group
• Assign User Accounts to the Group
• Remove User Accounts from the Group
• Assign Applications to the Group
• Remove Applications from the Group
• Import Groups
• Export Groups
• Remove Groups

Typical Workflow for Managing Oracle Identity Cloud Service Groups

With the group management feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing groups.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand groups.</td>
<td>Learn about groups, including how groups are used to link user accounts to applications in Oracle Identity Cloud Service.</td>
<td>Understand Groups</td>
</tr>
<tr>
<td>Create groups.</td>
<td>Create new groups using the Groups page.</td>
<td>Create Groups</td>
</tr>
<tr>
<td>View details about groups.</td>
<td>View details about groups using the Groups page.</td>
<td>View Details About Groups</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Modify groups.</td>
<td>Modify groups using the Groups page.</td>
<td>Edit Attribute Values for the Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign User Accounts to the Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove User Accounts from the Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign Applications to the Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove Applications from the Group</td>
</tr>
<tr>
<td>Import and export groups.</td>
<td>Import and export groups using the Groups page.</td>
<td>Import Groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Export Groups</td>
</tr>
<tr>
<td>Remove groups.</td>
<td>Remove groups using the Groups page.</td>
<td>Remove Groups</td>
</tr>
</tbody>
</table>

You can create, manage, and remove groups by using:

- The Identity Cloud Service console
- SCIM-based APIs

In this section, you learn how to create, manage, and remove groups by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

### Understand Groups

As an identity domain administrator or user administrator, you use Oracle Identity Cloud Service groups to manage the accounts of users to whom you want to grant access to Oracle applications or application roles.

In Oracle Identity Cloud Service, groups are the links between user accounts and applications. They contain privileges that you grant to users. Groups ease the administration of user privileges.

Using groups, you can:

- Designate the applications and application roles that users can access through the Identity Cloud Service console
- Assign users to the groups
- Designate other Oracle Identity Cloud Service administrators to perform actions on groups:
  - Assigning or removing members to or from the current group
  - Modifying other characteristics of the group, such as the group description
Note:

The **All Tenant Users** group is a group that's created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. If you assign this group to any of your applications, then all users are assigned to these applications indirectly.

For a user, the **All Tenant Users** group doesn't appear in the **Groups** tab because this group is assigned automatically when a new user is created. Also, because this group is created by Oracle Identity Cloud Service, and not by an administrator, you can't delete this group.

---

**Create Groups**

You can create groups in Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Groups**.
2. Click **Add**.
3. In the **Name** and **Description** fields of the **Add Group** window, enter the name and descriptive information about the group.
4. To allow users to request access to this group, click **User can request access**.
5. To assign user accounts to the group, go to step 6. Otherwise, click **Finish**.
6. Click **Next**.
7. Select the check box for each user account that you want to assign to the group, and then click **Finish**.

**Tip:**

To search for user accounts to assign to the group, in the search field, enter all or part of the beginning of the user names, first names, or last names of the user accounts that you want to locate, and then press **Enter**.

---

**View Details About Groups**

By default, in the **Groups** page, you can see the name and description for each group.

You can also see other information about a group, such as any user accounts assigned to the group.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Groups**.
2. Click the group about which you want to view additional information.
Tip:
To search for groups, enter all or part of the beginning of the group name that you want to locate in the Search Groups field, and then press Enter.

3. Click Details.
   In this tab, you see information about the group, including the name and description of the group, and whether users can request access to this group. You can edit attribute values for the group.

4. Click Users.
   In this tab, you see a list of user accounts assigned to the group. You can assign user accounts to the group or remove user accounts from the group.

5. Click Access.
   In this tab, you see a list of any applications assigned to the group. You can assign applications to the group or remove applications from the group.

**Edit Attribute Values for the Group**

You can modify a group by editing attribute values for the group.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click the group that you want to modify.
3. Click Details.
4. Enter or select the modification in the attribute field (for example, modify the group name in the Name field or select the User can request access check box).
5. Click Update.

**Assign User Accounts to the Group**

You can modify a group by assigning user accounts to the group.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click the group that you want to modify.
3. Click Users.
4. Click Assign.

Tip:
To search for user accounts to assign to the group, in the search field, enter all or part of the beginning of the user names, first names, or last names of the user accounts that you want to locate, and then press Enter.
5. In the Assign Users window, select the check boxes for the user accounts that you want to assign to the group.

6. Click OK.

Remove User Accounts from the Group

You can modify a group by removing user accounts from the group.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click the group that you want to modify.
3. Click Users.
4. Select the check box for each user account that you want to remove from the group.

Tip:
To search for user accounts to remove from the group, in the search field, enter all or part of the beginning of the user names, first names, or last names of the user accounts that you want to locate, and then press Enter.

5. Click Revoke.
6. In the Confirmation window, click OK.

Assign Applications to the Group

You can modify a group by assigning applications to the group.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click the group that you want to modify.
3. Click Access.
4. Click Assign.
5. In the Assign Applications window, click Assign for each application that you want to assign to the group.

Note:
If you’re assigning a managed application to the group, then a form appears for the application. Populate the fields of the form, and then click Save.

See Architecture Diagram Defining Oracle Identity Cloud Service and Provisioning Integration for more information about managed applications and application forms.
6. (Optional) To assign an application to all users, search for and click the All Tenant Users group, and then click Access. Click Assign, search for the application, and assign it to the group.

7. Click OK.

Note:
If you assigned a managed application to the group, then you can modify the values of the application form. To do this, click the Action menu, select Edit, change the appropriate values, and then click Save.

Remove Applications from the Group

You can modify a group by removing applications from the group.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click the group that you want to modify.
3. Click Access.
4. Select the check box for each application that you want to remove from the group.
5. Click Revoke.
6. In the Confirmation window, click OK.

Import Groups

If you are an identity domain administrator or a user administrator, you can batch import groups using a comma-separated values (CSV) file.

Before you can import groups, first create a CSV file that is properly formatted for the import process. To create and prepare a file for import, follow these steps.

1. Use these sample files as a starting point.
2. Extract the compressed file and then open the Groups.csv file.
3. Review and then delete any demo data in the Groups.csv file.

Tip:
To familiarize yourself with the import process, consider importing just the demo data. You can then delete the unwanted demo data from Oracle Identity Cloud Service before you begin importing live data.

4. Create an import file using the Groups.csv file. The Groups.csv file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table. At a minimum, the file must have these exact column headings.
   - Display Name
For each account, you create a new row (line) and enter data into each column (field). Each row equals one record.

**Important:**

The IDs of the users that you want to import into Oracle Identity Cloud Service must contain at least three characters. The names of the groups that you want to import into Oracle Identity Cloud Service must contain at least five characters.

The telephone numbers of the users that you want to import must meet the requirements of the RFC 3966 specification.

The maximum number of rows in group import file must not exceed 100,000 and the import file size must not exceed 52 MB.

To create a CSV file, you can use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.

5. Save your file in a CSV format.
   a. Open the CSV file with a text editor, such as Notepad.
   b. Save the file with UTF-8 for encoding. Saving the file in UTF-8 format ensures that non-English characters display properly.

**Note:**

If you do not save the file in a CSV format with UTF-8 encoding, the import fails.

To import groups:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Groups**.
2. Click **Import**.
3. In the **Import Groups** window, click **Browse** to locate and select the CSV file that contains the groups to import.
4. Verify that the path and name of the CSV file that you selected appear in the Select a file to import field.

5. Click Import.

The reasons for Oracle Identity Cloud Service not being able to import a group are that the group already exists or the group is missing a required value, such as the group name. If Oracle Identity Cloud Service can't import a group, then it evaluates the next group in the CSV file.

6. After Oracle Identity Cloud Service evaluates all groups, review the job results.
   - If the job can be processed immediately, then a dialog box appears with the Job ID link for your import job. Click the link and review the details that appear on the Jobs page.
   - If the job cannot be processed immediately, then a message appears with a Schedule ID in it. Copy that Schedule ID, and use it to search for the job on the Jobs page. The job will appear when processing completes. Go to Step 7.

7. On the Jobs page, locate the job that you want to view, and then click View Details.

   The Job Details page shows how many groups you imported, how many groups imported successfully, and how many groups can't be imported because of a system error. For each group that you imported successfully, this page also shows how many user accounts are assigned to the group.

8. To see more information about a group, click View Details.

   Note: If the group can be imported into Oracle Identity Cloud Service or the user accounts can be assigned to the group, then a Creation Succeeded or Update Succeeded link appears for the status, depending on whether you imported a new group or modification to an existing group or group membership. To see granular details about the group, click the link.

   If a group can't be imported, then a Creation Failed or Update Failed link appears for the status. To see information about why the group or modification can't be imported into Oracle Identity Cloud Service, click the link.
Export Groups

You can export groups from Oracle Identity Cloud Service in order to import groups into another identity domain.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click Export, and then select Export All to export all groups.
   OR
   To export only some groups, select the check box for each group that you want to export. Click Export, and then select Export Selected.

   Tip:
   The number that appears within parentheses to the right of the Export All menu item is the total number of groups in Oracle Identity Cloud Service. The number within parentheses to the right of the Export Selected menu item is how many groups you selected to export.

3. In the Confirmation window, click OK.
4. After Oracle Identity Cloud Service creates the export file, a Job ID link appears. Click the link.
5. In the Jobs page, review the job details such as how many groups you exported, how many groups Oracle Identity Cloud Service exported successfully, and how many groups can't be exported because of a system error.
6. Click View Details, and then click Download.
7. Save your file in a UTF-8 format. Saving the file in UTF-8 format ensures that non-English characters display properly.
8. (Optional) In addition to saving the file in UTF-8 format, if you're using Microsoft Excel to open and save the file, then perform the additional steps to ensure that non-English characters display properly.
   a. In Microsoft Excel, open a new workbook, click the Data tab, and then choose From Text.
   b. On the Import Text File window, choose your CSV file, and then click Import.
   c. For Original data type, select Delimited, for File origin, select 65001: Unicode (UTF-8), and then click Next.
   d. For Delimiters, select Comma, deselect all other options, and then click Next.
   e. For Column data format, select General, and then click Finish.
   f. Click OK.
   g. Save the file.

Remove Groups

You can remove unused groups from Oracle Identity Cloud Service.
1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Groups**.

2. Select the check box for each group that you want to remove, or to remove all groups, select the **Select All** check box.

3. Click **Remove**.

4. In the **Confirmation** window, click **OK**.
Manage Oracle Identity Cloud Service Applications

Learn how to manage applications for Oracle Identity Cloud Service.

Topics:

- Typical Workflow for Managing Oracle Identity Cloud Service Applications
- Understand Cloud Applications
- Architecture: SAML and Provisioning Integration with Oracle Identity Cloud Service
- Use Case: Adding Applications
- About Adding Applications
- View Details About Applications
- About Modifying Applications
- Activate Applications
- Deactivate Applications
- Remove Applications

Typical Workflow for Managing Oracle Identity Cloud Service Applications

With the application management feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing applications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand cloud applications.</td>
<td>You can learn about cloud applications, including the two types of applications you can manage in Oracle Identity Cloud Service: Oracle applications and custom applications. You can learn about cloud applications, including the two types of applications you can manage in Oracle Identity Cloud Service: Oracle applications and custom applications.</td>
<td>About Oracle and Custom Applications</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Use case for adding applications.</td>
<td>You can learn about a use case that describes the process flow for adding two custom applications in Oracle Identity Cloud Service: a trusted application and a resource server application.</td>
<td>Use Case: Adding Applications</td>
</tr>
<tr>
<td>Add applications.</td>
<td>You can add applications using the <strong>Applications</strong> page.</td>
<td>Add Applications</td>
</tr>
<tr>
<td>View details about applications.</td>
<td>You can view details about applications using the <strong>Applications</strong> page.</td>
<td>View Details About Applications</td>
</tr>
<tr>
<td>Modify applications.</td>
<td>You can modify applications using the <strong>Applications</strong> page.</td>
<td>About Modifying Applications</td>
</tr>
<tr>
<td>Activate and deactivate applications.</td>
<td>You can activate and deactivate applications using the <strong>Applications</strong> page.</td>
<td>Activate Applications</td>
</tr>
<tr>
<td>Import and export users and groups for Oracle application roles.</td>
<td>You can import and export users and groups for Oracle application roles using the <strong>Applications</strong> page.</td>
<td>Deactivate Applications</td>
</tr>
<tr>
<td>Remove applications.</td>
<td>You can remove applications using the <strong>Applications</strong> page.</td>
<td>Remove Applications</td>
</tr>
</tbody>
</table>

You can create, manage, and remove applications by using:

- The Identity Cloud Service console
- SCIM-based APIs

In the following sections, you learn how to manage applications by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

**Understand Cloud Applications**

Oracle Identity Cloud Service provides you with a secure and centralized cloud service to manage your applications.

**Topics:**

- About Cloud Applications
- About Oracle and Custom Applications
- About Enterprise Applications
- About the Relationship Between Oracle Identity Cloud Service and Applications
About Cloud Applications

**Cloud applications** are web-based applications that function in the cloud. These applications can be accessed from anywhere, and at any time, over the web. Examples of cloud applications are Google, Salesforce, and Dropbox.

About Oracle and Custom Applications

**Oracle applications** are a complete and modular set of enterprise applications, engineered to be cloud-ready. In Oracle Cloud, you'll find a broad range of software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) applications. You can use these applications as part of a subscription-based service; there's no software license or hardware to buy and manage. Oracle handles all the supporting underlying technologies.

You can extend Oracle applications or even build your own custom cloud applications in Oracle Cloud. **Custom applications** are applications (such as a mobile application, a web page, a client application, or a server application) that you can integrate with Oracle Identity Cloud Service. By default, for security purposes, custom applications are trusted or confidential.

Oracle Identity Cloud Service leverages the power of OpenID Connect and OAuth to deliver a highly-scalable, multi-tenant token service for securing programmatic access to custom applications by other custom applications, and for federated SSO and authorization integration with these applications:

- Use OAuth 2.0 to define authorization in Oracle Identity Cloud Service for your custom applications. OAuth 2.0 has an authorization framework, commonly used for third-party authorization requests with consent. Custom applications can implement both two-legged and three-legged OAuth flows.
- Use OpenID Connect to externalize authentication to Oracle Identity Cloud Service for your custom applications. OpenID Connect has an authentication protocol that provides Federated SSO, leveraging the OAuth 2.0 authorization framework as a way to federate identities in the cloud. Custom applications participate in an OpenID Connect flow.

Using the OAuth 2.0 and OpenID Connect standards provides the following benefits:

- Federated SSO between the custom application and Oracle Identity Cloud Service. Resource owners (users accessing the custom application) need a single login to access Oracle Identity Cloud Service plus all applications integrated. Oracle Identity Cloud Service handles the authentication and credentials itself, insulating custom applications. This capability is provided by OpenID Connect with OAuth 2.0.
- Authorization to perform operations on third-party servers with consent. Resource owners can decide at runtime whether the custom applications should have authorization to access data or perform tasks for them. This capability is provided by OAuth 2.0.

See Introduction to OAuth in Oracle Cloud in *Understanding Identity Concepts*. 
About Enterprise Applications

Enterprise applications are web applications that require App Gateway to integrate with Oracle Identity Cloud Service for authentication purposes.

To configure an enterprise application in Oracle Identity Cloud Service you need to know the following information about your web application:

- The web application’s base URL. For example, if a known URL of your application is `http://myapp.internal.example.com:3266/myapp/private/home`, then the base URL is `http://myapp.internal.example.com:3266`.

- The list of resources of your web application. For example, if your web application exposes the following URLs: functionalities A to Z in the following format `/myapp/private/funcA` to `/myapp/private/funcZ`, a home page `/myapp/private/home`, a logout URL `/myapp/logout`, an about page `/myapp/public/about`, and an index page `/myapp/index`, then the list of all resources of your web application is:
  - URLs from `/myapp/private/funcA` to `/myapp/private/funcZ`
  - `/myapp/private/home`
  - `/myapp/logout`
  - `/myapp/public/about`
  - `/myapp/index`

- For each resource, define which resources require the user to be authenticated, which don't require user authentication, and which resource represents the log out action. Below are examples of authenticated and non-authenticated resources:
  - Resources from `/myapp/private/funcA` to `/myapp/private/funcZ`, and `/myapp/private/home` require the user to be authenticated.
  - `/myapp/logout` logs the user out.
  - Both `/myapp/public/about` and `/myapp/index` are public resources and don't require the user to be authenticated.

- Identify URL patterns that apply to your list of resources. In the previous example, the URL pattern `/myapp/private/.*` matches all the application’s functionality URLs and the home page URL. All these URLs may require the same kind of authentication.

About the Relationship Between Oracle Identity Cloud Service and Applications

In Oracle Identity Cloud Service, each custom application is represented by an application template. This configuration template is used to define the identity, access, and configuration information that Oracle Identity Cloud Service requires to communicate with the application.

When you purchase an Oracle application, an instance of the application is created in your identity domain and appears in the Applications page automatically.

For a custom application, you must configure Oracle Identity Cloud Service so that it can communicate with the application. You use an application wizard to create a custom application. By doing so, in your identity domain, you add the information that
Oracle Identity Cloud Service uses to communicate with the application. See Add Applications.

You can use Oracle Identity Cloud Service to grant users access to applications in two ways:

- Directly: Assigning users to the applications
- Indirectly: Assigning groups to the applications. Any users who are members of the groups are granted access to the applications.

In addition to granting users and groups access to Oracle applications, you can grant users and groups access to entitlements within applications. For example, you use Oracle Identity Cloud Service to grant John Doe and Jane Doe access to Oracle Java Cloud Service. You want John Doe to have administrator privileges for Oracle Java Cloud Service, but Jane Doe to have only user privileges.

Each entitlement in an Oracle application is represented by an application role. So by assigning John Doe to the application administrator role of Oracle Java Cloud Service, he can access this Oracle Cloud service and he can function as an administrator within it.

Architecture: SAML and Provisioning Integration with Oracle Identity Cloud Service

Oracle Identity Cloud Service is enabled to integrate with the provisioning and SAML integration making it simple and convenient to use.

Topics:
- Architecture Diagram Defining Oracle Identity Cloud Service and SAML Integration
- Architecture Diagram Defining Oracle Identity Cloud Service and Provisioning Integration

Architecture Diagram Defining Oracle Identity Cloud Service and SAML Integration

Security Assertion Markup Language (SAML) is an XML-based system for authentication and authorization between a Service Provider (SP) and an Identity Provider (IdP). It is a standard single sign-on (SSO) format where authentication information is exchanged through digitally signed XML documents.

In this process, the SP trusts the IdP to authenticate users and in return, the IdP generates an authentication assertion suggesting that a particular user has been authenticated.

The following architecture diagram illustrates the integration between Oracle Identity Cloud Service and SAML.
Figure 8-1  Architecture Diagram: Oracle Identity Cloud Service and SAML Integration

SAML Authentication includes three important roles:

- Oracle Identity Cloud Service as the Identity Provider
- Pre-integrated Cloud Services as the Service Provider
- User (Web Browser/ Mobile Device)

Oracle Identity Cloud Service SAML integration currently supports the following features:

- SP initiated Web SSO
- IdP initiated Web SSO
- SP initiated Single Logout
- IDP initiated Single Logout

Oracle Identity Cloud Service provides a generic SAML template to connect to all custom SAML applications.

All applications listed in the Oracle Identity Cloud Service Application Catalog are partially configured templates. These applications are created and maintained by Oracle and contain pre-built integrations with major cloud services making them simple and convenient. Using these applications, you can configure SSO and configure other functionalities in a standard format.
Architecture Diagram Defining Oracle Identity Cloud Service and Provisioning Integration

The customer application is configured as a managed application of Oracle Identity Cloud Service. Through provisioning operations performed on Oracle Identity Cloud Service, accounts are created and updated on the target system for Oracle Identity Cloud Service Users. Through synchronization, account data that is created and updated directly on the target system is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service Users.

The Identity Connector Framework (ICF) is a component that is required to use identity connectors. ICF is distributed with Oracle Identity Cloud Service and doesn't require configuration or modifications.

The following architecture diagram illustrates the integration between Oracle Identity Cloud Service and Provisioning.

Figure 8-2  Architecture Diagram: Oracle Identity Cloud Service and Provisioning Integration

During provisioning:
1. App Management calls ICF.
2. ICF sends a CREATE request to the Connector Bundle.
3. The Connector Bundle calls the target API for provisioning.
4. The target API accepts provisioning data from the Connector Bundle.
5. The target API carries out the required operation on the target system.
6. The target API then sends the response from the target system to the Connector Bundle.

During synchronization:
1. A synchronization job calls ICF.
2. ICF sends a SEARCH request to the Connector Bundle.
3. The Connector Bundle calls the target API for the synchronization operation.
4. The API extracts user records that match the synchronization criteria.
5. The API sends these records through the Connector Bundle and ICF to the synchronization job, which syncs the records with Oracle Identity Cloud Service.

Each record fetched from the target system is compared with the user accounts that are already provisioned to Oracle Identity Cloud Service Users. If a match is found, then the update made to the account from the target system is copied to the user account in Oracle Identity Cloud Service. If a match isn't found, then the user ID of the record is compared with the user ID of each Oracle Identity Cloud Service User. If the user ID matches, then data in the target system record is used to provision the user account to the Oracle Identity Cloud Service User.

Use Case: Adding Applications

To understand how to add custom applications in Oracle Identity Cloud Service, read this use case.

For this use case, a user accesses the Customer Quotes trusted application. This trusted application is a client application that makes REST API calls to the abccorp.com resource server application. A resource server application is a third-party application that provides services that a trusted application can consume on behalf of the user.

For this example, the abccorp.com resource server application is a financial application that contains REST APIs that can be used to make a quote (/quote), request for a quote (/rfq), or get information about the user (/user).

When the user accesses the Customer Quotes trusted application, the application makes REST API calls to the abccorp.com resource server application on behalf of the user. In this example, the user doesn't communicate directly with the abccorp.com application.

Because the Customer Quotes application performs actions on behalf of the user, the application needs access to the /quote, /rfq, and /user REST APIs available with the abccorp.com application. To make these REST API calls, the Customer Quotes application might ask for the user's consent. This consent can come at any time that the Customer Quotes application calls for these REST APIs in the abccorp.com application.

The user logs in to Oracle Identity Cloud Service and accesses the Custom Quotes application, through single sign-on, by using OAuth 2.0 and Open ID Connect, as this is a way of federating identities in the cloud. Because the Customer Quotes application is authorized on behalf of the user to make the /quote, /rfq, and /user REST API calls to the abccorp.com application, the user can use the Customer Quotes application to make a quote, request for a quote, and get information about the user.
Any additional actions that the user wishes to perform through the Customer Quotes application won’t be allowed.

To build this workflow, you create and activate two custom applications in Oracle Identity Cloud Service:

- The abccorp.com resource server application. This application has REST APIs (resources) that other applications, such as the Customer Quotes application, can access. In this example, the user doesn’t access the resource server application directly, but indirectly through the Customer Quotes application.

  You register resources of the abccorp.com resource server application. Application resources are API calls that are authorized by Oracle Identity Cloud Service. For this example, the application resources are the /quote, /rfq, and /user REST APIs. For security and auditing purposes, you can specify whether the user must give consent to access these resources.

- The Customer Quotes trusted application. The user uses this application to access the REST APIs of the abccorp.com application.

  When you create this custom application, you want to generate an authorization code for the user when the user logs in to Oracle Identity Cloud Service. The authorization code is then sent to the Customer Quotes application to retrieve an access token. The access token contains all the rights that the user has to access the resource server application. For this example, these rights include making a quote, requesting a quote, and retrieving information about the user.

  Because the access token’s lifetime is short, you may want to generate a refresh token. A refresh token is a secure mechanism to obtain a new access token when the current access token expires. This way, the Customer Quotes application can access the APIs of the abccorp.com application without asking for user consent again.

See Add Applications, Activate Applications, and Deactivate Applications for more information about creating and activating custom applications in Oracle Identity Cloud Service.

### About Adding Applications

Learn about the various applications available and how to add them in Oracle Identity Cloud Service.

**Topics:**

- Add Applications
- Add a Confidential Application
- Configure Authorized Resources
- Add a Mobile Application
- Add a SAML Application
- Upgrade a SAML Application
- Secure Enterprise Applications with App Gateway
- About App Catalog Application
- Add Tags to an Application
Add Applications

You can add Oracle Applications or Custom Applications in Oracle Identity Cloud Service, if you are assigned to either the identity domain administrator role or the application administrator role.

See Add or Remove a User Account from an Administrator Role for information about assigning users to administrator roles.

You can add the following types of custom applications in Oracle Identity Cloud Service:

- **App Catalog application**: Add an application from the Application Catalog, which contains pre-configured application templates.

- **SAML application**: Accessed by multiple users and hosted in a secure and protected place (server). Create a Security Assertion Markup Language (SAML) application that supports SAML for single sign on. This allows users to single sign-on (SSO) into your software as a service (SaaS) applications that support SAML for SSO.

- **Mobile application**: Hosted directly on the resource owner's browser, machine, or mobile device. An example of this type of application is an Android or iPhone application. A mobile application can run in multiple environments outside of your control. Since these environments are not trusted, this type of application has reduced integration options.

- **Confidential application**: Accessed by multiple users and hosted in a secure and protected place (server). The application uses OAuth 2.0. Applications that can protect their OAuth client id and client secret are called confidential applications.

- **Enterprise application**: Enterprise applications are web applications that require App Gateway to integrate with Oracle Identity Cloud Service for authentication purposes.
Tip:

- When you purchase an Oracle Cloud application or service, an instance of the application is created in your identity domain and appears in the Applications page automatically.
- You can access the Onboarding Applications infographic to see how to add custom applications in Oracle Identity Cloud Service.
- You can access the Integrating a Custom Client Application tutorial to see how to integrate a custom client application with Oracle Identity Cloud Service.
- You can access the Integrating a Custom Resource Server Application tutorial to see how to integrate a custom resource server application with Oracle Identity Cloud Service.
- You can access the Secure Enterprise Applications with App Gateway topic to see how to integrate an enterprise application with Oracle Identity Cloud Service.

Add a Confidential Application

You can use Oracle Identity Cloud Service to add a confidential application. Confidential applications run on a protected server.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click Add.
3. In the Add Application page, click Confidential Application.
4. In the App Details pane of the Add Confidential Application window, use the following table to configure application details and the display settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the confidential application. You can enter up to 125 characters. For applications with lengthy names, the application name appears truncated in the My Apps page. Consider keeping your application names as short as possible.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the confidential application. You can enter up to 250 characters.</td>
</tr>
<tr>
<td>Application Icon</td>
<td>Click Upload to add an icon that represents the application. This icon appears next to the name of the application on the My Apps page and the Applications page.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application URL</td>
<td>Enter the URL (HTTP or HTTPS) where the user is redirected after a successful login. This value is also known as the SAML RelayState parameter. HTTPS format is suggested. HTTP should only be used for testing purposes.</td>
</tr>
<tr>
<td>Custom Login URL</td>
<td>In the Custom Login URL field, specify a custom login URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.</td>
</tr>
<tr>
<td>Custom Logout URL</td>
<td>In the Custom Logout URL field, specify a custom logout URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.</td>
</tr>
<tr>
<td>Custom Error URL</td>
<td>This is an optional field. Enter the error page URL to which a user has to be redirected, in case of a failure. If not specified, the tenant specific Error page URL will be used. If both the error URLs are not configured, then the error will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error). When a user tries to use social authentication (ex: Google, Facebook, and so on) for logging into Oracle Identity Cloud Service, the callback URL must be configured in the Custom Error URL field. Social providers need this callback URL to call Oracle Identity Cloud Service and send the response back after social authentication. The provided callback URL is used to verify whether the user exists or not (in the case of first time social login), and display an error if the social authentication has failed.</td>
</tr>
<tr>
<td>Linking callback URL</td>
<td>This is an optional field. Enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. When you create a custom app using Oracle Identity Cloud Service custom SDK and integrate with Oracle Identity Cloud Service Social Login, the custom app needs to have the Linking callback URL which can be redirected after linking of the user between social provider and Oracle Identity Cloud Service is complete.</td>
</tr>
<tr>
<td>Tags</td>
<td>Click Add Tag to add tags to your confidential applications to organize and identify them. See Adding Tags to an Application.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Display in My Apps | Select the check box if you want the confidential application to be listed for users on their My Apps pages. In this case you need to configure the application as a resource server.

When you select the Display in My Apps check box in applications, the app is then visible in the My Apps page, but selecting this check box doesn’t enable or disable SSO to the app.

The flag to enable or disable SSO comes from the app template. Use the Oracle Identity Cloud Service REST APIs to update this flag. You cannot set the SSO flag from the UI. See REST API for Oracle Identity Cloud Service.

User can request access | Select the check box if you want end users to be able to request access to the app from their My Apps page by clicking Add Access. If self service is not enabled, users won’t see the Add Access button.

5. Click Next to proceed. A confirmation message indicates that the application has been added in a deactivated state.

6. To configure authorization information for your application now, click Configure this application as a client now, and use the following table. Otherwise, click Skip for later and go to step 8.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Owner</td>
<td>Use when the resource owner has a trust relationship with the confidential application, such as a computer operating system or a highly privileged application, because the confidential application must discard the password after using it to obtain the access token.</td>
</tr>
<tr>
<td>Client Credentials</td>
<td>Use when the authorization scope is limited to the protected resources under the control of the client or to the protected resources registered with the authorization server. The client presents its own credentials to obtain an access token. This access token is either associated with the client’s own resources, and not a particular resource owner, or is associated with a resource owner for whom the client is otherwise authorized to act</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JWT Assertion</td>
<td>Use when you want to use an existing trust relationship expressed as an assertion and without a direct user approval step at the authorization server. The client requests an access token by providing a user JSON web token (JWT) assertion or a third-party user JWT assertion and client credentials. A <strong>JWT assertion</strong> is a package of information that facilitates the sharing of identity and security information across security domains.</td>
</tr>
<tr>
<td>SAML2 Assertion</td>
<td>Use when you want to use an existing trust relationship expressed as a SAML2 assertion and without a direct user approval step at the authorization server. The client requests an access token by providing a user SAML2 assertion or a third-party user SAML2 assertion and client credentials. A <strong>SAML2 assertion</strong> is a package of information that facilitates the sharing of identity and security information across security domains.</td>
</tr>
<tr>
<td>Refresh Token</td>
<td>Select this grant type when you want a refresh token supplied by the authorization server, and then use it to obtain a new access token. Refresh tokens are used when the current access token becomes invalid or expires and don't requiring the resource owner to reauthenticate.</td>
</tr>
<tr>
<td>Authorization Code</td>
<td>Select this grant type when you want to obtain an authorization code by using an authorization server as an intermediary between the client application and resource owner. An <strong>authorization code</strong> is returned to the client through a browser redirect after the resource owner gives consent to the authorization server. The client then exchanges the authorization code for an access (and often a refresh) token. Resource owner credentials are never exposed to the client.</td>
</tr>
<tr>
<td>Implicit</td>
<td>If the application can't keep client credentials confidential for use in authenticating with the authorization server, then select this check box. For example, your application is implemented in a web browser using a scripting language such as JavaScript. An access token is returned to the client through a browser redirect in response to the resource owner authorization request (rather than an intermediate authorization).</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
**Device Code** | Select the **Device Code** grant type if the client doesn't have the capability to receive requests from the OAuth Authorization Server, for example, it cannot act as an HTTP server such as game consoles, streaming media players, digital picture frames, and others. In this flow, the client obtains the user code, device code, and verification URL. The user then accesses the verification URL in a separate browser to approve the access request. Only then can the client obtain the access token using the device code.

**Allow non-HTTPS URLs** | Select this check box if you want to use HTTP URLs for the **Redirect URL**, **Logout URL**, or **Post Logout Redirect URL** fields. For example, if you are sending requests internally, want a non-encrypted communication, or want to be backward-compatible with OAuth 1.0, then you can use an HTTP URL. Also, select this check box when you are developing or testing your application and you may not have configured SSL. This option is provided as a convenience and is not recommended for production deployments.

**Redirect URL** | Enter the application URL where the user is redirected after authentication.

**Note:**

Provide an absolute URL. Relative URLs are not supported.

**Logout URL** | Enter the URL where the user is redirected after logging out of the confidential application.

**Post Logout Redirect URL** | Enter the URL where you want to redirect the user after logging out of the application.

**Client Type** | Select the client type. The available client types are **Trusted** and **Confidential**. Choose **Trusted** if the client can generate self signed user assertions. Then, to import your signing certificate that the client uses to sign its self-signed assertion, click **Import**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allowed Operations     | • Select the **Introspect** check box if you want to allow access to a token introspection end point for your application. If the confidential application can’t keep client credentials confidential for use in authenticating with the authorization server, then select this check box. For example, your confidential application is implemented in a web browser using a scripting language such as JavaScript. An access token is returned to the client through a browser redirect in response to the resource owner authorization request (rather than an intermediate authorization code).  
• Select the **On behalf Of** check box if you want to ensure that access privileges can be generated from the user’s privileges alone. This allows the client application to access endpoints to which the user has access, even if the client application by itself would not normally have access. |
| Authorized Resources   | Select one of the following options to allow a client application to access authorized resources:  
• **All** – Access any resource within a domain (All). See Accessing All Resources.  
• **Tagged** – Access any resource with matching tags (Tagged). See Accessing Resources With Matching Tags.  
• **Specific** – Access only those resources where an explicit association between the client and the resource (Specific) exists. See Accessing Resources With Specific Scopes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Note:**

The option to define an authorized resource is available to only confidential applications. Mobile applications don’t have the option to define a trust scope.

See Account Trust Scope for additional scope information as well as request and response examples for use with the Oracle Identity Cloud Service REST APIs.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tags</td>
<td><strong>Note:</strong> Tags are available only when you select the Tagged option. It remains hidden for the other two Authorized Resource options. Click Tagged to enable your confidential application to access tags from other applications. See Adding Tags to an Application.</td>
</tr>
<tr>
<td>Resources</td>
<td>If you want your application to access APIs from other applications, then click Add in the Token Issuance Policy section of the Add Confidential Application page. Then, in the Add Scope window, select the applications that your application references. <strong>Note:</strong> You can delete scopes by clicking the x icon next to the scope. However, you can't delete scopes that are protected.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant the client access to Identity Cloud</td>
<td>Click <strong>Add</strong> to enable your confidential application to access Oracle Identity Cloud Service APIs.</td>
</tr>
<tr>
<td>Service Admin APIs</td>
<td>In the <strong>Add App Role</strong> window, select the application roles that you want to assign to this application. This enables your application to access the REST APIs that each of the assigned application roles can access.</td>
</tr>
<tr>
<td></td>
<td>For example, select <strong>Identity Domain Administrator</strong> from the list. All REST API tasks available to the identity domain administrator will be accessible to your application.</td>
</tr>
<tr>
<td></td>
<td>You can delete the application roles by clicking the x icon for the row of the required application role.</td>
</tr>
</tbody>
</table>

#### Note:

You can’t delete protected application roles.

---

See Apps/App Roles endpoint for a complete list of which endpoints each application role can access.

---

7. Click **Next**.

8. To protect resources for your application now, click **Configure this application as a resource server now**, and use the following table. If you want the application to be visible on the **My Apps** page, then you need to configure the application as a resource server. Otherwise, to specify that no resources of your confidential application will be protected by OAuth 2.0, or to protect them at a later time, click **Skip for later**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token Expiration</td>
<td>Define how long (in seconds) the access token associated with your confidential application remains valid.</td>
</tr>
<tr>
<td>Is Refresh Token Allowed</td>
<td>Select this check box if you want to use the refresh token that you obtain when using the Resource Owner, Authorization Code, or Assertion grant types.</td>
</tr>
<tr>
<td>Refresh Token Expiration</td>
<td>Define how long (in seconds) the refresh token, which is returned with your access token and is associated with your confidential application, remains valid.</td>
</tr>
<tr>
<td>Primary Audience</td>
<td>Enter the primary recipient where the access token of your confidential application is processed.</td>
</tr>
</tbody>
</table>
### Configure Authorized Resources

Authorized resources define the way a client can access the resources in a confidential application.

**Topics:**
- Access All Resources
- Access Resources With Matching Tags
- Access Resources With Specific Scopes
Access All Resources

The **All** authorized resource option enables the client to access any resource within a domain.

Select **All** to allow your application to request an access token for trusted or confidential client using the scope `urn:opc:resource:consumer::all`. This option provides a wide scope. The access token in the response contains the audience `urn:opc:resource:scope:account` and the scope `urn:opc:resource:consumer::all`, which gives access to any of the services that are in the same domain without requiring explicit association with target services.

**Use only the `urn:opc:resource:consumer::all` scope in the request. An invalid scope error is returned if you attempt to include both the `urn:opc:resource:consumer::all` scope and another scope in the same request, such as `urn:opc:idm:__myscopes__`.**

In the account mode, clients can get token for any specific resource provided either `urn:opc:resource:consumer::all` or the specific resource is added in the allowed scopes.

Apart from the scope defined above, you can also specify fine-grained scope as follows:

- `urn:opc:resource:consumer:paas::read`
- `urn:opc:resource:consumer:paas:stack::all`
- `urn:opc:resource:consumer:paas:analytics::read`

**Note:**

The requested scope should always exist and match, either directly or hierarchically, the client's defined allowed scopes to allow the client access to the resource.

For example, a client uses the `urn:opc:resource:consumer:paas:analytics::read` scope in its request for access to a resource. If the scope directly matches an allowed scope defined, then in the returned access token the audience is `urn:opc:resource:scope:account` and the scope is `urn:opc:resource:consumer:paas:analytics::read`.

If the allowed scope defined by the client is `urn:opc:resource:consumer:paas::read`, then the client is allowed to access the resource hierarchically if the client requests one of the following scopes:

- `urn:opc:resource:consumer:paas::read`
- `urn:opc:resource:consumer:paas:analytics::read`

However, if the requested scope is `urn:opc:resource:consumer:paas:analytics::write` with a different qualifier, then the client isn't allowed access to the resource.
To generate a refresh token in addition to the access token, use the scope `urn:opc:resource:consumer::all offline_access` in the request.

Access Resources With Matching Tags

The Tagged authorized resource option enables the client to access any resource with matching tags.

Request an access token using the trusted or confidential client and request the scope `urn:opc:resource:consumer::all`. The access token in the response contains the audience `urn:opc:resource:scope:tag=<base64 encoded JSON>` and the scope `urn:opc:resource:consumer::all`, which gives access to Resource Apps that have tags that match the allowed tags specified in the Client App.

In the tags mode, clients can get token for any specific resource provided either the client has matching tags with the resource and `urn:opc:resource:consumer::all` or the specific resource is added in the allowed scopes.

Select Tagged to enable your confidential application to access tags from other applications.

When you select Tagged, you can choose scopes from an OPC application that aren't specific, such as `urn:opc:resource:consumer`.

To select scopes:
1. Select Tagged.
2. Select Add Scope under Resources.
4. Select the OPC scopes that you want to add and provide a named qualifier, such as read and write to each of the scopes. You can edit these qualifiers dynamically.
5. Click Add.

The scopes appear under Resources.

In addition to using the `urn:opc:resource:consumer::all` scope, you can also specify the following fine-grained scopes:

- `urn:opc:resource:consumer:paas::read`
- `urn:opc:resource:consumer:paas:stack::all`
- `urn:opc:resource:consumer:paas:analytics::read`
For example, a client uses the `urn:opc:resource:consumer:paas:analytics::read` scope in its request for access to a resource. If the scope directly matches an allowed scope defined, then in the returned access token the audience is `urn:opc:resource:scope:tag=<base64 encoded JSON>` and the scope is `urn:opc:resource:consumer:paas:analytics::read`.

For client allowed tags `color:green` and `color:blue`, the sample JSON is as follows:

```json
{"tags":[
  { "key":"color","value":"green"},
  { "key":"color","value":"blue" }
]}
```

If the allowed scope defined by the client is `urn:opc:resource:consumer:paas::read`, then the client is allowed to access the resource hierarchically if the client requests one of the following scopes:

- `urn:opc:resource:consumer:paas::read`
- `urn:opc:resource:consumer:paas:analytics::read`

However, if the requested scope is `urn:opc:resource:consumer:paas:analytics::write`, then the client isn't allowed access to the resource, since that isn't one of the allowed scopes defined by the client.

**Access Resources With Specific Scopes**

The **Specific** authorized resource option enables the client to access only those resources where an explicit association between the client and the resource exists.

Leave **Specific** selected (the default) to allow your application to acquire an access token with permissions based on an explicit association between the client and target services. Then, use the **Add** button to select the applications that your application references.

The **Specific** option is assigned by default to confidential applications created prior to Oracle Identity Cloud Service version 17.4.2. To use the **All** option, you must open the application from the Oracle Identity Cloud Service administration console, and then select **All**.

**Add a Mobile Application**

You can use Oracle Identity Cloud Service to add a mobile application. Mobile applications use OAuth 2.0 and they cannot maintain the confidentiality of their client secrets.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.
2. Click **Add**.
3. In the **Add Application** page, click **Mobile Application**.
4. In the **App Details** section of the Add Mobile Application page, use the following table to configure the application details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the mobile application. You can enter up to 125 characters. For applications with lengthy names, the application name appears truncated in the <strong>My Apps</strong> page. Consider keeping your application names as short as possible.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the mobile application. You can enter up to 250 characters.</td>
</tr>
<tr>
<td>Application Icon</td>
<td>Click <strong>Upload</strong> to add an icon that represents the application. This icon appears next to the name of the application on the My_apps page and the Applications page.</td>
</tr>
<tr>
<td>Custom Login URL</td>
<td>In the <strong>Custom Login URL</strong> field, specify a custom login URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.</td>
</tr>
<tr>
<td>Custom Logout URL</td>
<td>In the <strong>Custom Logout URL</strong> field, specify a custom logout URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.</td>
</tr>
<tr>
<td>Custom Error URL</td>
<td>This is an optional field. Enter the error page URL to which a user has to be redirected, in case of a failure. If not specified, the tenant specific Error page URL will be used. If both the error URLs are not configured, then the error will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error). When a user tries to use social authentication (ex: Google, Facebook, and so on) for logging into Oracle Identity Cloud Service, the callback URL must be configured in the Custom Error URL field. Social providers need this callback URL to call Oracle Identity Cloud Service and send the response back after social authentication. The provided callback URL is used to verify whether the user exists or not (in the case of first time social login), and display an error if the social authentication has failed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Linking callback URL</strong></td>
<td>This is an optional field. Enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. When you create a custom app using Oracle Identity Cloud Service custom SDK and integrate with Oracle Identity Cloud Service Social Login, the custom app needs to have the Linking callback URL which can be redirected after linking of the user between social provider and Oracle Identity Cloud Service is complete.</td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td>Click Add Tag to add tags to your mobile applications to organize and identify them. See Adding Tags to an Application.</td>
</tr>
<tr>
<td><strong>Display in My Apps</strong></td>
<td>Select the check box if you want the mobile application to be listed for users on their My Apps pages. In this case you need to configure the application as a resource server. When you select the Display in My Apps check box in applications, the app is then visible in the My Apps page, but selecting this check box doesn’t enable or disable SSO to the app. The flag to enable or disable SSO comes from the app template. Use the Oracle Identity Cloud Service REST APIs to update this flag. You cannot set the SSO flag from the UI. See REST API for Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td><strong>User can request access</strong></td>
<td>Select the check box if you want end users to be able to request access to the app from their My Apps page by clicking Add Access. If self service is not enabled, users won’t see the Add Access button.</td>
</tr>
</tbody>
</table>

5. Click Next. A message confirms that the application has been added in deactivated state.

6. In the Authorization and Accessing APIs from Other Application sections of the Add Mobile Application page, use the following table to configure application details.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allowed Grant Types</strong></td>
<td>Select the check box for the grant types that this application is allowed to use when requesting validation.</td>
</tr>
<tr>
<td>• <strong>Authorization Code</strong></td>
<td>Select the check box when you want to obtain an authorization code by using an authorization server as an intermediary between the client application and resource owner. An authorization code is returned to the client through a browser redirect after the resource owner gives consent to the authorization server. The client then exchanges the authorization code for an access (and often a refresh) token. Resource owner credentials are never exposed to the client.</td>
</tr>
<tr>
<td>• <strong>Implicit</strong></td>
<td>Select the Implicit check box if the application can't keep client credentials confidential for use in authenticating with the authorization server. An access token is returned to the client through a browser redirect in response to the resource owner authorization request (rather than an intermediate authorization code).</td>
</tr>
<tr>
<td>• <strong>Device Code</strong></td>
<td>Select the Device Code grant type if the client doesn't have the capability to receive requests from the OAuth Authorization Server, for example, it cannot act as an HTTP server such as game consoles, streaming media players, digital picture frames, and others. In this flow, the client obtains the user code, device code, and verification url. The user then accesses the verification url in a separate browser to approve the access request. Only then can the client obtain the access token using the device code.</td>
</tr>
<tr>
<td><strong>Allow non-HTTPS URLs</strong></td>
<td>Select this check box if you want to use HTTP URLs for the Redirect URL, Logout URL, or Post Logout Redirect URL fields. For example, if you are sending requests internally, want a non-encrypted communication, or want to be backward-compatible with OAuth 1.0, then you can use an HTTP URL. Also, select this check box when you are developing or testing your application and you may not have configured SSL. This option is provided as a convenience and is not recommended for production deployments.</td>
</tr>
<tr>
<td><strong>Redirect URL</strong></td>
<td>Enter the application URL where the user is redirected after authentication.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logout URL</td>
<td>Enter the URL where the user is redirected after logging out of the application.</td>
</tr>
<tr>
<td>Post Logout Redirect URL</td>
<td>Enter the URL where you want to redirect the user after logging out of the application.</td>
</tr>
</tbody>
</table>
| Allowed Operations                   | • Select the **Introspect** check box, if you want to allow access to a token introspection end point for your application.  
• Select the **On behalf Of** check box, if you want to ensure that access privileges can be generated from the user’s privileges alone, so that a client application can access endpoints to which the user has access, even if the client application by itself would not normally have access. |
| Resources                            | If you want your application to access APIs from other applications, then click **Add Scope** in the **Token Issuance Policy** section of the **Add Mobile Application** page. Then, in the **Add Scope** window, select the applications that your application will reference. |
| Grant the client access to Identity Cloud Service Admin APIs | Click **Add** to enable your mobile application to access Oracle Identity Cloud Service APIs.  
In the **Add App Role** window, select the application roles that you want to assign to this application. This enables your application to access the REST APIs that each of the assigned application roles can access.  
For example, select **Identity Domain Administrator** from the list. All REST API tasks available to the identity domain administrator will be accessible to your application.  
You can delete the application roles by clicking the x icon for the row of the required application role. |

**Note:**  
You can’t delete protected application roles.  
See Apps/App Roles endpoint for a complete list of which endpoints each application role can access.

7. Click **Next**.  
8. If you want Oracle Identity Cloud Service to control access to the application based on grants to users and groups, select the **Enforce Grants** as
Authorization check box. Select this check box if you want users to access only the application that you assigned or granted access to. If the check box is not selected, any authenticated user has access to the application regardless of the assignment status.

9. Click Finish. A message confirms that the application has been added in deactivated state. To activate your application see Activating Applications.

10. Note the Client ID that appears in the Application Added window. This information also appears on the Configuration tab in the Details section for the application. To integrate with your application, use this ID as part of your connection settings. Because a mobile application runs on a mobile device, Oracle Identity Cloud Service does not generate a Client Secret for this type of application.

11. Click Close.

Add a SAML Application

Create a Security Assertion Markup Language (SAML) application and grant it to users so that your users can single sign-on (SSO) into your SaaS applications that support SAML for SSO.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.

2. Click Add.

3. In the Add Application window, click SAML Application.

4. In the App Details section of the Add SAML Application page, provide values for the following fields:
   - In the Name field, enter a name for the application. For applications with lengthy names, the application name appears truncated in the My Apps page. Consider keeping your application names as short as possible.
   - In the Description field, enter 250 or fewer characters to provide a description of the application.
   - Click Upload to add an icon for your application.
   - In the Application URL / Relay State field, enter a value which will be sent to the SAML SP as the SAML RelayState parameter.
   - In the Custom Login URL field, specify a custom login URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.
   - In the Custom Logout URL field, specify a custom logout URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.
   - In the Custom Error URL field, enter the error page URL to which a user has to be redirected, in case of a failure. This is an optional field. However, if not specified, the tenant specific Error page URL will be used. If both the error URLs are not configured, then the error will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error).
When a user tries to use social authentication (ex: Google, Facebook, and so on) for logging into Oracle Identity Cloud Service, the callback URL must be configured in the Custom Error URL field. Social providers need this callback URL to call Oracle Identity Cloud Service and send the response back after social authentication. The provided callback URL is used to verify whether the user exists or not (in the case of first time social login), and display an error if the social authentication has failed.

- In the **Linking callback URL** field, enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. This is an optional field.

When you create a custom app using Oracle Identity Cloud Service custom SDK and integrate with Oracle Identity Cloud Service Social Login, the custom app needs to have the Linking callback URL which can be redirected after linking of the user between social provider and Oracle Identity Cloud Service is complete.

- Click **Add** to add **App Links** that are associated with the application. The **Link** window appears. App Links are services such as Mail or Calendar that are offered by applications such as Google or Office 365.

In the **Link** window:

  a. In the **Name** field, enter the **App Link** name.
  b. In the **Link** field, enter the URL used to access the application.
  c. Click **Upload** to upload an icon.
  d. Select **Visible** check box if you want your application to appear automatically on each user’s **My Apps** page.

  **Note:**
  Selecting this check box does not enable or disable SSO into the application.

  e. Click **Add**.

  The App Link information appears in the **App Details** section of the application page.

To remove an **App Link**, select the row, and then click **Remove**.

  **Note:**
  There is a delay (a few seconds) between clicking **Remove** and the App no longer appearing on the My Apps page. App Link deletion (and grants related to those App Links) is asynchronous. Wait a few seconds for the asynchronous task to remove the App and its grants before trying **My Apps** again.

5. In the **Tags** section of the Add SAML Application page, click **Add Tag** to add tags to your SAML application to organize and identify it. See **Adding Tags to an Application**.
6. In the **Display Settings** sections of the Add SAML Application page, make the following selections:

   • Select **Display in My Apps** check box to specify whether you want the SAML App to be listed on the My Apps page.

     When you select the **Display in My Apps** check box in applications, the app is then visible in the **My Apps** page, but selecting this check box doesn't enable or disable SSO to the app.

     The flag to enable or disable SSO comes from the app template. Use the Oracle Identity Cloud Service REST APIs to update this flag. You cannot set the SSO flag from the UI. See REST API for Oracle Identity Cloud Service.

   • Select the **User can request access** check box if you want the app to be listed in the Catalog. This option allows end users to request access to the app from their **My Apps** page by clicking **Add** and then selecting the app from the Catalog.

     **Note:**
     Don't forget to activate the application so that users can request access.

7. Click **Next** to configure SSO details for the SAML application.

8. In the **General** section of the SSO Configuration page, define the following:

   • **Entity ID**: Enter a globally unique name for a SAML entity. It usually takes a URL of an identity provider or a service provider as a value.

   • **Assertion Consumer URL**: Enter the URL to which the SAML identity provider will send the SAML assertion. This URL must begin with either the HTTP or HTTPS protocol.

   • **NameID Format**: Select the type of format to use for the NameID. The service provider and the identity provider use this format to easily identify a subject during their communication.

     **Note:**
     When you integrate Oracle Identity Cloud Service with MS SharePoint app based on WS Fed 1.1 protocol, the following options are not available in the NameID format: **Persistent**, **Kerberos**, and **Transient**.

   • **NameID Value**: Select the NameID Value to identify the user that is logged in. The available options are **User Name**, the user’s **Primary Email** address and **Expression**. When you select the **Expression** option, enter a regular expression as a value in the text box. There is no character limit for the value, however, there are validation rules that are performed on the value for any invalid characters that cannot be mapped.

   • **Signing Certificate**: Upload the signing certificate that is used to encrypt the SAML assertion.
9. Expand **Advanced Settings** on the SSO Configuration page, and then use the following table to define a more fine-grained SAML configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed SSO</td>
<td>Select <strong>Assertion</strong> to indicate that you want the SAML assertion signed. Select <strong>Response</strong> when you want the SAML authentication response signed.</td>
</tr>
<tr>
<td>Include Signing Certificate in Signature</td>
<td>Select the check box to include the signing certificate in the signature, for example, when the application requires that the signing certificate is sent along with the assertion.</td>
</tr>
<tr>
<td>Signature Hashing Algorithm</td>
<td>Select the type of signing algorithm that you want to use to sign the assertion or the response, either <strong>SHA-256</strong> or <strong>SHA-1</strong>. SHA-256 generates a fixed 256-bit hash. SHA-1 generates a 160-bit hash value known as a message digest.</td>
</tr>
<tr>
<td>Enable Single Logout</td>
<td>Select to configure SAML single logout. Single logout enables a user to log out of all participating sites in a federated session almost simultaneously. This check box is selected by default. Clear it if you do not want to enable single logout.</td>
</tr>
<tr>
<td>Logout Binding</td>
<td>Select whether the log out request is sent as a REDIRECT (transported using HTTP 302 status-code response messages) or a POST (transported in HTML form-control content, which uses a base-64 format). This list box appears only if you select the <strong>Enable Single Logout</strong> check box.</td>
</tr>
<tr>
<td>Single Logout URL</td>
<td>Enter the location (HTTP or HTTPS) where the log out request is sent. This field appears only if you select the <strong>Enable Single Logout</strong> check box.</td>
</tr>
<tr>
<td>Logout Response URL</td>
<td>Enter the location (HTTP or HTTPS) where the log out response is sent. This field appears only if you select the <strong>Enable Single Logout</strong> check box.</td>
</tr>
<tr>
<td>Encrypt Assertion</td>
<td>Select if you want to encrypt the assertion, and then define the encryption algorithm that you want to use and upload the encryption certificate.</td>
</tr>
<tr>
<td>Encryption Certificate</td>
<td>Click <strong>Upload</strong> to upload the encryption certificate that's used to encrypt the SAML assertion. This button appears only if you select the <strong>Encrypt Assertion</strong> check box.</td>
</tr>
</tbody>
</table>

**Note:**

In a FIPS enabled environment, set the **Signature Hashing Algorithm** to SHA-256, the only supported hashing algorithm, to avoid errors during SSO.
10. Expand **Attribute Configuration** on the SSO Configuration page to add user-specific and group-specific attributes to the SAML assertion. This is useful if your application uses user-specific or group-specific attributes, and you want to send that information as part of the SAML assertion.

11. Click the plus sign next to **Attributes**, and then use the following table to specify the user attribute that you want to include. User information in the attribute statement contains a list of attributes. Each attribute includes a name and a list of values (in the case of multiple attribute values). Each value includes a value and the format of the value.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the SAML assertion attribute.</td>
</tr>
<tr>
<td>Format</td>
<td>Select the format of this SAML assertion attribute: Basic, URI Reference, or Unspecified.</td>
</tr>
</tbody>
</table>

**Note:**

When you integrate Oracle Identity Cloud Service with MS SharePoint app based on WS Fed 1.1 protocol, **Format** drop-down is replaced with **Namespace**.
Option | Description
--- | ---
Type | Select one of the options below to specify the value of the assertion attribute:
- **User Attribute**
  Select this option to choose one of the predefined list of user attributes or group attributes in the Value drop-down as the value of the assertion attribute. In order to specify group attributes, select **User Attribute** and in the Value field, select **Group Membership**.
- **Expression/Literal**
  Select this option when you cannot use any of the predefined values in the Value drop-down. You can provide an expression in the Value text box to specify the value of the SAML assertion attribute.
  In order to specify group attributes, select **Expression/Literal** and specify an expression to fetch the groups.
  Example: The following expression specifies that the value of the SAML attribute should be the names of all the groups to which the user belongs: $\{user.groups[*].display\}$.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Value  | Select or enter the value to send as part of the assertion based on the **Type** that you have selected.  
When the type is **User Attribute**, you can select one of the predefined list of user attributes as the value of the assertion attribute. Select the **Group Membership** option in the drop-down if you want to send the users group membership as the value of the assertion attribute. The **Condition** and **Value** columns appear when you choose **Group Membership**.  
When the type is **Expression/Literal**, the value field is a text box and you can enter any path expression to specify what should be the value of the assertion attribute. Some examples of path expressions are listed below:  
• To send a list of literal values as the value of the assertion attribute, use ["value1", "value2", "value3"].  
• To send "home email" as the value of the assertion attribute, use $(user.emails[type eq "home"].value).  
• To send users first name concatenated with last name as the assertion attribute, use #concat($ (user.name.givenName), $(user.name.familyName)).  
• To send an account attribute called SALARY as the value of the assertion attribute, use $(account.SALARY).  
• To include an attribute department from custom schema extension, use $(user.urn:ietf:params:scim:schemas:idcs:extension:custom:User:department).  
• To send a literal value as the value of assertion, use aLiteralValue.  

| Condition | Select a condition from the drop-down to filter the group memberships. This field is enabled only when you select **User Attribute** as **Type** and **Group Membership** as **Value**. The available values are: **Equals**, **Starts with**, and **All Groups**. |
| Value     | Enter the filter value to use when filtering the group memberships. |

12. When you are creating SAML app from scratch rather than creating a preconfigured SAML app created from the App Catalog, the **Authentication and Authorization** section appears. The **Enforce Grants as Authorization** check box is selected by default. This check box enables users to access only the application that you assigned or granted access to. If the check box is selected, Oracle
Identity Cloud Service can control access to the SAML application based on grants to users and groups. If the check box is not selected, any authenticated user has access to the application regardless of the assignment status.

13. To import the Identity Cloud Service signing certificate into your application, click **Download Signing Certificate** to first download the certificate file in PEM format. This certificate is used by the SAML application to verify that the SAML assertion is valid.

14. To import the Identity Cloud Service Identity Provider metadata into your application, click **Download Identity Provider Metadata** to first download the metadata file in XML format. The SAML application needs this information so that it can trust and process the SAML assertion that is generated by Identity Cloud Service as part of the federation process. This information includes, for example, profile and binding support, connection endpoints, and certificate information. To get the issuing Oracle Identity Cloud Service root certificate, see Obtaining the Root CA Certificate from Oracle Identity Cloud Service.

15. Click **Finish**. The application is added in a deactivated state. To activate your application, see Activating Applications.

Upgrade a SAML Application

You can upgrade your SAML application if there is any upgradable change to your application.

If your SAML application has an update, you will see the **Upgrade** button visible in the UI. Click and upgrade the application. After upgrading to a provisioning application, you need to configure the provisioning parameters and run a Full Sync similar to adding a new provisioning application.

See Adding an App Catalog Application for information on configuring the provisioning parameters.

Secure Enterprise Applications with App Gateway

In this chapter, you will learn about App Gateway, why you should use App Gateway, how to configure App Gateway, and how to secure enterprise applications using App Gateway.

Topics:

- Typical Workflow for Securing Enterprise Applications with App Gateway
- Understand App Gateway
- Secure Enterprise Applications
- How to Use App Gateway
- How to Enable and Access App Gateway Logs
- Troubleshoot App Gateway

Typical Workflow for Securing Enterprise Applications with App Gateway

You can integrate Enterprise Applications with Oracle Identity Cloud Service for authentication purposes using App Gateway. Configure both enterprise application
and App Gateway in Oracle Identity Cloud Service, learn the options you have to install App Gateway, and then test, monitor, and troubleshoot the integration.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand App Gateway</td>
<td>Understand the concepts and the architecture of this integration.</td>
<td>Understand App Gateway</td>
</tr>
<tr>
<td>Configure Enterprise</td>
<td>Understand what an enterprise application is and how to configure an</td>
<td>Configure App Gateway</td>
</tr>
<tr>
<td>Applications</td>
<td>enterprise application in Oracle Identity Cloud Service.</td>
<td></td>
</tr>
<tr>
<td>Configure App Gateway</td>
<td>Add an App Gateway in Oracle Identity Cloud Service, download the App</td>
<td>How to Use App Gateway</td>
</tr>
<tr>
<td></td>
<td>Gateway binary file from the Downloads page, install, configure, and then</td>
<td></td>
</tr>
<tr>
<td></td>
<td>start the App Gateway server.</td>
<td></td>
</tr>
<tr>
<td>Enable and Access App</td>
<td>Locate and enable App Gateway log files and log levels.</td>
<td>How to Enable and Access App Gateway</td>
</tr>
<tr>
<td>Gateway logs</td>
<td></td>
<td>Logs</td>
</tr>
<tr>
<td>Troubleshoot the</td>
<td>Learn about common problems that you might encounter when using App</td>
<td>Troubleshoot App Gateway</td>
</tr>
<tr>
<td>Integration</td>
<td>Gateways and learn how to solve them.</td>
<td></td>
</tr>
</tbody>
</table>

**Understand App Gateway**

Understand what an App Gateway is, why you should use it, and how App Gateway works to protect access to your web applications.

- **What is App Gateway?**
- **Why Should You Use App Gateway?**
- **How Does App Gateway Work?**
- **Set Up High Availability**

**What is App Gateway?**

App Gateway is a software appliance that enables you to integrate applications hosted either on a compute instance, in a cloud infrastructure, or in an on-premises server with Oracle Identity Cloud Service for authentication purposes.

App Gateway acts as a reverse proxy protecting web applications by restricting unauthorized network access to them. App Gateway intercepts any HTTP request to these applications and ensures that the users are authenticated with Oracle Identity Cloud Service before forwarding the request to these application. App Gateway propagates the authenticated user's identity to the applications.

If the user isn't authenticated with Oracle Identity Cloud Service, then App Gateway redirects the user to Oracle Identity Cloud Service's **Sign In** page for credential validation.
Why Should You Use App Gateway?

App Gateway is a non-intrusive integration method that uses a middle-tier layer to integrate web applications with Oracle Identity Cloud Service for authentication purposes.

Use App Gateway to:

• Integrate enterprise applications hosted either on-premises or in a cloud infrastructure with Oracle Identity Cloud Service for authentication purposes.

For example, if you have a web applications hosted on-premises or in a cloud infrastructure, you can integrate this application with any other cloud-based applications for single sign-on. Use App Gateway to integrate your web application with Oracle Identity Cloud Service, and then make sure that the other cloud-based applications use Oracle Identity Cloud Service as their authentication mechanism. All these applications will make use of the single sign-on provided by Oracle Identity Cloud Service.

• Expose intranet web applications to internet access.

If your web application is hosted and accessed over your intranet and you want to expose access to this application over the internet, use App Gateway to proxy any internet request and to require users to authenticate with Oracle Identity Cloud Service before accessing your intranet web application. In this case, you deploy App Gateway in your network DMZ while your application remains in the intranet zone.

• Integrate with applications that lack a native authentication mechanism and don't support SAML federation, OAuth, or OpenID Connect integration methods.

If your application doesn't support the standards for authentication that Oracle Identity Cloud Service supports (SAML, OAuth, and OpenID Connect), and you can't use Oracle Identity Cloud Service's SDKs in your application, then you can use App Gateway to integrate your web application with Oracle Identity Cloud Service.

• Integrate with applications that support the HTTP Header-based authentication.

For web applications that support HTTP Header-based authentication, the App Gateway integration method requires no change to the web application's source code. You need to configure the application's authentication policies in Oracle Identity Cloud Service to add header variables in the request before App Gateway forwards the request to the application. By doing so, the application can identify the user authenticated with Oracle Identity Cloud Service.

How Does App Gateway Work?

The App Gateway is deployed within a customer's infrastructure, regardless of whether the infrastructure is in the cloud, on-premises, or a hybrid one.

The App Gateway works as a reverse proxy, intercepting all requests from the client to the application. The App Gateway then verifies if a user is already logged in to Oracle Identity Cloud Service. If the user has logged in, then App Gateway adds header variables to the request so that the application being protected can access the header variable. The application trusts App Gateway has identified the signed in user in Oracle Identity Cloud Service values and create the user session.
Ensure that the communication between App Gateway and application is secure to avoid changes in the header variable values before the request is sent to the application.

The following steps explain the form-based authentication flow between the web browser, App Gateway, and an enterprise application:

1. In a web browser, a user requests access to an application through a URL exposed by App Gateway.
2. App Gateway intercepts the request, verifies the user doesn't have a session with Oracle Identity Cloud Service, and then redirects the user's browser to the Oracle Identity Cloud Service's Sign In page.
   In step 2, if the user has a session with Oracle Identity Cloud Service, it means that the user has already signed in to Oracle Identity Cloud Service. If so, then an access token is sent to App Gateway, and then the remaining steps are skipped.
3. Oracle Identity Cloud Service presents the Sign In page or whichever sign-in mechanism has been configured for Oracle Identity Cloud Service.
4. The user signs in to Oracle Identity Cloud Service.
5. Upon successful authentication, Oracle Identity Cloud Service creates a session for the user and issues an access token to App Gateway.
6. App Gateway uses the token to identify the user. It then adds header variables to the request and forwards the request to the application.
7. The application receives the header information, validates the user's identity, and starts the user session.

Any subsequent request to the application's protected resources is intercepted by App Gateway. App Gateway identifies the user, adds header variables to the request, and forwards the request to the application.

To sign out, the user calls an application's logout URL. The App Gateway identifies the logout URL and redirects the user to the Oracle Identity Cloud Service's OAuth logout endpoint (/oauth2/v1/userlogout). After Oracle Identity Cloud Service signs the user out, Oracle Identity Cloud Service can redirect the user's browser to a URL of the application which can then remove the application's user session.
Set Up High Availability

Use a load balancer to achieve high availability for multiple instances of App Gateway.

If high-availability is a requirement to access your web application, you can have multiple App Gateways, configure each of them to integrate with Oracle Identity Cloud Service, and use a load balancer to balance the request among the App Gateway instances.

The following architecture diagram shows the components required for high availability.

This architecture requires that you install and configure more than one instance of App Gateway. Each App Gateway instance can be configured to use the same Oracle Identity Cloud Service instance or different instances. If you use different instances of...
Oracle Identity Cloud Service, then you need to maintain the synchronization of the configurations in each Oracle Identity Cloud Service instance.

Use a load balancer to distribute request between the App Gateway instances. The load balancer must be configured with session persistence to redirect subsequent user browser requests to the same App Gateway instance for the duration of a session.

Additionally, the load balancer must perform health checks via HTTPS with HTTP keepalives enabled for a duration that exceeds the health check interval. This prevents the load balancer from redirecting browser requests to an offline App Gateway instance.

Secure Enterprise Applications

Understand what an enterprise application is and how to add an enterprise application in Oracle Identity Cloud Service.

• About Enterprise Applications
• Add an Enterprise Application

About Enterprise Applications

Enterprise applications are web applications that require App Gateway to integrate with Oracle Identity Cloud Service for authentication purposes.

To configure an enterprise application in Oracle Identity Cloud Service you need to know the following information about your web application:

• The web application’s base URL. For example, if a known URL of your application is http://myapp.internal.example.com:3266/myapp/private/home, then the base URL is http://myapp.internal.example.com:3266.

• The list of resources of your web application. For example, if your web application exposes the following URLs: functionalities A to Z in the following format /myapp/private/funcA to /myapp/private/funcZ, a home page /myapp/private/home, a logout URL /myapp/logout, an about page myapp/public/about, and an index page /myapp/index, then the list of all resources of your web application is:

  – URLs from /myapp/private/funcA to /myapp/private/funcZ
  – /myapp/private/home
  – /myapp/logout
  – /myapp/public/about
  – /myapp/index

• For each resource, define which resources require the user to be authenticated, which don't require user authentication, and which resource represents the log out action. Below are examples of authenticated and non-authenticated resources:

  – Resources from /myapp/private/funcA to /myapp/private/funcZ, and /myapp/private/home require the user to be authenticated.
  – /myapp/logout logs the user out.
  – Both myapp/public/about and /myapp/index are public resources and don't require the user to be authenticated.
• Identify URL patterns that apply to your list of resources. In the previous example, the URL pattern /myapp/private/*/ matches all the application's functionality URLs and the home page URL. All these URLs may require the same kind of authentication.

Add an Enterprise Application

Add an enterprise application to represent the web application you protect by using App Gateway.

To add an enterprise application in Oracle Identity Cloud Service, you need to configure the list of application resources (web application's URLs or URL patterns) and create an authentication policy for each resource. For each authentication policy, you define an authentication method, and header variables for App Gateway to include in the request before forwarding the request to the application.

1. Sign into the Identity Cloud Service console as an application administrator.
2. Expand the Navigation Drawer and then click Applications.
3. Click Add.
4. In the Add Application page, click Enterprise Application.
5. In the Details pane of the Add Enterprise Application page, provide a name for the application, enter the application URL, and then click the Next > icon.

Note:
The application URL is the URL that you want users to use to access your enterprise application. Use the host name and port number of the App Gateway. If you have multiple instances of App Gateway, then use the host name and port number of the load balancer.

6. In the SSO Configuration pane, click Finish.
7. Click Activate, and then click OK in the Confirmation widow to activate the application.

Configure Resources

You can create resources individually by adding one resource for each of your application's URLs, or use regular expression to create a resource which represents a collection of URLs for your application.

A resource represents a URL or URL Pattern for which you want to restrict access or intend to give anyone to access. You need the list of resources of your application. See About Enterprise Applications

1. In the Application Details page, click the SSO Configuration tab of your enterprise application page, expand the Resources section, and then click Add to add a resource.
2. In the Add Resource dialog, provide a name for the resource and the resource URL. If you want to use a regular expression as the resource URL value, then select Regex, so that App Gateway evaluates the Resource URL value as a pattern.
For example, if you want to protect the application endpoint `http://myapp.internal.example.com:3266/private/home`, you can enter `/private/home` as the value for **Resource URL**. If you want to protect any page under the `/private` folder, then enter `/private/.*` as value for **Resource URL**, and select **Regex**.

See [Use Regular Expressions](#).

**Configure an Authentication Policy**

Create an authentication policy for each resource you created for your enterprise application.

An authentication policy defines which authentication method to use to protect your enterprise application's resources, and whether App Gateway will add header variables to the request it forwards to the application.

1. In the **SSO Configuration** tab of your enterprise application page, expand the **Authentication Policy** section, and then click **Add** under **Managed Resources**.

2. In the **Add Resource** window, select the resource for which you want to configure an authentication policy from the list of resources that you created in the **Resources** section.

3. Use the following table to define the **Authentication Method** for the resource you have selected:

**Table 8-1 Authentication Methods**

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Basic Auth**           | The **Basic Auth** method performs HTTP Basic authentication. If the request doesn't contain an Authentication Basic header, then user's browser will prompt for credentials.  
                           | The credentials sent in the Authentication Basic header is validated in Oracle Identity Cloud Service.                                      |
| **Basic Auth+Logout**    | This method is used to protect the application's resource (URL) that represents the application's log out process.  
                           | When App Gateway intercepts a request to this resource, the HTTP logout process is initiated. This process deletes any HTTP session cookie created by the **Basic Auth+Session** authentication method.  
                           | After the logout process finishes, App Gateway forwards the user browser to the requested application's resource.  
                           | Note that the HTTP logout process doesn't clear any credentials cached by the browser in the current browser session and then the user may not be prompted again for later requests. |
| **Basic Auth+Session**   | Works the same as **Basic Auth**. After the credential is validated, it creates an HTTP session cookie (ORA_OCIS.CG_BA_SESSION).             |
### Table 8-1 (Cont.) Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Form or Access Token  | In this authentication method, App Gateway delegates credentials collection and validation to Oracle Identity Cloud Service.  
If an Authorization Bearer header is present in the request, then the authentication is similar to a resource server flow. If a user-agent header is present, then a user browser flow takes place.  
The user browser flow redirects the user browser to Oracle Identity Cloud Service for credentials collection and validation, and then creates an OAuth session cookie (ORA_OCIS.CG_SESSION_*).  
If an Authorization session header is present in the request and the OAuth session cookie is missing or invalid, then the usual OAuth login flow is suppressed and a 401 HTTP error code will be returned along with a WWW-Authenticate: Bearer error="invalid_session" header. This is used by applications that may trigger an unwanted login when their requests contain a user-agent header, but not an Authorization Bearer header, allowing them to handle re-authentication themselves. |
| Form+Logout           | This method is used to protect the application's resource (URL) that represents the application's log out process.  
This resource's URL doesn't need to be exposed by the application, as App Gateway redirects the user browser to Oracle Identity Cloud Service's OAuth logout endpoint (/oauth2/v1/userlogout), instead of forwarding the request to the application URL.  
In the Add Resource window, the Post-Logout URL is the URL which Oracle Identity Cloud Service redirects the user browser after signing the user out. You can also provide a Post-Logout State parameter value to be used by the post-log out URL page of the application. |
| Multitoken            | Performs authentication based on the contents of the Authorization header of the request:  
• If the request contains an Authorization Basic header, then App Gateway handles this authentication as Basic Auth.  
• If the request contains an Authorization Bearer or Authorization Session header, App Gateway handles this authentication as Form or Access Token.  
• If the Authorization header is missing or has any other value, then a 401 Unauthorized HTTP error is returned. |
### Table 8-1  (Cont.) Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multitoken+Fallthrough</td>
<td>Same as Multitoken, but if the Authorization header is not Basic, Bearer, or session, then instead of presenting the 401 Unauthorized HTTP error, the request is forwarded to the application as if the authentication method was Public. The application must understand the Authorization header and perform its own authentication using the header information.</td>
</tr>
</tbody>
</table>
| Anonymous                     | • If a valid OAuth session cookie is present, then the headers configured in the authentication policy are added to the request and the request is forwarded to the application.  
  • If the OAuth session cookie is missing or expired, works the same as the Public authentication method. In this case, a REMOTE_USER header with value anonymous is added to the request.  
  For both options, the headers configured in the authentication policy are added to the request, but authentication is not performed. |
| Public                        | No authentication is performed. The request is forwarded to the application as is.                                                                                                                                                  |
| Unsupported                   | This method always returns 500 Not Supported HTTP error code. For example, you can use this method to disable access to a protected URL that is available in the application but you don't want users to access it.                                      |

4. The authentication method you selected in the previous step is valid for all HTTP Methods (GET, HEAD, DELETE, PUT, OPTIONS, CONNECT, POST, or PATCH). If you want to specify different authentication methods for HTTP methods (for example, the Form + Access Token authentication method for the GET HTTP method and the Multitoken authentication method for the POST HTTP method), then you can do so by using the Authentication Method Overrides menu. Select the HTTP Method, and then the Authentication Method you want. If you need to override more than one HTTP method, then repeat this step multiple times.

5. If you want to add an header variable to the request so that App Gateway forwards it to the application, click the plus + icon for Headers, and then provide the name and value for the header variable. To add more than one header variable, click the + icon for Headers multiple times.

For example, let's suppose the application requires a header variable named USERLOGGEDIN to be present in every request so that the applications knows the ID of user signed in to Oracle Identity Cloud Service. You need to add one header variable, enter USERLOGGEDIN for the Name field, and $subject.user.userName for Value.
In the **Configure Authentication Policy for this application** section, confirm that **Require Secure Cookies** is selected. This flag sets the secure header to avoid cookies being used in non-secure HTTP communication.

For security reasons, make sure the **Disable Audience Validation** check box isn't selected. The audience validation check box is used to ensure the token has been issued by App Gateway's known issuer, in this case Oracle Identity Cloud Service. If you disable audience validation, App Gateway won't validate the audience of the token, which makes the application vulnerable to attacks.

### Use Regular Expressions

Use regular expressions (regex) to define a URL pattern which represents more than one URL of your enterprise application and for which you can apply the same authentication policy.

You need a list all the URLs for your application to define URL patterns that map similar URLs.

**Example 8-1  Use of Regular Expression**

For example, if you want to allow only authenticated users access for any page of the application that starts with `my` and are under the path `/mybank`, then you can use the regular expression `/mybank/[^/]*`

The URLs `/mybank/myCredits` and `/mybank/myDebits` fall into that pattern, but `/mybank/about` doesn't.

### Supported Header Value Expressions

You can configure App Gateway to dynamically forward generated header values to the application instead of only static values.

In the header **Value** field you can provide a simple literal string or an attribute identifier. If you use an attribute identifier, App Gateway attempts to replace the attribute identifier by the value of the attribute.

The following types of attribute identifiers are supported:

- **Application**: This attribute identifier accesses the information of the enterprise application registered in Oracle Identity Cloud Service.
  
  **Format**: `$subject.client.<attr>`

- **User**: This attribute identifier accesses information of the user signed in to Oracle Identity Cloud Service.
  
  **Format**: `$subject.user.<attr>`

- **Request**: This attribute identifier accesses request information.
  
  **Format**: `$request.<attr>`
For user attribute scope, App Gateway supports any simple top-level attribute in the JSON Response from `/admin/v1/Users` such as `string`, `boolean`, or `int` values.

**Table 8-2  User Attribute Scope Names and Return Values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Header Value Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>$subject.user.name</td>
<td>The user's user name.</td>
</tr>
<tr>
<td>emails</td>
<td>$subject.user.emails</td>
<td>The user's primary email address.</td>
</tr>
<tr>
<td>phoneNumbers</td>
<td>$subject.user.phoneNumbers</td>
<td>The user's phone number.</td>
</tr>
<tr>
<td>addresses</td>
<td>$subject.user.addresses</td>
<td>The user's mailing address.</td>
</tr>
<tr>
<td>groups</td>
<td>$subject.user.groups</td>
<td>The groups to which the user is assigned to through direct membership, nested groups, or dynamically calculated membership.</td>
</tr>
<tr>
<td>idcsCreatedBy</td>
<td>$subject.user.idcsCreatedBy</td>
<td>The display name of the user or application who created this resource.</td>
</tr>
<tr>
<td>idcsLastModifiedBy</td>
<td>$subject.user.idcsLastModifiedBy</td>
<td>The display name of the user or application who modified this resource.</td>
</tr>
</tbody>
</table>

**Example of supported values for request attribute scope:**

**Table 8-3  Request Attribute scope names and supported values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Header Value Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy_appname</td>
<td>$request.policy_appname</td>
<td>Returns the name of the enterprise application registered in Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>policy_name</td>
<td>$request.policy_name</td>
<td>Returns the policy name of the specific policy matched for the request.</td>
</tr>
</tbody>
</table>
| policy_res       | $request.policy_res              | Returns the resource URL pattern matched for the request. The format is: "<type>:<pattern>"  
Example: text:/my/resource or regex:/my/resource/.*  
| policy_action    | $request.policy_action           | Returns the HTTP Method (GET, POST, etc) used to access the requested resource. |
| res_host         | $request.res_host                | Returns the host name from the original Request.                            |
| res_port         | $request.res_port                | Returns the port number from the original Request.                          |
| res_type         | $request.res_type                | Returns the protocol (HTTP or HTTPS) of the original Request.               |
| res_url          | $request.res_url                 | Returns the full requested URL.                                             |
How to Use App Gateway

Use the Identity Cloud Service console to register an App Gateway and download the App Gateway binary file. Then install and configure the App Gateway server.

Register an App Gateway

Before installing the binary file for App Gateway that appears on the Downloads page, you must register your App Gateway using Identity Cloud Service console.

To register an App Gateway you must add hosts and associate each host to an enterprise application your App Gateway will protect:

• In the Hosts pane, you define host identifiers. Each host identifier represents a domain name and port number App Gateway uses to proxy an enterprise application.
• In the Apps pane, you associate an enterprise application with a host identifier.

To register an App Gateway, you must be assigned to either the Identity Domain Administrator role or the Security Administrator role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, click App Gateways, and then click Add.
2. In the Details pane, specify the name of your App Gateway, and then click Next (>).
3. In the Hosts pane, click Add.
4. In the Add Host dialog, provide a name in the Host Identifier field.
5. Enter the Host and Port values that the App Gateway server will respond to HTTP requests.

   The port number you provide in this step is used by the App Gateway server to respond to HTTP requests.
6. To have your App Gateway listen to HTTP requests in secure mode (HTTPS), select the SSL Enabled check box. Otherwise, clear this check box and your App Gateway will listen to non-secure HTTP requests only.
7. If you select the SSL Enabled check box, then populate the Additional Properties text area with the following values to specify the certificate key pair the App Gateway server will use, protocols and ciphers for SSL:

   ```
   ssl_certificate /usr/local/example.com.rsa.crt;
   ssl_certificate_key /usr/local/example.com.rsa.key;
   ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
   ssl_ciphers HIGH:!aNULL:!MD5;
   ```

   The /usr/local/example.com.rsa.crt is the full path of a certificate file in the App Gateway server. The /usr/local/example.com.rsa.key is the secret key of that certificate file. You must upload both files to the App Gateway server after you install the App Gateway binary file.
8. In the Add Host dialog, click Save.
9. In the Hosts pane, click Next >.
10. In the Apps pane, click Add.

11. In the Assign an App to Gate dialog, map App Gateway to an enterprise application using the values below, and then click Save.

   - **Application**: Select the enterprise application you want to protect using this App Gateway.
   - **Select a Host**: Select the host identifier associated with the application you selected.
   - **Resource Prefix**: Enter the URL prefix used by App Gateway to proxy the enterprise application.
   - **Origin Server**: This is the actual base URL where the application is hosted. If the application is not directly accessible, but accessible through a web proxy, then enter the URL of the web proxy. See example diagram below.
   - **Additional Properties**: If the application is accessible through a web proxy, then enter the values below:

```
proxy_pass_header on;
proxy_set_header host "myapp.internal.example.com";
```

   where "myapp.internal.example.com" is the domain name where the application is hosted.

The following figure provides examples of the mappings that you're configuring between App Gateway and your enterprise application:

12. Click Finish.

13. In the App Gateway Details page, note the value of the **Client ID**.

14. Click **Show Secret** and note the value of the **Client Secret**.

   The **Client ID** and **Client Secret** are equivalent to a credential (for example, an ID and password) that your App Gateway server uses to communicate with Oracle Identity Cloud Service. You'll need these values when you configure the App Gateway server.

15. In the Navigation Drawer, click App Gateways.

16. In the App Gateways page, select your App Gateway, click **Activate**, and then click OK in the **Confirmation** window to activate your App Gateway.
Download and Extract the App Gateway Binary File

The App Gateway binary file you download from Identity Cloud Service console is a compressed (.zip) file. This file contains an Open Virtual Appliance (.ova) file which you use to install the App Gateway server.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Downloads.
2. In the Downloads page, click Download to the right of App Gateway for Identity Cloud Service.
3. Verify that a Success status appears to the right of App Gateway for Identity Cloud Service.
4. Extract the content of the zip file you downloaded to a location on your desktop. For Example, c:\temp.

The c:\temp\app-gateway-<version>.ova file will be created.

Note:
The App Gateway for Identity Cloud Service doesn't replace the App Gate for Identity Cloud Service. The App Gateway for Identity Cloud Service software is based on NGINX web server and is used to protect access of enterprise applications. The App Gate for Identity Cloud Service software is an OEM product that has similar but not the same features.

Install App Gateway

Use the App Gateway Open Virtual Application (ova) file to install the App Gateway server. You can run the server in a compute instance on Oracle Cloud Infrastructure or in a virtual machine hosted in your network environment.

To install the App Gateway server, see the following topics:

• Install App Gateway on Oracle Cloud Infrastructure
• Install App Gateway Using Oracle VM Virtual Box Software

Install App Gateway on Oracle Cloud Infrastructure

To install App Gateway on Oracle Cloud Infrastructure, you need to upload the App Gateway virtual disk image file to a Bucket in Oracle Cloud Infrastructure, create a Custom Image using the App Gateway virtual disk image file, and then create a Compute instance based on this custom image.

• Upload the App Gateway Virtual Machine Disk Image File to Oracle Cloud Infrastructure
• Create a Custom Image in Oracle Cloud Infrastructure Based on the App Gateway Virtual Machine Disk Image File
• Create a Compute Instance Using App Gateway's Custom Image

Upload the App Gateway Virtual Machine Disk Image File to Oracle Cloud Infrastructure
Before creating a compute instance on Oracle Cloud Infrastructure to run App Gateway, you need to create a Virtual Machine Disk Image (VMDK) file using the App Gateway Open Virtual Appliance (OVA) file, and then upload this VMDK file to Oracle Cloud Infrastructure.

To create the VMDK file, follow the procedure to import the App Gateway’s Open Virtual Appliance (OVA) file using Oracle VM Virtual Box software, but don’t start the machine or configure port forward rule for it. See Import the Open Virtual Appliance Image File in Virtual Machine Software.

1. Sign in to Oracle Cloud.
2. In the Oracle Cloud console, expand the Navigation Drawer, move the mouse over Object Storage, and then click Object Storage.
3. In the Object Storage page, click the name of a bucket in your compartment to upload the image. If there aren't buckets available, click Create Bucket, click Create Bucket in the Create Bucket dialog, and then click the name of the bucket you created.

   Contact your Oracle Cloud Infrastructure administrator for more information about which compartment to create buckets.

4. On the Bucket Detail page, click Upload Object in the Objects section.
5. Click select files to browse and open the App Gateway’s VMDK file, and then click Upload Objects.
6. After the file uploads, click Close.
7. Click the menu on the right for your object entry, and then record the URL Path (URI) value.

Create a Custom Image in Oracle Cloud Infrastructure Based on the App Gateway Virtual Machine Disk Image File

To create a compute instance on Oracle Cloud Infrastructure to run App Gateway, you need to create a custom image from the App Gateway’s Virtual Machine Disk Image (VMDK) file you uploaded to a bucket on Oracle Cloud Infrastructure.

Make sure your Oracle Cloud Infrastructure account has compartments, a virtual cloud network, and subnets previously set up.

Make sure you have selected a compartment in Oracle Cloud console, before proceeding.

Note:
The components design should align with your Oracle Cloud Infrastructure operational model. Contact your Oracle Cloud Infrastructure administrator for more information.

1. In the Oracle Cloud console, click the top-left menu, mouse over Compute, and then click Custom Images.
2. In the Images page, select the same compartment where you uploaded your VMDK file, and then click Import Image.
3. In the Import Image dialog box, enter or select the following values, and then click Import Image.
• **CREATE IN COMPARTMENT**: Select the compartment to import the image. The compartment must be the same where your compute instance will be created.

• **NAME**: App Gateway Custom Image

• **OPERATING SYSTEM**: Select Linux.

• **OBJECT STORAGE URL**: Enter the URL path you recorded after you uploaded the VMDK file.

• **IMAGE TYPE**: Select VMDK.

• **LAUNCH MODE**: Select EMULATED MODE.

Wait until the custom image creation finishes.

Create a Compute Instance Using App Gateway's Custom Image

After you uploaded the App Gateway's Virtual Machine Disk Image (VMDK) file to a bucket in Oracle Cloud Infrastructure and created a custom image using this VMDK file, you can create a compute instance to run App Gateway.

1. In the Oracle Cloud console, click the top-left menu, mouse over Compute, and then click Instances.

2. In the Instances page, click Create Instance.

3. In the Create Compute Instance page, enter My App Gateway Server in the Name your instance field, and then click Change Image Source.

4. In the Browse All Images dialog, click Custom Images, select the appropriate compartment, select App Gateway Custom Image, and then click Select Image.

5. In the Add SSH Key section, add a public SSH key, by either uploading a public key file or pasting the public key value in the SSH Key field.

See Creating an SSH Key Pair Using PuTTY Key Generator section in Managing Key Pairs on Linux Instances.

6. In the Configure networking section, select a compartment in Virtual cloud network compartment.

If your compartment doesn't have virtual cloud network configured, then enter App Gateway VNC as Name in the New virtual cloud network section. If your compartment has virtual cloud network configured, then select the values for Virtual cloud network, Subnet compartment, and Subnet in which your compute instance will be created.

7. Click Create, and wait until your compute instance is provisioned and running.

8. Record the value of the Public IP Address assigned to this compute instance.

Make sure that you have a Security List configured so that you can connect to the My App Gateway Server compute instance using a SSH client software such as PuTTY. Contact your Oracle Cloud Infrastructure administrator for more information.

---

**Note:**

The component design should align with your Oracle Cloud Infrastructure operational model. Contact your Oracle Cloud Infrastructure administrator for more information.
Install App Gateway Using Oracle VM Virtual Box Software

To install App Gateway using Oracle VM Virtual Box, import the App Gateway Open Virtual Appliance (OVA) file in a Oracle VM Virtual Box, and then configure the App Gateway virtual machine to receive HTTP request.

- Import the Open Virtual Appliance Image File in Virtual Machine Software
- Configure Port Forwarding Rules

Import the Open Virtual Appliance Image File in Virtual Machine Software
To run App Gateway in a virtual machine, import the App Gateway Open Virtual Appliance (OVA) image file in virtual machine software such as Oracle VM Virtual Box.

The following procedure requires access to a Windows server as administrator. This server must have Oracle VM Virtual Box software installed.

1. Log in to the Windows server, and upload the App Gateway OVA file from your desktop to a working folder in the server. For example, c:\temp. See Download and Extract the App Gateway Binary File.

2. Launch the Oracle VM Virtual Box Manager software, and then select Import Appliance from the File menu.

3. Locate the OVA file on the Windows server, and then click Next.

4. In the Import Virtual Appliance window, update the Name field with the value App Gateway Server.

5. To define a new MAC address to the App Gateway server network component, select Reinitialize the MAC address of all network cards.

6. Click Import.

7. Verify App Gateway server is listed in the Oracle VM Virtual Box Manager.

After you import App Gateway, a virtual disk image file (VMDK) will be created in the Windows server.

To locate this file, select App Gateway Server in Oracle VM Virtual Box Manager, click Settings, click Storage, and then click the name that appears under Controller: SATA in the Storage Devices section. The location of the VMDK file appears in the Location field under Information.

Configure Port Forwarding Rules
Create a port forwarding rule to allow the requests received by the Windows server hosting the App Gateway virtual machine to be forwarded to the App Gateway server.

1. In the Oracle VM Virtual Box Manager software, select the App Gateway server, and then click Settings.

2. Select Network on the left menu, expand Advanced, and then click Port Forwarding.

3. In the Port Forwarding Rules window, click , configure a rule to forward the requests from the host port to the guest port, and then click OK.

For example, if your App Gateway is configure to use port 4443, then enter 4443 in both Host Port and Guest Port columns.
The port number must be the same as the port value that you provided during App Gateway registration.

4. In the Port Forwarding Rules dialog box, click OK.
5. In the App Gateway Settings dialog box, click OK.
6. Select the App Gateway server, and then click Start.

Configure, Start, and Test App Gateway

After you install App Gateway, you need to configure the App Gateway server to communicate with Oracle Identity Cloud Service. Learn how to start and stop the server, and then test the enterprise application protected by App Gateway.

- Configure the App Gateway Server
- Start and Stop App Gateway
- Test Access to Your Application Using App Gateway

Configure the App Gateway Server

Before you start the App Gateway server for the first time, you need to configure the server to connect with Oracle Identity Cloud Service.

1. Use a SSH client such as PuTTY and the following credentials to log in to the App Gateway server.
   - Localhost login: oracle
   - Password: cloudgateR0X!
     You are required to change the provisioned password on the first login.

2. Execute the `ping <idcs-tenant>.identity.oraclecloud.com` command to verify if the App Gateway server can reach the Oracle Identity Cloud Service instance.

3. If ping command fails, then execute the following procedure:
   a. Execute the `sudo su -` command to login as root, and the provide the oracle password when prompted.
   b. Execute the `vi /etc/hosts` command, and then add an entry to map your Oracle Identity Cloud Service host name if it isn't publicly available. For example: `<your_identity_cloud_service_ip> idcs-tenant.identity.oraclecloud.com`
   c. Execute the `vi /etc/hosts` command, and then add an entry to map your Oracle Identity Cloud Service host name if it isn't publicly available. For example: `<your_identity_cloud_service_ip> idcs-tenant.identity.oraclecloud.com`
   d. Execute the `vi /etc/resolv.conf` command, and then add a nameserver entry to configure the Virtual Machine as a nameserver. For example: `nameserver 127.0.0.1`

   This is necessary because App Gateway makes HTTP requests to itself.
e. Install and start `dnsmasq` on the App Gateway server using the following command lines:

   ```
   yum install dnsmasq
   chkconfig dnsmasq on
   service dnsmasq start
   ```

f. Install `telnet` by running the following command:

   ```
   yum install telnet
   ```

g. Run the following `telnet` command and try to establish a connection to your Oracle Identity Cloud Service instance and your application from the App Gateway server.

   ```
   telnet <idcs-tenant>.identity.oraclecloud.com 443
   ```

   If `telnet` can't connect to your Oracle Identity Cloud Service, then contact your network administrator to apply any other network configuration to enable the App Gateway server to establish connection with your Oracle Identity Cloud Service instance.

h. Execute the `exit` command, to log out from root account.

4. Navigate to the `/scratch/oracle/cloudgate/ova/bin/setup` folder, and then edit the `cloudgate-env` file present in this folder (vi `cloudgate-env`).

5. Enter values for the following parameters, and then save the file:
   - **IDCS_INSTANCE_URL**: The URL of your Oracle Identity Cloud Service instance.
     For example, `https://idcs-123456789.identity.oraclecloud.com`
   - **CG_APP_TENANT**: The tenant name of the Oracle Identity Cloud Service instance.
     For example, `idcs-123456789`
   - **CG_APP_NAME**: The client ID value you made note during the App Gateway registration in Identity Cloud Service console.
   - **CG_APP_SECRET**: The client secret value you made note during the App Gateway registration in Identity Cloud Service console.

6. In the `/scratch/oracle/cloudgate/ova/bin/setup` folder, execute `./setup-cloudgate` command.

7. When prompted, enter `y` to proceed with the configuration.

   App Gateway service and agent service will start after the configuration finishes.

Start and Stop App Gateway

Use the following scripts to start and stop App Gateway.

- Use a Terminal window to run the following command on the App Gateway server to start App Gateway:

  ```
  /scratch/oracle/cloudgate/home/bin/cg-start
  ```
To stop App Gateway, run the following command:

```
/scratch/oracle/cloudgate/home/bin/cg-stop
```

When you start App Gateway, App Gateway contacts Oracle Identity Cloud Service to retrieve the port number you configured during the App Gateway registration. The App Gateway server starts using this port number.

To check the running status of the App Gateway server, run the following command:

```
/scratch/oracle/cloudgate/home/bin/cg-status
```

Test Access to Your Application Using App Gateway

After you configure the App Gateway server to communicate with your Oracle Identity Cloud Service instance, and start the server, test access to your enterprise application.

The following diagram provides an example of how App Gateway and Oracle Identity Cloud Service interact when an HTTP request to an application resource is sent by the user browser through App Gateway.

Because App Gateway proxies your web application, use the App Gateway base URL to access the application instead of the application actual URL.

Figure 8-3  Workflow of protecting an application using App Gateway

1. Open a new web browser and access your application using the App Gateway URL.
   
   In this example, the URL is: https://myappgateway.example.com:4443/myapp/private/home
   
   The actual application https://myapp.internal.example.com:3266/myapp/private/home isn't accessible by the user browser.
2. App Gateway intercepts the request and communicates with Oracle Identity Cloud Service to verify if the URL corresponds to an enterprise application.

   In this example, My Enterprise Application is registered, and the authentication policy for this enterprise application is Form or Access Token.

3. App Gateway verifies the request contains a valid Oracle Identity Cloud Service's access token in the Authorization Bearer header or Oracle Identity Cloud Service's session cookie, indicating the user has already signed in to Oracle Identity Cloud Service.

4. If the user hasn't signed in to Oracle Identity Cloud Service, then App Gateway redirects the user browser to Oracle Identity Cloud Service Sign In page.

5. If the user has signed in, then App Gateway adds header variables and a cookie to the request, and then forwards the request to the application.

   The application receives the request, uses the header variables to identify the user and to present the content of the /myapp/private/home page.

How to Enable and Access App Gateway Logs

App Gateway provides log files to help you monitor App Gateway's behavior. Learn how to configure and access these log files.

- Configure App Gateway Logs
- View App Gateway Logs

Configure App Gateway Logs

Enable App Gateway log files and configure logging levels.

To disable logs or change the log levels of the App Gateway server, login to the server, edit the /usr/local/nginx/conf/cloudgate.config file, and then under the general section, change the value of the logLevel attribute, and then save the file.

The following are default values for App Gateway:

```
"general":{
   "disableAuthorize":false,
   "logLevel":"warn",
   "logFolder":"
   "policyMode":"gateway",
   "policyRefreshTime":300,
   "policyStaleTime":3600,
   "policyExpiryTime":604800
}
```

Note:

Values for the logLevel attribute are: off | crit | security | config | fail | warn | info | trace1 | trace2 | trace3.
By Default, the log files are located in the /usr/local/nginx/logs folder. If you want to change the default log folder, then update the value of the logFolder attribute under the general section of the /usr/local/nginx/conf/cloudgate.config file.

To change the log level for the agent service of the App Gateway, modify the /usr/local/nginx/conf/cloudgate.config file, and set the logLevel and logFolder attributes under the agentConfig section as follows:

For example, to change the log level to trace3 and the log folder to /tmp, update the /usr/local/nginx/conf/cloudgate.config file with the following values, and then save the file.

"agentConfig":{
  "pollIntervalSecs":60,
  "daemon":true,
  "logFolder":/tmp,
  "logLevel":"trace3"
}

The log level and log folder changes takes effect next time you start App Gateway. See Start and Stop App Gateway.

View App Gateway Logs

Learn about the different log files App Gateway uses.

App Gateway is based on a NGINX Server. The following NGIX native log files are located in the /usr/local/nginx/logs/ directory:

Table 8-4   NGINX Native Log Files

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access.log</td>
<td>NGINX Native access log contains information about all HTTP requests received by NGINX, and by App Gateway.</td>
</tr>
<tr>
<td>error.log</td>
<td>NGINX Native debug log.</td>
</tr>
<tr>
<td>nginx.pid</td>
<td>Contains the NGINX Server process ID number.</td>
</tr>
</tbody>
</table>

The following App Gateway specific log files are located in the /usr/local/nginx/logs/ directory:

Table 8-5   App Gateway Log Files

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cg-trace-main.log</td>
<td>App Gateway main log file.</td>
</tr>
<tr>
<td>cg-trace-policy.log</td>
<td>Logs information about a policy refresh, when App Gateway contacts Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>cg-trace-session.log</td>
<td>Logs information about the sessions created and handled by App Gateway.</td>
</tr>
</tbody>
</table>
Table 8-5  (Cont.) App Gateway Log Files

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cg-trace-token.log</td>
<td>Logs information about the access tokens received by App Gateway.</td>
</tr>
<tr>
<td>cg-trace-agent.log</td>
<td>Agent logging file.</td>
</tr>
<tr>
<td>cg-trace-init.log</td>
<td>Contains information about the initialization process.</td>
</tr>
</tbody>
</table>

Troubleshoot App Gateway

Learn about common problems that you might encounter when setting up App Gateway and how to solve them:

- **I Made Changes in Oracle Identity Cloud Service but the App Gateway Server Doesn't Reflect the Changes**
  
  Changes you make to enterprise application and App Gateway definitions in Oracle Identity Cloud Service may not be get reflected immediately on App Gateway because App Gateway caches Oracle Identity Cloud Service information, such as resources and authentication policies of enterprise applications.

  **Explanation:** App Gateway contacts Oracle Identity Cloud Service using an agent to collect host and port information. When you start App Gateway, its NGINX server is automatically configured with this information. Any changes to Oracle Identity Cloud Service is periodically polled by the agent.

  If you want the changes to be reflected immediately, restart the App Gateway server. See [Start and Stop App Gateway](#).

- **Error Log Files Contain Invalid_session Message**
  
  When App Gateway can't communicate correctly with Oracle Identity Cloud Service, you'll find *invalid_session* messages in the App Gateway error log files.

  The following is an example of an *invalid_session* messages in error.log:

  ```
  www-authenticate: Bearer error="invalid_session",
  error_description="Authentication Failure"
  ```

  This can be because of the way App Gateway processes a client request to a protected resource. App Gateway uses NGINX sub requests to make requests to Oracle Identity Cloud Service, and then App Gateway requires Linux NGINX resolver to be configured appropriately to allow these sub requests to function correctly.
1. Verify that the resolver setting in the file `/usr/local/nginx/conf/nginx-cg-sub.conf` is set to the correct IP.

2. Verify that the tenant name in `/usr/local/nginx/conf/cloudgate.config` file is configured correctly.

Error Log Files Contain GET 127.0.0.1:53 Command Responding Error Number 500

Because App Gateway makes sub requests to an internal servlet, App Gateway requires your virtual machine to listen to port 53.

The App Gateway server must communicate to itself through IP address 127.0.0.1 and port 53.

If you're running App Gateway in a virtual machine software, configure port forward for this port from the host to the guest. See Configure Port Forwarding Rules

About the App Catalog Application

Learn how to create an App Catalog application, enable provisioning and synchronization, import, and synchronize user accounts in this section. The App Catalog is a collection of partially configured application templates for popular Software as a Service (SaaS) applications, such as Amazon Web Services and Google Suite. Using the templates, you can define the application, configure SSO, and configure provisioning.

Topics:

- Add an App Catalog Application
- Enable Provisioning for an App Catalog Application
- Enable Synchronization for an App Catalog Application
- Import User Accounts from a Software as a Service Application
- Synchronize User Accounts
- Work with the Synchronization Failure Report

Add an App Catalog Application

Oracle creates and maintains the App Catalog, which is a collection of application templates, for you and provides step-by-step instructions on how to configure most of the popular Software as a Service (SaaS) applications, such as Amazon Web Services and Google Suite.

See Oracle Identity Cloud Service - Application Catalog to find the runbook for your application.

To add an App Catalog application:

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.

2. Click Add.

3. In the Add Application window, click App Catalog.
4. Locate an application by choosing a **Category** (predefined by Oracle), searching for the application by entering a string that begins with the application name, or to see all applications, click **All**.

5. Click **Add**.

6. Complete the **App Details** by entering a **Name**, **Description**, and **Application URL**.

   **Note:**
   For applications with lengthy names, the application name appears truncated in the **My Apps** page. Consider keeping your application names as short as possible.

7. In the **Custom Error URL** field, enter the error page URL to which a user has to be redirected, in case of a failure. This is an optional field. However, if not specified, the tenant specific Error page URL will be used. If both the error URLs are not configured, then the error will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error).

   When a user tries to use social authentication (ex: Google, Facebook, and so on) for logging into Oracle Identity Cloud Service, the callback URL must be configured in the Custom Error URL field. Social providers need this callback URL to call Oracle Identity Cloud Service and send the response back after social authentication. The provided callback URL is used to verify whether the user exists or not (in the case of first time social login), and display an error if the social authentication has failed.

8. In the **Linking callback URL** field, enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. This is an optional field.

   When you create a custom app using Oracle Identity Cloud Service custom SDK and integrate with Oracle Identity Cloud Service Social Login, the custom app needs to have the Linking callback URL which can be redirected after linking of the user between social provider and Oracle Identity Cloud Service is complete.

9. In the **Tags** section, click **Add Tag** to add tags to your App Catalog application to organize and identify it. See **Adding Tags to an Application**.

10. In the **Display Settings** section, select **Display in My Apps**.

   **Important:**
   If you do not select **Display in My Apps**, the application does not display in the **My Apps** page.

   When you select the **Display in My Apps** check box in applications, the app is then visible in the **My Apps** page, but selecting this check box doesn't enable or disable SSO to the app.

   The flag to enable or disable SSO comes from the app template. Use the Oracle Identity Cloud Service REST APIs to update this flag. You cannot set the SSO flag from the UI. See REST API for Oracle Identity Cloud Service.
11. Select the **User can request access** check box, if you want the app to be listed in the **Catalog**. This option allows end users to request access to applications from their **My Apps** page by clicking **Add** and then selecting the app from the **Catalog**. Don’t forget to activate the application so that users can request access.

12. Click **Next** and complete the **SSO Configuration**.

   - Click **Download Signing Certificate** to import the Oracle Identity Cloud Service signing certificate into your application. This certificate is used by the SAML application to verify that the SAML assertion is valid.

   - Click **Download Identity Provider Metadata** to import the Oracle Identity Cloud Service Identity Provider metadata into your application. The SAML application needs this information so that it can trust and process the SAML assertion that is generated by Oracle Identity Cloud Service as part of the federation process. This information includes, for example, profile and binding support, connection endpoints, and certificate information.

To get the issuing Oracle Identity Cloud Service root certificate, see **Obtaining the Root CA Certificate from Oracle Identity Cloud Service**.

13. Click **Finish**. The application has been added in deactivate state. To activate your application see **Activating Applications**.

14. Click **Applications**, locate the application that you just added, and activate it.

15. Select the application.

16. To assign users to the application, click **Users**.

The applications you assign to the user display on the **My Apps** page. Newly assigned applications and applications that a user has not yet accessed appear first in the application list and have an asterisk icon in the application tile. The icon appears on the tile until the user accesses the application.

### Enable Provisioning for an App Catalog Application

User provisioning and synchronization are an important aspect of application management. Provisioning allows you to manage the lifecycle of accounts in applications like creating and deleting accounts using Oracle Identity Cloud Service. For example, when you grant the user access to an application such as Google Suite, then this user account is automatically created in Google Suite. This allows you to quickly add new users to multiple applications and de-provision users from those applications instantly when they change roles or leave your organization.

You can enable and configure provisioning for App Catalog applications either when adding the app or later when modifying it. When you enable provisioning by selecting the option, the following steps appear:

1. **Configure Connectivity**

   Configure your app connectivity by providing values for the respective fields and by testing connectivity.

2. **Configure Attribute Mapping**

   Using **Attribute Mapping** you can map Oracle Identity Cloud Service attributes to the attributes in your application account. You can verify the existing default mapping and, if necessary, change mappings by selecting appropriate values from the drop-down list for the required user attribute. You can add rows to map missed attributes and delete rows to exclude duplicate attribute mapping. To add a new
attribute for provisioning, click **Add Row**, specify the attributes in the **User** and your application account columns, and then click **OK**. For example, if you want to add the **External ID** field, enter $(user.externalId) in the **User** column, and then select the corresponding field from the drop-down list in the applications account column.

---

**Note:**

As a best practice, don’t share allowed values between app templates. There must be a one-to-one mapping between an app template and an allowed value, since an associated allowed value is deleted when an app template is deleted.

---

3. **Select Provisioning Operations**

Any app that supports provisioning and synchronization can be an authoritative app. If authoritative sync is configured, using Oracle Identity Cloud Service, you can automatically create, modify, delete, and activate or disable users based only on the corresponding data from the authoritative application. However, the regular provisioning operations are not allowed while authorization sync is enabled.

When authoritative sync is enabled, the following actions happen automatically:

- If a user is not present in Oracle Identity Cloud Service, then the user is automatically created.
- If an authoritative synced user is deleted from the application, then the user is also deleted from Oracle Identity Cloud Service.
- If attributes of an authoritative synced user are modified, then the attributes for the user are also modified in Oracle Identity Cloud Service.

When **Authoritative Sync** is enabled, then the provisioning operations aren’t permitted from Oracle Identity Cloud Service to the target application. To manage user accounts in the application using provisioning, clear the **Authoritative Sync** check box. The following provisioning operations appear:

- **Create Account**: Select to create an account when the app is granted to the user.
- **De-activate Account**: Select to disable this account. To activate the account, clear the check box.
- **Delete Account**: Select to delete the account in the app when the Oracle Identity Cloud Service user is deleted.

---

**Important:**

When you configure the connection between your app and Oracle Identity Cloud Service, check and verify any pre-filled user name and password field entries as these may not be the credentials to access your application.

---

To configure provisioning and synchronization for your application, follow the specific runbook for the application. See Oracle Identity Cloud Service - Application Catalog. After you have enabled Provisioning, you can perform the following actions:
• Assign users or groups to your App Catalog application to start the user provisioning process for your application. See Assigning Users to Custom Applications and Assigning Groups to Custom Applications.

• Enable and configure synchronization. To enable and configure synchronization, see Enable Synchronization for an App Catalog Application.

Enable Synchronization for an App Catalog Application

User provisioning and synchronization is an important aspect of application management. After enabling provisioning, synchronization allows you to control how operations like creating and deleting accounts in Software as a Service (SaaS) applications are reflected in Oracle Identity Cloud Service.

You can enable and configure synchronization for App Catalog applications either when adding the app or later when modifying it. Be aware that you can only enable synchronization after enabling provisioning. To enable provisioning, see Enabling Provisioning for an App Catalog Application. Follow the runbook for your specific SaaS app to enable and configure synchronization.

To enable and configure synchronization:

1. If not already there, click Applications and then the name of the SaaS app that you want to configure.

2. Click the Provisioning tab.

3. Click the Enable Synchronization switch.

4. In the Configure Synchronization section, modify the attributes following the runbook for your specific SaaS application.

Synchronization has to be enabled in order to import user accounts from your SaaS app.

Note:

If the number of created objects (user accounts) and deleted recorded objects (synced user accounts) exceeds the maximum number allowed, the sync job aborts. The maximum number of objects created or recorded objects deleted is an approximate maximum limit, not a precise limit due to the parallel processing of synced objects.

See Importing User Accounts from a Software as a Service Application.

Import User Accounts from a Software as a Service Application

After enabling provisioning and synchronization for your App Catalog app, you may want to import the existing user accounts from your Software as a Service (SaaS) applications and link them to Oracle Identity Cloud Service users.

To import your SaaS user accounts you need to verify that:

• The app is activated. To activate your app, see Activating Applications.

• Provisioning is enabled. See Enabling Provisioning for an App Catalog Application.
• Synchronization is enabled. See Enabling Synchronization for an App Catalog Application.

1. If not already there, click Applications and then the name of the app that you want to configure.

   The Details page is displayed. Verify that the app is activated.

2. Click the Import tab.

   The page lists the result of the last import if any and the actions you need to perform. See Synchronizing User Accounts.

3. If you want to invoke an on-demand synchronization, click the Import icon. If the icon is grayed out, click the Provisioning tab and verify that Provisioning and Synchronization are enabled, and the app is activated.

4. A message confirms that the job for importing user accounts is running successfully.

After the import finishes the page lists the imported user accounts.

Synchronize User Accounts

After synchronizing your SaaS app with Oracle Identity Cloud Service, you will see the result of the import including the number of users created, deleted, and updated. You can do a general search based on account name, user e-mail or user name. You can also filter and search the results based on Situation and Synchronization Status. Select values from the respective drop-down lists to view user accounts matching the search criteria. These are helpful when you have to find a set of user accounts based on their situation or status from a huge number of results.

The Import page provides you with the overall status information, whether the Last Import succeeded, failed, or is still running. If the import succeeded, then the result is listed as follows:

• Start Date is the date and time you started the import job.

• End Date determines date and time the import job finished.

• Accounts Created shows the number of Oracle Identity Cloud Service accounts that got created during the import based on your synchronization settings.

• Accounts Deleted lists the number of Oracle Identity Cloud Service accounts that got deleted during the import based on your synchronization settings.

• Accounts Updated notes the number of Oracle Identity Cloud Service accounts that got changed during the import.

1. This table summarizes the result of successfully running an import. For each SaaS app account it shows whether there exists a matching Oracle Identity Cloud Service user and the action that you need to perform to link the SaaS user account to an Oracle Identity Cloud Service user.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Shows the name of the SaaS app user account.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Situation | Lists whether a matching Oracle Identity Cloud Service user exists or does not exist based on your synchronization configuration:  
  • **No match is found** indicates that you need to manually select which action to take.  
  • **Exact match is found** indicates that an Oracle Identity Cloud Service user exists that matches the synchronization criteria that you configured.  
  • **Multiple Matches are found** indicates that there are multiple matches found for a user. You need to manually select one of the available actions.  
  • **Manually linked** is the result of any action that you performed to link this SaaS app account to an Oracle Identity Cloud Service user. |
| User | Shows the email address and user name of the Oracle Identity Cloud Service user. |
| Action | If there is no matching Oracle Identity Cloud Service user you need to select the appropriate action from the drop-down list:  
  • **Assign Existing User**: The Assign User page lists all existing Oracle Identity Cloud Service users and allows you to select the one that you want to link with this SaaS app account.  
  • **Create New User and Link**: The Add User page allows you to create a new Oracle Identity Cloud Service user. |
| Status | Lists the status or whether you need to confirm linking the SaaS app account to the Oracle Identity Cloud Service user. |

2. Take the appropriate action to link your SaaS user accounts with Oracle Identity Cloud Service accounts.

Work with the Synchronization Failure Report

You can view the synchronization failure report of a provisioning application from the Import tab. The report contains the sync failures for the selected application. This report is useful in finding out the reason behind sync failures that occurred during account and object sync of an application.

1. Select the Import tab of the application, and click Synchronization Failure.
2. In the Synchronization Failure Report page, you can use the filters to narrow down the result based on the following criteria:
   a. **Dates Range**
      
      Choose the number of days for which you need the failure report. The possible values are: 30 Days, 60 Days, 90 Days and Custom Dates. Select Custom Dates to run the filter for a customized date range. Enter the Start Date and the End Date in the text box or select them from the calendar.
   b. **Application**
      
      The Application filter is case sensitive.
   c. **Object Type**
To narrow down the result based on Application or Object Type, choose a value from the drop-down menu and enter a corresponding value in the text box. The available drop-down values are: **Equals**, **Contains**, **Begins With** and **Ends With**.

**Example:**

If you select **Equals** as the value for drop-down menu and enter Google App in the text box, the filter will display entries only for Google App. If you select **Begins With** as the value for drop-down menu and enter G in the text box, the filter will display entries for applications starting with the letter G.

3. Once you have set the filter, click **Run** to display the search result.

The following table describes the various columns in the search filter:

<table>
<thead>
<tr>
<th>Filter Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Displays the name of the Application.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Displays the type of the Object, for example, Account, Group, Organization, Printer, and so on.</td>
</tr>
<tr>
<td>Object Identifier</td>
<td>Displays the unique ID of the object from which sync is performed.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the object on which sync is performed.</td>
</tr>
<tr>
<td>Date</td>
<td>Displays the time when the sync was performed on the object.</td>
</tr>
<tr>
<td>ECID</td>
<td>Displays the value of the Event Correlation Identifier (ECID).</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Displays the reason behind the synchronization failure.</td>
</tr>
</tbody>
</table>

4. Click **Download** to export the search result in the tabular column to a CSV file.

**Add Tags to an Application**

You're an identity domain administrator or application administrator who wants to create custom attributes for your applications that can be used to search for the applications more effectively. To do this, you add tags to your applications. Tags are key-value pairs that are used to organize and identify applications.

For example, suppose you're creating three versions of an application: one for development purposes, one for testing purposes, and one that will be used in production. You can create the following tags for these versions: **Version: Development**; **Version: Testing**; and **Version: Production**.

There are two kinds of tags that you can add to your application:

- **Tags**
  
  You can create new tags for your Confidential, Mobile, SAML, and App Catalog applications using the **Tags** section in the **Details** pane. You can use these tags to identify and organize your applications.
To add new tags to your application:

1. In the Tags area of the Details pane, click Add Tag.
2. In the Tag Key and Tag Value fields of the Add Tags window, enter or select the key-value pair for the tag you're creating.

To create more tags, click Add Tag, and repeat the process. You can add up to 100 tags.

- **Tagged**
  
  You can add existing tags from other applications to Confidential Applications only using the Tagged of Token Issuance Policy section. Based on the tags selected, your client application can access resource applications that have similar tags.

  To add existing tags from other applications:
  
  1. In the Tagged area of the Token Issuance Policy pane, click Add Tag.
  2. In the Add Tags window, search for the key-value pair of the tag that you're adding from another application by entering the search criteria in the Tag Key and Tag Value fields.

  **Note:**

  You can delete tags by clicking the X icon next to the tag. However, some tags are protected and cannot be deleted.

Assign Applications to Oracle Identity Cloud User Using Account Form

Account Form will be visible in the UI with account attributes for a provisioning application if the underlying App Template supports it. With Account Form, when you grant a provisioning application to a user, you can provide account values and when you edit a provisioned account, you can update existing account values.

To provide specific values using account form:

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Select User tab and click Assign.
3. In the Assign Users window, select a user who needs access to the application.
4. Click Assign for each user you want to assign to the application.
5. In the Assign Application window, the attribute values are populated based on the mappings already provided in the Attribute Mapping section in the Provisioning configuration tab. You can choose to keep the populated values or update any attribute value.
6. Click Save to create the account for the user chosen in step 3.
7. Select the next user you want to provide access to this application. Repeat steps 3 through 5 for the next user.
8. Click OK after you have assigned the application to the users. The user account is assigned.
When you want to update account attribute, activate or deactivate the account or revoke the account in Oracle Identity Cloud Service, it would automatically update the respective changes in the application.

Create a Custom Secure Form Fill App

Create and edit custom secure form fill applications for Oracle Identity Cloud Service.

Topics:
• Typical Workflow for Creating a Custom Secure Form Fill App
• Understand Custom Secure Form Fill Apps
• Prerequisites for Creating a Custom Secure Form Fill App
• Install the Secure Form Fill Admin Client
• Create a Secure Form Fill Configuration File
• Create a Secure Form Fill App in Oracle Identity Cloud Service
• Install the Google Chrome Plugin
• Test a Custom Secure Form Fill App
• Update a Custom Secure Form Fill App

Typical Workflow for Creating a Custom Secure Form Fill App

Create, manage, and update custom secure form fill apps in Oracle Identity Cloud Service.

The following table summarizes the suggested tasks that you perform when creating a custom secure form fill app.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Secure Form Fill Admin Client (Oracle Enterprise Single Sign-On (ESSO) Administrative Console).</td>
<td>The ESSO Administrative Console is part of the Secure Form Fill Admin Client. Use the ESSO Administrative Console to create secure form fill configuration files for your custom secure form fill apps in Oracle Identity Cloud Service.</td>
<td>Install the Secure Form Fill Admin Client</td>
</tr>
<tr>
<td>Create a secure form fill configuration file.</td>
<td>The ESSO Administrative Console is part of the Secure Form Fill Admin Client. Using the ESSO Administrative Console, create a secure form fill configuration file to be used when creating a custom secure form fill app in Oracle Identity Cloud Service.</td>
<td>Create a Secure Form Fill Configuration File Update a Custom Secure Form Fill App This documentation explains, at a high level, how to use the ESSO Administrative Console only as it pertains to custom secure form fill apps and Oracle Identity Cloud Service. For additional instructions, see the help in the ESSO Administrative Console.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Export the secure form fill configuration file.</td>
<td>The ESSO Administrative Console is part of the Secure Form Fill Admin Client. Using the ESSO Administrative Console, export the secure form fill configuration file that you will import into Oracle Identity Cloud Service when creating or updating a custom secure form fill app in Oracle Identity Cloud Service.</td>
<td>Create a Secure Form Fill Configuration File</td>
</tr>
<tr>
<td>Create a custom secure form fill app.</td>
<td>Using the Oracle Identity Cloud Service Admin Console, create a custom secure form fill app.</td>
<td>Create a Secure Form Fill App in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Assign users and groups.</td>
<td>Using the Oracle Identity Cloud Service Admin Console, assign users and groups to the custom secure form fill app.</td>
<td>About Modifying Applications</td>
</tr>
<tr>
<td>Activate the app.</td>
<td>Using the Oracle Identity Cloud Service Admin Console, activate the app so that users can access it.</td>
<td>Activate Applications</td>
</tr>
<tr>
<td>Install the secure form fill plugin.</td>
<td>Install the Oracle Secure Form Fill Plugin in order to launch secure form fill apps.</td>
<td>Install the Google Chrome Plugin</td>
</tr>
<tr>
<td>Test the custom secure form fill app.</td>
<td>Test the custom secure form fill app that you created before releasing the app.</td>
<td>Test a Custom Secure Form Fill App</td>
</tr>
<tr>
<td>Update the custom secure form fill app.</td>
<td>Update the custom secure form fill app that you created as needed.</td>
<td>Update a Custom Secure Form Fill App</td>
</tr>
</tbody>
</table>

**Understand Custom Secure Form Fill Apps**

Custom secure form fill apps give you the flexibility to define tenant-level form fill apps that are not in the global Oracle App Catalog.

Secure Form Fill is the Oracle Identity Cloud Service alternative for single sign-on into apps that require auto-form fill but don't support OAuth, SAML, or federated sign-on methods.

Users enter their application credentials for form-fill-enabled apps in Oracle Identity Cloud Service once. Oracle Identity Cloud Service stores and encrypts the information, and automatically fills in the login form so that users can sign in without having to re-enter the information each time.

Oracle Identity Cloud Service stores the user's credentials in an encrypted format using strong encryption combined with a customer-specific private key. When a user launches the secure form fill application, which in turn prompts the login page, Oracle Identity Cloud Service detects and securely fills the user's credentials, submits the credentials to the app login page, and then the user is automatically signed in.
Prerequisites for Creating a Custom Secure Form Fill App

Learn the prerequisites for creating a custom secure form fill app.

Ensure that you have the following prerequisites in place before creating and testing a secure form fill app.

- A Windows operating system version 7, 8 or 10 with:
  - Local admin rights enabled
  - 32-bit Java Runtime Environment (JRE) in order to access local help content for the Secure Form Fill Admin Client.

- At least one of the following supported desktop browsers:
  - Mozilla Firefox
  - Google Chrome

**Note:**
The mobile browsers are not certified. To view the list of certified browsers, see Supported Web Browsers.

- Secure Form Fill Admin Client. See Install the Secure Form Fill Admin Client.

**Note:**
The ESSO Administrative Console is part of the Secure Form Fill Admin Client.

- Oracle Identity Cloud Service tenant (17.2.2 or greater)

- Administrator privileges for Oracle Identity Cloud Service. See Understand Administrator Roles.

Install the Secure Form Fill Admin Client

You use the Secure Form Fill Admin Client (Oracle Enterprise Single Sign-On (ESSO) Administrative Console) to create and update secure form fill configuration files for your custom secure form fill apps in Oracle Identity Cloud Service. Use these instructions to install the Secure Form Fill Admin Client.

1. On the Download page, locate the Secure Form Fill Admin Client and download it. See Downloading Oracle Identity Cloud Service SDKs and Applications.

**Note:**
The ESSO Administrative Console is part of the Secure Form Fill Admin Client.
2. In the download location, unzip the file.
3. Double-click the installer to launch the install wizard, and then click Next.
4. Choose the **Complete** installation option, click Next, and then click Install.
5. When the installation completes, click Finish.

---

**Note:**

This documentation explains, at a high level, how to use the ESSO Administrative Console only as it pertains to custom secure form fill apps and Oracle Identity Cloud Service. For additional instructions, see the help in the ESSO Administrative Console.

---

### Create a Secure Form Fill Configuration File

You use the Secure Form Fill Admin Client (Oracle Enterprise Single Sign-On (ESSO) Administrative Console) to create secure form fill configuration files for your custom secure form fill apps in Oracle Identity Cloud Service. Use these instructions to create secure form fill configuration files and then import those files into Oracle Identity Cloud Service.

**Prerequisite:** An installation of Secure Form Fill Admin Client. See Install the Secure Form Fill Admin Client.

---

**Note:**

This documentation explains, at a high level, how to use the Secure Form Fill Admin Client only as it pertains to custom secure form fill apps and Oracle Identity Cloud Service. For additional instructions, see the help in the ESSO Administrative Console.

---

1. Launch the Secure Form Fill Admin Client.
2. Right-click **Applications**, and then choose **New Web App**. Alternatively, use any of the following options:
   - Click **Applications, Add**, and then choose **Application Type: Web** in the first pane of the wizard.
   - Choose **Insert, Application**, and then choose **Application Type: Web** in the first pane of the wizard.
3. On the Add Application dialog, enter the name of the application.

---

**Important:**

The application name must be the same name that you use when you create the secure form fill application in Oracle Identity Cloud Service.

---

4. Leave all other default options selected, and then click Finish.
5. Choose the **Logon** form type. This form is used to set up your Web app template.
6. In the **Address** field, enter the URL for the Web app, click **Go**, and then navigate to the login page.

A list of all fields on the login page appear on the bottom of the screen. Select any field in the list on the bottom of the screen to highlight the field on the page.

7. Using the fields on the bottom of the screen, complete the following steps:

   ![Note:]
   
   No other form type is supported at this time.

a. Select the user name field, right-click, and then choose **Username/ID**.

b. Select the password field, right-click, and then choose **Password**.

c. Select the submit button, right-click, and then choose **Submit**.

8. Click **OK**.

9. On the Web dialog, make any of the following changes as necessary.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Identification Tab** | Click **Edit** to make changes. This is the URL or the URLs of the form to configure. For applications that have varying text in their URLs, you can use substrings or regular expressions to specify how to match the variable text. Your Match Type change options are:  
  • **Exact Match.** Exact match matches a URL exactly as specified. This is generally an edge case and rarely used.  
  • **Wildcards.**  
    - ? matches any single character.  
    - * matches zero or more occurrences of any character. If wildcards are used, to avoid a potential security issue, do not perform mid-string wildcard matches. Always exact match the start of the URL, for example, https://server?.somesite.com/*.
  • **Regular Expressions.** This is the recommended option. Use the set of regular expressions to specify a string pattern that the form-fill agent should recognize as a match, for example, URL1=.*?https://www\expedia\co\jp/user/login.* |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Fields Tab** | Click a field, and then using the **Edit** button, adjust the primary form fields used for detection and injection of the user name and password fields as well as the submit button.  

**Note:**  
Do not use the **SendKeys** or the **SendKeys using journal hook** options.  
Check each field type to ensure that it is the appropriate type (such as Password for password input fields, and so on).  

Your Field options are:  
• **Field Identification.** Allows you to fine tune how the input fields for the form are located. Field identification can be adjusted for any form field. Click the ellipsis to display the Field identification options. Identify fields by:  
  – **Name.** The default and recommended option. Beware that not every input field has a name or sometimes the name is not consistent every time the page is loaded. If so, then it is recommended to use the Matching option.  
  – **Ordinal.** This option identifies fields based on sequence. This option is not the recommended alternative since it is easily impacted by minor changes to the page. Also, the fields and the field ordinals can be inconsistent across browsers.  
  – **Matching.** Identifies fields based on tag types, attribute values, HTML, and so on. This option is the recommended option if Name is not possible. Often, matching is used to match the “id” attribute of the input field or a regex on the name attribute. Matching can be a regex, substring match, or whole string match.  
• **Events.** Pre Inject and Post Inject events allow secure form fill to trigger a specific event on the field before and after injecting the credentials into that field. This is useful as some fields will not recognize that injection has occurred unless a specific event is triggered in that field. Event values are: blur, change, click, focus, focusin, focusout, input, keydown, keypress, keyup, and mouseover.  

| **Matching Tab** | Create or modify granular page matching criteria for the selected web form. Secure Form Fill in Oracle Identity Cloud Service uses the matching criteria you supply here to distinguish among similar forms. Matching can also be used to refine the detection match criteria, that is, the set of HTML tags and values you use to identify a specific field to perform more specific matching beyond just the form fields themselves.  

| **Proxy Tab** | Do not change these settings.  

10. Click **OK**.  
11. Use the following tabs to make any necessary changes:
**Note:**

Do not change any other options on any other sub tabs other than those listed in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Tab</strong></td>
<td>Enter a description for the Web app. Add, edit, or delete forms. This option allows you to set all the forms relevant for this Web app. Use this option if you have multiple login forms for your Web app. All other settings are not required for secure form fill and should not be changed.</td>
</tr>
<tr>
<td><strong>Error Loop Tab</strong></td>
<td>Secure form fill supports the detection of an error loop condition. Error loop conditions generally occur if secure form fill has the wrong credentials for the Web app and attempts to submit these credentials repeatedly to the Web app.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Logon timeout (sec.)</strong>. The maximum time in seconds between successive logon attempts before a logon error is triggered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Max. retries</strong>. The maximum number of retries (after first try) allowed before a logon error is triggered.</td>
</tr>
<tr>
<td><strong>Miscellaneous Tab</strong></td>
<td>• <strong>Logon Loop Grace Period</strong>. Allows control over the response during login grace period (for example, controls reinjection).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto-submit</strong>. Use this option to turn auto-submit on or off for all forms used by the app.</td>
</tr>
</tbody>
</table>

12. Click **File**, and then **Save**.

**Tip:**

Name the Web app file, the *.ini file, and the name of the Oracle Identity Cloud Service app with the same name.

13. To export the file, click **File**, **Export**, select the application to export, and then click **OK**.

14. Name the file.

**Important:**

The *.ini file name must match the name of the application created in Oracle Identity Cloud Service.

**Post requisite:** Create an Oracle Identity Cloud Service secure form fill app. See *Create a Secure Form Fill App in Oracle Identity Cloud Service*.

**Create a Secure Form Fill App in Oracle Identity Cloud Service**

After you create a configuration file in the Oracle Enterprise Single Sign-On (ESSO) Administrative Console, the next step is to create a secure form fill app in Oracle Identity Cloud Service.
1. In the Identity Cloud Service console, expand the Navigation Drawer, click Applications, and then click Add.

2. In the Add Application window, click App Catalog.

3. In the Type of Integration section, click Form Fill, locate Generic Secure FormFill App Template, and then click Add.

4. Complete the App Details by entering a Name, Description, and Application URL.

   **Important:**
   
   The application name must match the file name of the .ini file created in the ESSO Administrative Console.

5. Optional. In the Tags section, click Add Tag to add tags to your App Catalog application to organize and identify it.

6. In the Display Settings section, select Display in My Apps.

   **Important:**
   
   If you do not select Display in My Apps, the application does not display in the My Apps page for users.

When you select the Display in My Apps check box in applications, the app is then visible in the My Apps page, but selecting this check box doesn't enable or disable SSO to the app.

7. Select the User can request access check box, if you want the app to be listed in the Catalog. This option allows end users to request access to applications from their My Apps page by clicking Add and then selecting the app from the Catalog.

8. Click Add.

9. Click Import to import the secure form fill configuration file that you created in the ESSO Administrative Console.

   The application has been added in deactivate state. To activate your application, click Activate next to the app name.

10. To assign users to the application, click Users.

   **Tip:**
   
   Assign the application to yourself or a test user. This will save you time when testing the secure form fill app.

11. To assign groups to the application, click Groups.

   The applications you assign to the user or group displays on the My Apps page. Newly assigned applications and applications that a user has not yet accessed appear first in the application list and have an asterisk icon in the application tile. The icon appears on the tile until the user accesses the application.
Install and Use the Secure Form Fill Plugin

You must install the Oracle Secure Form Fill Plugin in order to launch secure form fill apps. Once installed, you are able to access My Apps from your browser toolbar.

**Topics:**
- Install the Google Chrome Plugin
- Install the Mozilla Firefox Plugin
- Access My Apps from the Browser Using the Plugin

Install the Google Chrome Plugin

If you are using Google Chrome and you need to install the plugin, you are prompted to go to the Extensions on Google Chrome and install the Oracle Secure Form Fill Plugin from the Oracle Identity Cloud Service user interface. You will be prompted to download the plug-in from the My Apps page the first time that you access to a secure form fill app.

Install the Mozilla Firefox Plugin

If you are using Mozilla Firefox and you need to install the plugin, instead of downloading the Secure Form Fill Mozilla Firefox plug-in from the Mozilla Store, install the Secure Form Fill Mozilla Firefox plug-in from the My Apps page. You will be prompted to download the plug-in from the My Apps page the first time that you access to a secure form fill app.

Access My Apps from the Browser Using the Plugin

After you install the Oracle Secure Form Fill Plugin, when you are logged in to Oracle Identity Cloud Service you can access My Apps from your browser toolbar.

Search for apps and see favorite apps by clicking the My Apps icon.

Test a Custom Secure Form Fill App

After you create a custom secure form fill app in Oracle Identity Cloud Service, you should test the app before deploying it to your organization.

**Prerequisites:**
- A custom secure form fill app created in Oracle Identity Cloud Service.
- The custom secure form fill app is set to display on the My App page.
- The custom secure form fill app is assigned to you as a user or as a group.

1. Log in to the Identity Cloud Service console to access the My Apps page.
2. Install the secure form fill plug in, if you have not already installed it, and then refresh your browser.
3. Launch the app, enter the credentials for the application, and then click **Login**.
A successful result is Oracle Identity Cloud Service injecting the user name and password, and then clicking the submit button.

If you are having issues, check the settings for your Web app in the Oracle Enterprise Single Sign-On (ESSO) Administrative Console, export the *.ini file if necessary, check the settings for your app in Oracle Identity Cloud Service, and try again.

Update a Custom Secure Form Fill App

To update a custom secure form fill app, you first update the Web app using the Secure Form Fill Admin Client, export the configuration file in (*.ini), and then update the custom secure form fill app in Oracle Identity Cloud Service.

Prerequisite:
- A Web app created in the Secure Form Fill Admin Client. See Installing the Secure Form Fill Admin Client.
- A custom secure form fill app created in Oracle Identity Cloud Service.

1. If you need to update the Web app and configuration file created in Secure Form Fill Admin Client, update the Web app first, and then save and export the file. See Create a Secure Form Fill Configuration File.

2. If you need to make changes to the custom secure form fill app in Oracle Identity Cloud Service, access the application as an Identity domain administrator, make any necessary changes, import the new configuration file (if necessary), and then save the app. See Create a Secure Form Fill App in Oracle Identity Cloud Service.

You should now test your new configuration. See Test a Custom Secure Form Fill App.

Import and Synchronize User Accounts Using a Flat File in Oracle Identity Cloud Service UI

You can import and synchronize user accounts of third party cloud applications using a flat file and manage them in Oracle Identity Cloud Service.

Topics:
- Import User Accounts Using Oracle Identity Cloud Service UI
- Synchronizing Imported User Accounts

Import User Accounts Using Oracle Identity Cloud Service UI

You can perform a full sync import of the user accounts of third party cloud applications using a flat file in the Oracle Identity Cloud Service UI. In a full sync import, the imported user accounts in the CSV file replaces any existing user who is already assigned into the application.

To import user accounts:
1. Create a CSV file for import in the following format or download the CSV file along with user data from the target system apps:

```
ID, NAME, ACTIVE
hercule.poirot@sampleapp.com, hercule.poirot@sampleapp.com, true
```

This table provides a description of the attributes in the CSV format file:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The unique identifier of the account in the target.</td>
<td><a href="mailto:hercule.poirot@sampleapp.com">hercule.poirot@sampleapp.com</a></td>
</tr>
<tr>
<td>NAME</td>
<td>The name of the account. NAME is the primary input that is matched with the username of a particular user in Oracle Identity Cloud Service.</td>
<td><a href="mailto:hercule.poirot@sampleapp.com">hercule.poirot@sampleapp.com</a></td>
</tr>
<tr>
<td>ACTIVE</td>
<td>The status of the account on the target. The possible values are true and false. If the value is true, the user account is imported and activated. If the value is false, the user is imported in a deactivated state.</td>
<td>true</td>
</tr>
</tbody>
</table>

2. In the Admin Console, expand the Navigation Drawer, and select **Applications**.
3. Select the required application in which you want to import user accounts.
4. Navigate to the **Import** tab.

5. **Note:**

   Import from CSV file is enabled for applications that support flat file synchronization.

   Select **Import**, browse for the CSV file, and import it.

6. Refresh the page to view the import result. If the import succeeds, then the user accounts present in the CSV file displays.
7. Select **Users** tab to view the imported users.

   **Note:**
   
   You need to refresh the **Users** tab to view the imported users.

8. Observe that the users with a true value for **ACTIVE** attribute are activated. However, if a user account has false value for **ACTIVE** attribute, the user account is imported in a deactivated state.
9. Synchronize the imported user accounts.

See Synchronizing Imported User Accounts to synchronize the imported user accounts with the users in Oracle Identity Cloud Service.

Synchronize Imported User Accounts

After you import the user accounts, if a matching user account doesn't exist in Oracle Identity Cloud Service, you can either assign the user account to an existing user or create a new user for the user account.

If the imported user account exists, an exact match is found and no further action is required. The synchronization status of the user account is set as confirmed.

Topics:
- Assign an Existing User
- Create and Link a New User with the User Account
- Manage Synchronized User Accounts

Assign an Existing User

You can assign an existing user to the imported user account in the Import tab if the user is present in Oracle Identity Cloud Service and the import failed to match the user.

To assign an existing user:

1. Select Assign Existing User option from the Select an Action drop-down list.
2. In the Assign User window, search for an existing user, select the required user and click OK.

The user account is manually linked to the existing user and the synchronization status is confirmed.

Create and Link a New User with the User Account

You can create a new user and link the user with the imported user account in the Import tab if there are no existing users to assign.

To create and link a new user:

1. Select Create New User and Link option from the Select an Action drop-down list.
2. In the Add User window, enter the following user details: First Name, Last Name, User Name or Email.
3. Select Use the email address as the user name option if you want to use the email address as your user name and click OK.

The user account is manually linked to the new user and the synchronization status is confirmed.
Manage Synchronized User Accounts

You can activate, deactivate, assign and revoke imported user accounts from the Users tab.

You can perform the following actions on the synchronized user accounts:

- To activate an imported user account, select the Action menu, and click Activate.
- To deactivate an imported user account, select the Action menu, and click Deactivate.
- To remove any imported user account, select the user, and click Revoke.
- To assign any other user to the application apart from the synchronized users from the flat file, click Assign. Choose a user from the list of existing users and click OK. The assigned user account is displayed and is in an activated state.

View Details About Applications

By default, you can see the name and description for each application in Oracle Identity Cloud Service.

By clicking an application name, you can view high-level and configuration information about the application. For Oracle applications, you can also see the roles associated with the application, and the Oracle Identity Cloud Service groups and users assigned to the application.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.

2. In the Applications page, click the application name for which you want additional information.

   Tip:

   To search for applications, enter all or part of the beginning of the application name that you want to locate in the search field, and then press Enter. To fine-tune your search, click the search field again, and then select a status.

3. To view high-level information about the application, such as the application type, name, description, icon, URL, links, and whether the application will appear on the My Apps page, click Details.

4. To view configuration information about the application, click Configuration. For custom SAML applications, this tab is labeled SSO Configuration because, by granting SAML applications to users, they can single sign-on (SSO) into SaaS applications that support SAML for SSO. See Add a Confidential Application, Add a Mobile Application, and Add a SAML Application.

When you purchase an Oracle application, an instance of the application is created in your identity domain and appears in the Applications page automatically. For Oracle applications, you can't edit values that appear in the Details tab or the Configuration tab.
Because you can add custom applications to your identity domain, you can edit high-level and configuration information for these applications. See About Modifying Applications.

5. For Oracle applications, to view roles associated with the application, click Application Roles. You can assign users and groups to an application role or remove users and groups from the application role. See About Modifying Applications.

6. For Oracle applications, to view the names and descriptions of any groups assigned to the application, click Groups.

7. For Oracle applications, to view the names, email addresses, and phone numbers of any users assigned to the application, click Users. You can filter and sort this list of users.
   • To display only those users who are assigned to a particular application role, click Show, and then select the application role.
   • To display users who are assigned to any application role, click Show, and then select All Role Members.
   • To sort the users in ascending order by their names or email addresses, click Sort By, and then select Name or Email.

About Modifying Applications

Learn about assigning users and groups to applications; and importing and exporting users and groups for Oracle and custom applications.

Topics:
• Modify Applications
• Modify Oracle Applications
• About Importing Users and Groups for Oracle Application Roles
• Export Users and Groups for Oracle Application Roles
• Modify Custom Applications

Modify Applications

After configuring, you can modify Oracle and custom applications to assign users and groups, edit high-level information, import users and groups into the applications, export users and groups from applications, and perform specific configuration tasks for custom applications.

To modify applications:

1. In the Identity Cloud Service admin console, expand the Navigation Drawer, and then click Applications.

2. Click the application you want to modify. The Applications page expands to open a sub page that displays high-level information about the application.

You can perform the following tasks in Oracle and custom applications:
• Oracle Applications:
  – Assign users and groups.
– Remove users and groups.

The **Groups** and **Users** tabs are used to display groups and users assigned to application roles of an Oracle application. Although you can filter and sort this list of users and groups, you can't modify the list. You can't edit values that appear in these tabs.

– Import Users and Groups for Oracle Application Roles.

– Export Users and Groups for Oracle Application Roles.

**Note:**

If you assign user accounts to Oracle application roles and then deactivate the accounts, Oracle Identity Cloud Service prevents the users from accessing the roles. To enable the users to access the Oracle application roles to which they are assigned, activate the user accounts. See **Activate User Accounts** and **Deactivate User Accounts**.

– View High-Level Information

See **Modify Oracle Applications**.

**Custom Applications:**

– Assign users and groups.

– Remove users and groups.

– Edit high-level information and configuration information.

– Edit Web Tier Policies for Trusted Applications.

– Regenerating a Client Secret and generating tokens for Trusted Applications

– Edit single sign-on (SSO) configuration for SAML Applications.

See **Modify Custom Applications**.

## Modify Oracle Applications

You can assign and remove users and groups to Oracle Applications, and import and export users and groups for Oracle Application Roles. You can just view the high level information and cannot edit any of the values in Oracle Applications.

**Topics:**

- **Assign Users to Oracle Applications**
- **Remove Users from Oracle Applications**
- **Assign Groups to Oracle Applications**
- **Remove Groups from Oracle Applications**
- **Edit High-Level Information for Oracle Applications**
Assign Users to Oracle Applications

To assign users to Oracle applications, use the Application Roles tab. You can assign users to Oracle applications only after you activate the applications.

1. Click Application Roles.
2. Select the check box for the application role of the Oracle application to which you want to assign users.
3. Click More, and then select Assign Users.
4. In the Assign Users window, select the check box for each user that you want to assign to the application role.
5. Click Assign.
   The application role displays a user icon and a Users Assigned link. The link displays the number of users that you assigned to the application role.
6. Click Users Assigned.
7. In the Users Assignments window, verify that you see the users that you assigned to the application role.
8. Click Close.

Remove Users from Oracle Applications

To remove users from Oracle applications, use the Application Roles tab. You can remove users from Oracle applications only after you activate the applications.

1. Click Application Roles.
2. Select the check box for the application role of the Oracle application from which you want to remove users.
3. Click More, and then select Revoke Users.
4. In the Revoke Users window, select the check box for each user that you want to remove from the application role.
5. Click Revoke.

Assign Groups to Oracle Applications

Once you activate the applications, you can assign groups to Oracle applications by using the Application Roles tab.

1. Click Application Roles.
2. Select the check box for the application role of the Oracle application to which you want to assign groups.
3. Click More, and then select Assign Groups.

4. In the Assign Groups window, select the check box for each group that you want to assign to the application role.

5. Click Assign.

**Note:**

The All Tenant Users group is a default group that's created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. If you assign this group to any of your applications, then all users are assigned to these applications indirectly.

The application role displays a group icon and a Groups Assigned link. The link displays the number of groups that you assigned to the application role.

6. Click Groups Assigned.

7. In the Groups Assignments window, verify that you see the groups that you assigned to the application role.

8. Click Close.

Remove Groups from Oracle Applications

You can remove groups from Oracle applications from the Application Roles tab. You can remove groups from Oracle applications only after you activate the applications.

1. Click Application Roles.

2. Select the check box for the application role of the Oracle application from which you want to remove groups.

**Tip:**

You can see which application roles have groups assigned to them by the group icon and the Groups Assigned link that appears in the application role.

3. Click More, and then select Revoke Groups.

4. In the Revoke Groups window, select the check box for each group that you want to remove from the application role.

**Note:**

The All Tenant Users group is a default group that's created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. If you remove the All Tenant Users group from your applications, then access rights to these applications are revoked for every Oracle Identity Cloud Service user.

5. Click Revoke.
Edit High-Level Information for Oracle Applications

When you create an instance of an Oracle application in your identity domain, the application instance appears in the **Applications** page. As a Service Administrator, you can edit some of the high-level information for Oracle Applications. However, you can't edit attributes that are protected. Even in an editable attribute, you can't update certain values that were seeded by the system.

To view and edit high-level information about Oracle application, such as the application type, name, description, icon, URL, links, and whether the application will appear on the **My Apps** page, click **Details**.

As of 18.2.6 release, the tabular column lists the editable UI field names, respective attributes, whether the seeded values can be updated and whether new values can be added to the editable field names:

<table>
<thead>
<tr>
<th>UI Elements</th>
<th>Attributes</th>
<th>Update Seeded Values</th>
<th>Add New Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>description</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Tags</td>
<td>tags</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allowed Scopes</td>
<td>allowedScopes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allowed Tags</td>
<td>allowedTags</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>redirectUris</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Access Token Expired</td>
<td>accessTokenExpriy</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Refresh Token Expired</td>
<td>refreshTokenExpriy</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Scope</td>
<td>scopes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Secondary Audiences</td>
<td>protectableSecondaryAudiences</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Is Refresh Token Allowed</td>
<td>allowOffline</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Enforce Grants as Authorization</td>
<td>allowAccessControl</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Trust Scope</td>
<td>trustScope</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Activate</td>
<td>active</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Not all attributes correspond to UI fields:


- `grantedAppRoles` attribute records each App Role defined by another application that has been granted to the client.

- `signonPolicy` editable attribute indicates that you can assign Oracle Applications to Sign-On Policy.
**Note:**

You cannot change any of the fields other than the ones listed above for Oracle Public Cloud applications. You will encounter an error if you click Save after you try editing any of these values.

Apart from editing certain attributes, you can perform the following with Oracle Public Cloud Applications:

- Edit only single scope. Bulk removal of scopes is not supported.
- Grant client access to the Oracle Identity Cloud Service APIs

In order to enable your application to access Oracle Identity Cloud Service APIs, click **Add**.

In the **Add App Role** window, select the application roles that you want to assign to this application. This enables your application to access the REST APIs that each of the assigned application roles can access.

For example, select **Identity Domain Administrator** from the list. All REST API tasks available to the identity domain administrator will be accessible to your application.

You can't remove the following:

- The assigned application roles from the application by clicking the x icon for the row of the required application role
- The App Roles that were granted when an Oracle Public Cloud application was created because those seeded values are protected

See Apps/App Roles endpoint for a complete list of which endpoints each application role can access.

### About Importing Users and Groups for Oracle Application Roles

You can use Oracle Identity Cloud Service to import users and groups to assign them to Oracle application roles of Oracle applications automatically.

See Add or Remove a User Account from an Administrator Role for information about assigning users to administrator roles.

**Topics:**

- Create and Prepare a Comma-Separated Value File
- Import Users and Groups for Oracle Application Roles

### Create and Prepare a Comma-Separated Value File

Learn how to create and prepare a comma-separated value (CSV) file to import either a single user or group, or multiple users or groups.

To create and prepare a CSV file:

1. Use these sample files as a starting point.
2. Extract the compressed file and then open the AppRoleMembership.csv file.
3. Review and then delete any demo data in the `AppRoleMembership.csv` file.

   To familiarize yourself with the import process, consider importing just the demo data. You can then delete the unwanted demo data from Oracle Identity Cloud Service before you begin importing live data.

4. Create an import file using the `AppRoleMembership.csv` file. The `AppRoleMembership.csv` file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table. At a minimum, the file must have these exact column headings:

   - Entitlement Value
   - Grantee Name
   - Grantee Type

5. As a best practice, ensure that the fields in these columns are unique.

6. For each account, create a new row (line) and enter data into each column (field). Each row equals one record. The maximum number of membership roles that can be imported in a single job must not exceed 10,000.

7. To create a CSV file, use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or use a text editor, such as Notepad or TextPad.

8. Save your file in a CSV format. If you do not save the file in a CSV format with UTF-8 encoding, the import fails.

   **Note:**

   If you exported application role memberships prior to version 17.2.2 of Oracle Identity Cloud Service, and you want to import them back into Oracle Identity Cloud Service, you need to change the column headings in your CSV file to **Entitlement Value**, **Grantee Name**, and **Grantee Type** before doing so.

---

**Import Users and Groups for Oracle Application Roles**

You can use Oracle Identity Cloud Service to import users and groups using a comma-separated value (CSV) file to assign them to Oracle application roles.

**Note:**

To import or export users and groups for application roles, you must be assigned to either the identity domain administrator role or the application administrator role.

To import users and groups for Oracle application roles:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.

2. In the **Applications** page, click the Oracle application that has roles to which you want to assign users and groups.

3. Click **Application Roles**.
4. Click **Import**.

5. In the **Import Application Roles** window, click **Browse** to locate and select the CSV file that contains the users and groups to import.

   **Note:**
   
   Click **Download sample file** in the dialog box to download a sample file.

6. Verify that the path and name of the CSV file that you selected appear in the **Select a file to import** field.

7. Click **Import**.

   If a user or a group is missing a required value, such as the user name or the group name, then Oracle Identity Cloud Service can't import the user or group. If Oracle Identity Cloud Service can't import the user or group, then it evaluates the next user or group in the CSV file.

8. After Oracle Identity Cloud Service evaluates all users and groups, review the job results.

   - If the job can be processed immediately, then a dialog box appears with the **Job ID** link for your import job. Click the link. Review the details that appear on the **Jobs** page.
   
   - If the job cannot be processed immediately, then a message appears with a **Schedule ID** in it. Copy that ID and use it to search for the job on the **Jobs** page. The job will appear when processing completes. Go to Step 9.

   Oracle Identity Cloud Service assigns a job ID to each file that's imported or exported, for auditing purposes.

9. On the **Jobs** page, locate the job that you want to view, and then click **View Details**.

   A table appears that displays the user names or group names, classification types (User or Group), and status of the users and groups that you imported and assigned to Oracle application roles in Oracle Identity Cloud Service.

   See **Export Job Errors** to download a CSV file of any errors to your local machine.

---

**Export Users and Groups for Oracle Application Roles**

You can use Oracle Identity Cloud Service to export users and groups assigned to Oracle application roles of Oracle applications.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.

2. In the **Applications** page, click the Oracle application that has application roles with users and groups assigned to them.

3. Click **Application Roles**.

4. To export all application roles that have users and groups assigned to them, click **Export**, and then select **Export All**.

   To export only some application roles, select the check box for each application role that you want to export. Click **Export**, and then select **Export Selected**.
Tip:
The number that appears within parentheses to the right of Export All is how many application roles are created for the Oracle application. The number within parentheses to the right of Export Selected is how many application roles that you selected to export.

5. In the Export Application Roles window, click Export Application Roles.

6. After Oracle Identity Cloud Service creates the export file, a Job ID link appears. Click the link.

7. Review the details that appear in the Jobs page. This page shows how many application roles that you attempted to export, how many application roles Oracle Identity Cloud Service exported successfully, and how many application roles can't be exported because of a system error.

8. Click Download.
See Export Job Errors to download a CSV file of any errors to your local machine.

Modify Custom Applications
You can assign and remove users and edit high-level information in custom applications.

Topics:
• Assign Users to Custom Applications
• Remove Users from Custom Applications
• Assign Groups to Custom Applications
• Remove Groups from Custom Applications
• Edit High-Level Information for Custom Applications
• Edit Configuration Information for Custom Applications
• Edit SSO Configuration Information for SAML Applications
• Import User Accounts from a Flat File Using REST APIs
• Regenerate a Client Secret for Confidential Applications
• Generate Tokens for Trusted Applications

Assigning Users to Custom Applications
Custom applications are non Oracle Public Cloud (OPC) services. You can modify custom applications by assigning users to them. Users can access the My Apps page to view these applications.

Prerequisite:
• The application must be activated.
• The application must be assigned to the current user who is accessing My Apps page.
The Display in My Apps check box must be selected in the Details tab in the applications.

You can directly assign users to an application as follows.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the application that you want to modify.
3. Click Users.
4. Click Assign.
5. In the Assign Users window, do one of the following.
   - Select the check boxes for each user that you want to assign to the application.
   - For a provisioned application, select Assign next to the user that you want to assign to the application. In the Assign Application window, enter the required values in the form and click Save.
6. Click OK.

**Note:**

You can activate or deactivate an user's account assigned to a synchronized app that is created from App Catalog. To do so:

1. Click the Action menu to the right of the user account that you assigned to the application.
2. Click Activate or Deactivate.
3. In the Activate Account? or Deactivate Account? window, click OK.

See Enabling Provisioning for an App Catalog Application for more information about configuring provisioning for an application to manage the lifecycle of user accounts in the application.

Remove Users from Custom Applications

You can modify custom applications by removing users from them. Users can no longer view these applications through the My Apps page.

**Prerequisite:** The application must be activated.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the application that you want to modify.
3. Click Users.
4. Select the check box for each user that you want to remove from the application.
5. Click Revoke.
6. Complete one of the following choices:
Assign Groups to Custom Applications

You can modify custom applications by assigning groups to them. Users who are members of these groups can access the My Apps page to view these applications.

**Prerequisite:** The application must be activated.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the application that you want to modify.
3. Click Groups.
4. Click Assign.
5. In the Assign Groups window, do one of the following:
   - Select the check boxes for all groups that you want to assign to the application.
   - For a provisioned application, select Assign next to the group that you want to assign to the application. In the Assign Application window, enter the required values in the form and click Save.

**Note:**
The All Tenant Users group is a default group that's created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. If you assign this group to any of your applications, then all users are assigned to these applications indirectly.

6. Click OK.

Remove Groups from Custom Applications

You can modify custom applications by removing groups from them. Users who are members of these groups can no longer view these applications through the My Apps page.

**Prerequisite:** The application must be activated.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the application that you want to modify.
3. Click Groups.
4. Select the check box for each group that you want to remove from the application.

The All Tenant Users group is a default group that's created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. If you remove the All Tenant Users group from your applications, then
access rights to these applications are revoked for every Oracle Identity Cloud Service user.

5. Click **Revoke**.

### Edit High-Level Information for Custom Applications

You can edit high-level information for custom applications.

1. Click **Details**.
2. To modify an attribute value, enter the modification in the attribute field (for example, modify the application name in the **Name** field).
3. Click **Save**.

### Edit Configuration Information for Custom Applications

You can edit configuration information for custom applications.

1. Click **Configuration**.
2. Expand the **Client Configuration** node.
3. Modify a configuration value for the custom application by:
   - Entering the value in the attribute field (for example, in the **Redirect URL** field, entering the application URL where the user is redirected after authentication)
   - Clicking a button (for example, adding a resource to the custom application by clicking **Add** or removing a scope for a trusted application by clicking **Remove**)
   - Selecting or clearing the check box (for example, allowing the resource owner to be a grant type for the custom application by selecting **Resource Owner**)
   - Selecting the value from the menu (for example, selecting **User Administrator** from the **Grant the client access to Identity Cloud Service Admin APIs**. list to enable the custom application to access user administrator-related APIs)
4. If your custom application is a trusted application, then expand the **Resources** node.
   
   If your custom application is a mobile application, then the **Resources** node doesn't appear in the **Configuration** tab. This is because trusted applications run on a protected server, and mobile applications run on an unauthenticated web browser or a mobile device.
5. Modify a configuration value for the protected resources of your trusted application. See step 3 for more information about how to edit configuration values.
6. Click **Save**.

See Add a Confidential Application, Add a Mobile Application, and Add a SAML Application for more information about the configuration settings for client applications.
Edit Consent Information for Custom Applications

Application administrators can customize the information that appears in the OAuth consent page for applications.

If your application's resources is configured to require consent, then Oracle Identity Cloud Service provides a consent page in which users must allow to access the application's resources. By default, this consent page is branded with Oracle Identity Cloud Service information, but you can customize the information that appears in the page.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the application that you want to modify, and then click the Configuration tab.
3. Expand the Consent Information node.
4. Provide values for the fields that you want to customize, and then click Save.

Edit SSO Configuration Information for SAML Applications

You can edit SSO configuration information for SAML applications.

See Add a SAML Application for more information about the SSO configuration settings for SAML applications.

To edit SSO configuration:

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Select the SAML application from the list of applications listed.
3. Click SSO Configuration.
4. In the General section, modify required SAML assertion attributes for the SAML application by:
   • Entering a value in the attribute field (for example, in the Assertion Consumer URL field, entering the endpoint at the service provider to which the SAML assertion will be sent by the SAML identity provider)
   • Selecting a value from a list (for example, selecting the type of format to use for the NameID from the NameID Format list)
   • Clicking a button (for example, uploading the signing certificate that is used to encrypt the SAML assertion by clicking Upload)
5. Expand the Advanced Settings section to modify optional advanced SAML assertion settings for the SAML application (for example, selecting Assertion from the Signed SSO list to indicate that you want the SAML assertion signed).
6. Expand the Attribute Configuration section to modify user-specific and group-specific attributes for the SAML application (for example, selecting User Attribute from the User Attribute list or selecting the condition by which you want to filter the group memberships from the Condition list).
7. Click Save.
Import User Accounts from a Flat File Using REST APIs

Some target applications do not support synchronization with Oracle Identity Cloud Service. You can onboard the user accounts from these applications by importing the accounts from a flat file using REST APIs.

To import user accounts from a flat file:

1. Create a CSV file for import in the following format or download the CSV file along with user data from the target system apps:

   ID, NAME, ACTIVE
   hercule.poirot@sampleapp.com, hercule.poirot@sampleapp.com, true

   This table provides a description of the attributes in the CSV format file:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The unique identifier of the account in the target. The ID should match the target attribute that is defined for this application.</td>
<td><a href="mailto:hercule.poirot@sampleapp.com">hercule.poirot@sampleapp.com</a></td>
</tr>
<tr>
<td>NAME</td>
<td>The name of the account.</td>
<td><a href="mailto:hercule.poirot@sampleapp.com">hercule.poirot@sampleapp.com</a></td>
</tr>
<tr>
<td>ACTIVE</td>
<td>The status of the account on the target. The possible values are true and false.</td>
<td>true</td>
</tr>
</tbody>
</table>

2. Upload the flat file to the storage server. You can use the below curl command to upload a file to storage using the tenant admin access token.

   curl -k
   -X POST
   -H "Authorization: Bearer <Tenant Admin Access Token Value>"
   -F "contentType=text/csv"
   -F "isPublic=false"
   -F file="/scratch/$USER/flatfile.csv" "https://<tenant base url>/storage/v1/Files"

   Make note of the fileName attribute from the response.

3. To get the value of the application id, use the following request:

   curl -k
   -X GET
   -H "Authorization: Bearer <Tenant Admin Access Token Value>"
   -H "Content-Type:application/scim+json"
   "https://<tenant base url>.identity.oraclecloud.com/admin/v1/Apps?filter=displayName co "<Your application name>""

   Make note of the value of the id attribute from the response.
4. To get the value for the `resourceType`, use the following request:

```
curl -k
-X GET
-H "Authorization: Bearer <Tenant Admin Access Token Value>"
-H "Content-Type: application/scim+json"
"https://<tenant base url>.identity.oraclecloud.com/admin/v1/Apps/<appID>?
```

Copy the value of the `objectClasses.resourceType` from the response. The `resourceType` value has a prefix of "ManagedApp" followed by a GUID.

5. Run the `ManagedObjectSync` reconciliation job using a json file with information of the `resourceType` and the csv file you uploaded. Create and save a JSON file with the following content:

```
{
    "schemas": [
        "urn:ietf:params:scim:schemas:oracle:idcs:JobSchedule"
    ],
    "jobType": "ManagedObjectSync",
    "runNow": true,
    "parameters": [
        {
            "name": "resourceType",
            "value": "<Dynamic ResourceType ID from app>
        },
        {
            "name": "isIncremental",
            "value": "false"
        },
        {
            "name": "isFileBased",
            "value": "true"
        },
        {
            "name": "fileURI",
            "value": "<fileURI of the file in the storage. Format: files/201702110205/testFileName-1486778745812-5318.csv>"
        }
    ]
}
```

POST request:

```
curl -k
-X POST
-H "Content-Type: application/scim+json"
-H "Authorization: Bearer <Tenant Admin Access Token Value>"
-d @"/scratch/$USER/runjob.json"
https://<tenant base url>/job/v1/JobSchedules
```
After you run the command, verify that the users in the csv file have been assigned to the application.

6. Optionally, you can check the status of the scheduled job using the JobHistories API. See REST API for Oracle Identity Cloud Service.

Regenerate a Client Secret for Confidential Applications

When you create a confidential application, you use a Client ID and a Client Secret as part of your connection settings. You can regenerate your Client Secret at any time for a confidential application using the Identity Cloud Service console.

**Prerequisite:** An existing confidential application in Oracle Identity Cloud Service

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.
2. Click the confidential application for which you want to regenerate a Client Secret.
3. Click **Configuration**.
4. Expand the **General Information** node.
5. Click **Regenerate**. The new Client Secret appears in the **Client Secret** dialog box.
6. Click **Close**.

Generate Tokens for Confidential Applications

When you create a confidential application and you configure the client to use the **JWT Assertion** grant type, you can generate access tokens at any time using the Identity Cloud Service console.

**Prerequisite:** An existing trusted application in Oracle Identity Cloud Service with the client configured to use the **JWT Assertion** grant type and activated.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.
2. Click the confidential application for which you want to generate an access token.
3. Click **Generate Access Token**.
4. In the **Generate Token** pop-up window, use the following table to configure which scopes should be included in the access token:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Scopes</td>
<td>Click <strong>Available Scopes</strong> to get the access token to access any resources configured for the application. If the scopes are defined from multiples resource servers, the token cannot be generated. Use the <strong>Customized Scopes</strong> option and make sure that the selected scopes are from the same resource server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Customized Scopes using Invokes Identity Cloud Service APIs | a. Click Customized Scopes and Invokes Identity Cloud Service APIs.  

b. From the list of all the roles that are assigned to the client application you can select those roles that you want to include or remove to limit the scopes to be populated in the resulting token.  

| Customized Scopes using Invokes Other APIs | a. Click Customized Scopes and Invokes Other APIs.  

b. The UI displays a list of all the scopes assigned to the application. You can select any desired scopes as long as those scopes are from the same resource server.  

| Include Refresh Token | If the Refresh Token grant type is configured for your client application and the resource server which the scopes belong to allows the refresh token to be generated, the Include Refresh Token check box is enabled to be used. The refresh token is used to obtain a new access token without requiring the user to reauthenticate. |

5. Click **Download Token**.

Note:
The downloaded token gets saved as a `tokens<n>.tok` file in the download folder of your browser.

Activate Applications

Activating applications reinstates the access rights to applications for users and groups. You can use Oracle Identity Cloud Service to activate multiple applications simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click **Applications**.

2. Select the check box for each deactivated application that you want to activate, or to activate all deactivated applications, search for accounts with a status of **Inactive**. Then, select the Select All check box.

   Tip:
   
   A red circle with a white line through the circle indicates a deactivated application.

3. Complete one of the following choices:
To activate one application, click **Activate**, and then click **OK** in the **Confirmation** window.

To activate more than one application, click **Activate**, and then click **OK** in the **Confirmation** window.

---

**Note:**

You cannot activate an Oracle Public Cloud application from the UI. You will encounter an error if you try activating any Oracle Public Cloud application.

---

### Deactivate Applications

Deactivating an application temporarily disable the access rights to applications that users or groups have. You can use Oracle Identity Cloud Service to deactivate multiple applications simultaneously.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.
2. Select the check box for each activated application that you want to deactivate, or to deactivate all applications, search for accounts with a status of **Active**. Then, select the **Select All** check box.

**Tip:**

A green check mark indicates an activated application.

3. Complete one of the following choices:
   - To deactivate one application, click **Deactivate**, and then click **OK** in the **Confirmation** window.
   - To deactivate more than one application, click **Deactivate**, and then click **OK** in the **Confirmation** window.

**Note:**

You cannot deactivate an Oracle Public Cloud application from the UI. You will encounter an error if you try deactivating any Oracle Public Cloud application.

---

### Remove Applications

You can use Oracle Identity Cloud Service to remove multiple applications simultaneously.

1. In the Identity Cloud Service admin console, expand the **Navigation Drawer**, and then click **Applications**.
2. To remove an application, deactivate it first.
3. Select the check box for each application that you want to remove, or to remove all applications, select the Select All check box.

4. Complete one of the following choices:
   - To remove one application, click Remove, and then click OK in the Confirmation window.
   - To remove more than one application, click Remove, and then click OK in the Confirmation window.

Note:
You cannot remove an Oracle Public Cloud application from the UI. You will encounter an error if you try removing any Oracle Public Cloud application.
Manage Oracle Identity Cloud Service Jobs

Learn how to bulk load data into Oracle Identity Cloud Service.

Topics:
- Understand Bulk Loading Data
- Typical Workflow for Bulk Loading Data
- Use Best Practices for Bulk Loading Data
- View Jobs and Job Details
- Export Job Errors

Understand Bulk Loading Data

Oracle Identity Cloud Service may be one among many repositories in your organization. When you start using Oracle Identity Cloud Service, you might want to load data from the other repositories into Oracle Identity Cloud Service. Bulk loading offers a solution to this requirement.

Bulk loading is aimed at automating the process of loading a large amount of data into Oracle Identity Cloud Service. You can bulk load data after you subscribe to Oracle Identity Cloud Service or at any time during the production lifetime. You can bulk load users, groups, and application roles. Onboarding Users and Groups are administrative tasks.

You can access the Bulk Loading Users and Groups Using CSV Files tutorial to see how to import user accounts into Oracle Identity Cloud Service.

You can bulk load data using the following methods:
- The Identity Cloud Service console
- SCIM-based APIs

In this section, you learn how to bulk load data by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Typical Workflow for Bulk Loading Data

To start bulk loading data, refer to the typical workflow described in this section.

After each import step, analyze the data recorded during the bulk load operation.

If the job can be processed immediately, a dialog box appears with the Job ID link for your import job, click the link. Review the details that appear on the Jobs page.
If the job can't be processed immediately, a message appears with a **Schedule ID** in it. Copy that **Schedule ID**, and use it to search for the job on the **Jobs** page. The job will appear when processing completes.

This page shows how many accounts you imported, how many accounts imported successfully, and how many accounts can't be imported because of a system error. Common issues that prevent the system from importing the account include:

- Invalid email address format
- Invalid field formats
- Missing required fields
- Invalid CSV file

If there are many invalid accounts, correct the errors in the import file and then import the file again. See **Viewing Jobs and Job Details**.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Import users.</td>
<td>Use this task to create users only.</td>
<td><strong>Import User Accounts</strong></td>
</tr>
<tr>
<td>Step 2: Import groups.</td>
<td>Use this task to create groups and user memberships.</td>
<td><strong>Import Groups</strong></td>
</tr>
<tr>
<td>Step 3: Import application role memberships.</td>
<td>Use this task to create application role memberships for users and groups.</td>
<td><strong>Import Users and Groups for Oracle Application Roles</strong></td>
</tr>
<tr>
<td>Step 4: (Optional) Gather diagnostic data from the bulk load operation.</td>
<td>If you encounter errors during a bulk load operation and you cannot fix them by modifying the entries in the import file, you can set a diagnostics level to capture operational logs during the bulk load operation. You can then view those logs to help you to determine the cause of the problem.</td>
<td>See <strong>Run Oracle Identity Cloud Service Reports</strong>.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 5: (Optional) Resolving errors after a bulk load operation.</td>
<td>If you encounter errors during a bulk load operation, resolve the errors and then try the bulk load operation again. &lt;br&gt;One of the reasons that Oracle Identity Cloud Service cannot import a user account is, for example, because the account is missing a required value, such as the user's first name, last name, or user name. &lt;br&gt;If Oracle Identity Cloud Service can't import a user account, then it evaluates the next account in the CSV file. &lt;br&gt;View the details of the import job. If the job contains errors, you can export those errors to see the cause. &lt;br&gt;If you cannot resolve the errors, use the diagnostic data report to capture operational logs to see if you can determine the cause of the problem.</td>
<td>View Jobs and Job Details&lt;br&gt;See Run Oracle Identity Cloud Service Reports.&lt;br&gt;Export Job Errors</td>
</tr>
</tbody>
</table>

Use Best Practices for Bulk Loading Data

Implementing these best practices when bulk loading data reduces the possibility of errors occurring during the bulk load process. Read and understand this section before you start bulk loading data.

Use the following sections to learn about key elements for bulk loading data.

Topics:
- Bulk Loading File Specifications
- Sample Files
- Workflow
- Deactivate Notifications
- Testing

Bulk Loading File Specifications

Learn about the bulk loading files specification to reduce the possibility of errors.

Regardless of which data that you are bulk loading, the bulk loading file itself must meet the following specifications:
- Use a comma as the delimiter between the values
- Save the file in a CSV format (*.csv)
• Limit file size to 52 MB

**Tip:**

Although the system upload limit is 52 MB, as a best practice, segment your bulk load files into small, manageable sets of data. For example, import just one *user* to familiarize yourself with the process. You can then import a larger set of *users*, for example, 100 *users*. If you do not experience any import errors, increase the import file size according to your level of comfort.

The bulk load file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table. At a minimum, the import file must have these exact column headings.

<table>
<thead>
<tr>
<th>Bulk Load File</th>
<th>Required Column Headings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>User ID</td>
</tr>
<tr>
<td></td>
<td>Last Name</td>
</tr>
<tr>
<td></td>
<td>First Name</td>
</tr>
<tr>
<td></td>
<td>Work Email</td>
</tr>
<tr>
<td>Groups</td>
<td>Display Name</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>User Members</td>
</tr>
<tr>
<td>Application Role Membership</td>
<td>Entitlement Value</td>
</tr>
<tr>
<td></td>
<td>Grantee Name</td>
</tr>
<tr>
<td></td>
<td>Grantee Type</td>
</tr>
</tbody>
</table>

For each account, you create a new row (line) and enter data into each column (field). Each row equals one record.

To create an import file, you can use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.

**Important:**

Whichever application you use to create the file, ensure that you save the file in a valid CSV format.

Spreadsheet applications make it easy to create, edit, and save import files. You can use standard features to add and delete rows of data, edit individual fields, search for records, or sort the list. The following illustration shows an example of group account data defined in a Microsoft Excel file. The layout lets you easily review the data.
When you save your spreadsheet as type CSV (*.csv), a comma separates the values in each row. For example, the following illustration shows the group data from the Microsoft Excel spreadsheet, saved as CSV file, and opened in Notepad.

Sample Files

To assist you to bulk load data, Oracle provides sample files for you to use. You can download the compressed sample files in the Identity Cloud Service console or from a link provided by Oracle. Whether you download the sample files from the Identity Cloud Service console or from a link provided by Oracle, the sample files are the same.

To download the sample files from the Identity Cloud Service console, click the Download sample file link.

To create an import file, you can use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.
Important:

If you’re using the sample file to import application role memberships, then make sure the column headings are Entitlement Value, Grantee Name, and Grantee Type (instead of Display Name, Member, and Member Type). If the column headings aren’t correct, then change them accordingly.

Also, if you exported application role memberships before version 17.2.2 of Oracle Identity Cloud Service, and you want to import them back into Oracle Identity Cloud Service, then you must change the column headers before doing so.

Tip:

First import the appropriate sample file with the sample data to familiarize yourself with the process. When you are comfortable with the process, delete the sample data, and then import live data.

Workflow

Before you start bulk loading data, make sure that you understand the typical bulk loading data workflow.

Workflow is described in Typical Workflow for Bulk Loading Data.

Deactivate Notifications

While you are testing, deactivate notifications so that users don’t receive unnecessary notifications.

You can deactivate all notifications or you can choose which notifications are enabled and which notifications are not enabled. See Deactivate Notifications.

Testing

Test bulk loading data with a small sample set to ensure that the import file is successfully configured.

After successful testing, you can then import live data.

View Jobs and Job Details

Review the overall status of all jobs, the details for a specific job, and download a job file on the Jobs page.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Jobs.
2. Use the following options to search for a specific job or to filter the job results that currently display:
To search for a specific job, enter your search criteria in the search field.

To specify a custom date range, click **Date Range**. To activate a date picker tool to select this range, click the **Calendar** icon in the **Start Date** and **End Date** fields.

To display jobs with only a specific status, choose a status from the **Filter by Status** drop-down list.

3. (Optional) To view the details of any job, in any job row, click **View Details**.

4. (Optional) To download a job file, in the **Job Details** view, click **Download**.

### Export Job Errors

To help you to resolve errors, export a list of the job errors.

To make it easier to review and correct errors, you can export those errors to a CSV file on your local machine.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Jobs**.

2. Locate the specific job for which you want to export errors.

   You can only export errors for a job with a **Completed with Errors** status. Jobs with a **Failed** status do not have errors to export.

3. Click **View Details**.

4. Click **Export Errors**.

   A comma-separated value (CSV) file downloads to your local machine. The CSV file contains a record for each error that includes the error type and the error description.
Run Oracle Identity Cloud Service Reports

Learn about the types of reports available and how to view Oracle Identity Cloud Service reporting data.

Topics:
- Typical Workflow for Running Oracle Identity Cloud Service Reports
- Understand the Types of Reports
- Organize the Report Data
- Run Reports

Typical Workflow for Running Oracle Identity Cloud Service Reports

With the reporting feature in Oracle Identity Cloud Service, you can run user, application, and diagnostic data reports.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the types of reports.</td>
<td>Learn about the types of reports that you can run.</td>
<td>Understand the Types of Reports</td>
</tr>
<tr>
<td>Organize the report data.</td>
<td>To improve efficiency, filter and sort the data for each report.</td>
<td>Organize the Report Data</td>
</tr>
<tr>
<td>Run reports.</td>
<td>From the Reports page, you can run reports.</td>
<td>Run Reports</td>
</tr>
</tbody>
</table>

You can run user, application, and diagnostic data reports by using:
- The Identity Cloud Service console
- SCIM-based APIs

In the following sections, you learn how to run reports by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand the Types of Reports

As an audit administrator, identity domain administrator, or application administrator, you can run operational or historical reports that capture data about Oracle Identity Cloud Service users, applications, and diagnostic log levels.

Two user reports are available with Oracle Identity Cloud Service:
• Successful Login Attempts: View users who have logged in to Oracle Identity Cloud Service successfully.
• Unsuccessful Login Attempts: View users who have not logged in to Oracle Identity Cloud Service successfully.

Two application reports are available with Oracle Identity Cloud Service:
• Application Access: View how many times users logged in to both Oracle Identity Cloud Service, and Oracle and custom applications in your identity domain.
• Application Role Privileges: View application role grants and revokes for users and groups for applications that are configured in Oracle Identity Cloud Service.

One diagnostic data report is available with Oracle Identity Cloud Service.
• Diagnostic Data: View logging data captured in Oracle Identity Cloud Service.

You can access the Auditing Users, Groups, and Applications and Performing Self-Service Diagnostics infographics to see how to run user, application, and diagnostic data reports in Oracle Identity Cloud Service.

Note:
Oracle Identity Cloud Service maintains audit logs for reports for 90 days.

Organize the Report Data

With Oracle Identity Cloud Service, you can organize the report data to increase your efficiency by:
• Filtering the report data: After you run a report, Oracle Identity Cloud Service displays the report data in tabular form, which can sometimes contain a large amount of data. Instead of scrolling through many report pages for the information that you need, refine the data by filtering it. For example, view all the report data that Oracle Identity Cloud Service recorded over a designated time interval. Or, customize a date or time range to see this data.
• Sorting the report data: Sort the report data in the table in ascending or descending order. Place the mouse pointer in a column heading to see an up-arrow button. Click the up-arrow button once to sort the data in ascending order, and click the button again to sort the data in descending order.
• Oracle Identity Cloud Service supports CSV, JSON, and PDF report generation. However, the result count for the PDF report is restricted to 1000 rows. For any report exceeding 1000 rows, only the CSV download is available.

Run Reports

To run Oracle Identity Cloud Service reports, you must be assigned to the identity domain administrator role, the audit administrator role, or the application administrator role.

See Add or Remove a User Account from an Administrator Role for more information about assigning administrator roles to users.
Run the Successful Login Attempts Report

You can use the Successful Login Attempts report to view users who have logged in to Oracle Identity Cloud Service successfully.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Reports.
2. In the Reports page, expand the Users node.
3. Click the Successful Login Attempts report. Detailed report information appears.
4. Filter the data that appears in the Successful Login Attempts report by completing one of the following options:
   • To view successful login attempts over a period of days, click 30 Days or 60 Days or 90 Days.
   • To specify a custom date range, click Custom Dates. To activate a date picker tool to select this date range, click the Calendar icon in the Start Date and End Date fields.

   **Tip:**
   You can sort the report data in the table in ascending or descending order.

5. To download a comma-separated values (CSV) version of the report, click Download Report.

Run the Unsuccessful Login Attempts Report

You can use the Unsuccessful Login Attempts report to view users who have not logged in to Oracle Identity Cloud Service successfully.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Reports.
2. In the Reports page, expand the Users node.
3. Click the Unsuccessful Login Attempts report. Detailed report information appears.
4. Filter the data that appears in the Unsuccessful Login Attempts report:
   • To view unsuccessful login attempts over a period of days, click 30 Days or 60 Days or 90 Days.
   • To specify a custom date range, click Custom Dates. To activate a date picker tool to select this date range, click the Calendar icon in the Start Date and End Date fields.

   **Tip:**
   You can sort the report data in the table in ascending or descending order.
5. To download a comma-separated values (CSV) version of the report, click Download Report.

Run the Application Access Report

You can use the Application Access report to view how many times users logged in to both Oracle Identity Cloud Service, and Oracle and custom applications in your identity domain.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Reports.
2. In the Reports page, expand the Applications node.
3. Click the Application Access report. Detailed report information appears.
4. Filter the data that appears in the Application Access report:
   • To view how many times users logged in to Oracle Identity Cloud Service, their Oracle applications, or their custom applications over a period of days, click 30 Days or 60 Days or 90 Days.
   • To specify a custom date range, click Custom Dates. To activate a date picker tool to select this date range, click the Calendar icon in the Start Date and End Date fields.

   Tip:
   You can sort the report data in the table in ascending or descending order.

5. To download a comma-separated values (CSV) version of the report, click Download Report.

Run the Application Role Privileges Report

You can use the Application Role Privileges report to view application role grants and revokes for users and groups for applications that are configured in Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Reports.
2. In the Reports page, expand the Applications node.
3. Click the Application Role Privileges report. Detailed report information appears.
4. Filter the data that appears in the Application Role Privileges report by performing one of the following options:
   • To view application role grants and revokes for applications that are configured in Oracle Identity Cloud Service over a period of days, click 30 Days or 60 Days or 90 Days.
   • To specify a custom date range, click Custom Dates. To activate a date picker tool to select this date range, click the Calendar icon in the Start Date and End Date fields.
To download a comma-separated values (CSV) version of the report, click Download Report.

### Run the Diagnostic Data Report

Use the Diagnostic Data report to view logging data captured in Oracle Identity Cloud Service for diagnostic purposes.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Diagnostics.
2. Click Diagnostics Type to set the Oracle Identity Cloud Service log level.
   - To capture high-level logging information only, select Activity View.
   - To capture both mid-level and high-level logging information, select Data View.
   - To capture detailed logging information, select Service View.
3. Click Save to activate data logging in Oracle Identity Cloud Service. You can view logging data captured over the next 15 minutes for diagnostic purposes.

### Note:

After 15 minutes, the Oracle Identity Cloud Service log level reverts to None automatically.

4. In the Identity Cloud Service console, go to the Reports page.
5. In the Reports page, expand the Diagnostics node.
6. Click the Diagnostic Data report. Detailed report information appears.
7. Filter the data that appears in the Diagnostic Data report:
   - To view logging data captured in Oracle Identity Cloud Service over a period of minutes, click 15 Minutes or 30 Minutes or 60 Minutes.
   - To specify a custom date and time range, click Custom Time. To activate date and time picker tools to select the range, click the Calendar and Clock icons in the Start Time and End Time fields.
8. Click Log Type, and then select the Activity View, Data View, or Service View log level.
   This log level contains logging data that you want Oracle Identity Cloud Service to capture.
9. To download a comma-separated values (CSV) version of the report, click Download Report.
Part IV
Configure Administrator Settings

Learn how to configure important administrative settings.

Chapters

• Change Oracle Identity Cloud Service Default Settings
• Manage Oracle Identity Cloud Service Trusted Partner Certificates
• Customize Oracle Identity Cloud Service Notifications
• Manage Oracle Identity Cloud Service Password Policies
• Brand the Oracle Identity Cloud Service Interface
• Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service
• Manage Oracle Identity Cloud Service Session Settings
• Manage Self-Registration Profiles in Oracle Identity Cloud Service
• Download Oracle Identity Cloud Service SDKs and Applications
• Customize Schemas in Oracle Identity Cloud Service
Change Oracle Identity Cloud Service Default Settings

Learn how to manage your default identity domain settings for Oracle Identity Cloud Service.

To manage default identity domain settings, you must be assigned to the identity domain administrator or security administrator role. See Add or Remove a User Account from an Administrator Role.

Topics:

- Change Default Settings
- Purge Audit Data for the Deleted User
- Obtaining the Root CA Certificate from Oracle Identity Cloud Service

Change Default Settings

Default settings are applied to your entire identity domain in the Cloud. You can specify settings such as the time zone, password recovery email, and language.

To open this page, you must be assigned the identity domain administrator role or the security administrator role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Default Settings.

2. Set the locale. Users can override the default time zone and language settings in the My Profile Details tab in the My Profile console.
   - To specify a default time zone, from the Timezone Setting drop-down list, select a time zone.
   - To specify a default language, from the Language Setting drop-down list, select a language.

   - Turn on this option to allow clients to access the tenant signing certificate without logging in to Oracle Identity Cloud Service.

Important:

Choose the language of the target audience. Do not choose a country-specific language unless you are targeting a specific country. For example, choose French to display the text to all French users. Choose French (Canada) to display the text to all Canadian French users but not other French speaking users.
• Turn off this option to prevent clients from accessing the tenant signing certificate until they authenticate by logging in to Oracle Identity Cloud Service.

4. In the Email Addresses field, provide the default contact email addresses. These email addresses appear in notifications sent to users. Enter the email addresses that you want users to contact if they need help. To separate multiple email addresses, use a comma.

5. Select Audit Retention Interval as either 30, 60 or 90 days. The tenant will purge the audit data for all the users, based on the interval set here. As an administrator, when you delete a user, you can manually purge the audit data of that user by entering the GUID. The entire audit data of that user will be deleted permanently from the Tenant.

6. Click Save.

Purge Audit Data for the Deleted User

When you delete a user, the audit data of the user remains in the system. Using Purge option, you can manually and immediately purge the audit data of that deleted user.

To purge the audit data of the deleted user, perform the following procedure:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Default Settings.

2. Under the Audit section, in the Purge audit data for the deleted user text box, enter the GUID of the deleted user and click Purge.

Obtain the Root CA Certificate from Oracle Identity Cloud Service

When you setup Service Providers and Identity Providers for Federated SSO, you need to download the metadata file and the signing and encryption certificates. However, these certificates are not self-signed and are issued by a root certificate. Hence, for a proper setup and function, you need to get the root certificate and install it at the Federation partner. Follow the procedure below to obtain the root certificate.

To obtain the root CA certificate:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Default Settings.

2. Turn on the switch under Access Signing Certificate to enable clients to access the tenant signing certificate without logging in to Oracle Identity Cloud Service.

3. Click Save to save the default settings.

4. Refer to the REST API document for the detailed installation of cURL.

5. Use this URL https://tenant-base-url/admin/v1/SigningCert/jwk as the endpoint.

6. Execute the following cURL command to save the root certification file:

   ```
curl -k -i -H "Accept: application/scim+json,application/json" --request GET "https://tenant-base-url/admin/v1/SigningCert/jwk"
   ```

   After you execute the command, the following code is returned:
7. Open a Notepad and paste the key in the following manner:

```
-----BEGIN CERTIFICATE-----
[Paste the highlighted key here]
-----END CERTIFICATE-----
```

For example (abbreviated):

```
-----BEGIN CERTIFICATE-----
"MIIDdDCCAlygAwIBAgIGAVw4Ns68MA0GCS......./VaWgoMQ6J9t9CLarai"
-----END CERTIFICATE-----
```

8. Save this file as your root certification file.
Manage User Settings in Oracle Identity Cloud Service

This section describes how to manage user settings in Oracle Identity Cloud Service.

Topics:
- Typical Workflow for Managing User Settings in Oracle Identity Cloud Service
- Change User Settings

Typical Workflow for Managing User Settings in Oracle Identity Cloud Service

With the user settings feature in Oracle Identity Cloud Service, you can perform tasks such as changing user settings. For example, you can make the primary email address for a user account a required or optional attribute.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change user settings.</td>
<td>Change settings for Oracle Identity Cloud Service user accounts using the User Settings page.</td>
<td>Change User Settings</td>
</tr>
</tbody>
</table>

You can manage user settings by:
- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage user settings by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Change User Settings

You can change settings associated with user accounts. For example, you can make the primary email address for a user account a required or optional attribute.

By making the primary email address optional, if Oracle Identity Cloud Service integrates with another cloud service or on-premises application, then a user's email address can be propagated from that service or application back into Oracle Identity Cloud Service, and designated to be the user's primary email address in Oracle Identity Cloud Service.
To change user settings, you must be assigned to the identity domain administrator role or the security administrator role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click User Settings.

2. If you don't want the primary email address to be a required attribute for user accounts, then turn on the Allow primary email address as optional switch.

   OR

   If you want the primary email address to be a required attribute, then turn off this switch.

3. Click Save.

4. In the Confirmation window, click OK.

Note:
You must sign out and sign back in to the Identity Cloud Service console for the change you made to the Allow primary email address as optional switch to take effect.
Manage Oracle Identity Cloud Service Trusted Partner Certificates

Learn how to manage trusted partner certificates for Oracle Identity Cloud Service.

Topics

• Typical Workflow for Managing Oracle Identity Cloud Service Trusted Partner Certificates
• Understand Trusted Partner Certificates
• Import a Trusted Partner Certificate
• View Details About a Trusted Partner Certificate
• Delete a Trusted Partner Certificate

Typical Workflow for Managing Oracle Identity Cloud Service Trusted Partner Certificates

With the trusted partner certificate feature in Oracle Identity Cloud Service, you can perform tasks such as importing, viewing, and deleting trusted partner certificates.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand trusted partner certificates.</td>
<td>Learn about trusted partners and trusted partner certificates.</td>
<td>Understand Trusted Partner Certificates</td>
</tr>
<tr>
<td>Import a trusted partner certificate.</td>
<td>You can import a trusted partner certificate using the Trusted Partner Certificates page.</td>
<td>Import a Trusted Partner Certificate</td>
</tr>
<tr>
<td>View details about a trusted partner certificate.</td>
<td>View details about a trusted partner certificate using the Trusted Partner Certificates page.</td>
<td>View Details About a Trusted Partner Certificate</td>
</tr>
<tr>
<td>Delete a trusted partner certificate.</td>
<td>Delete a trusted partner certificate using the Trusted Partner Certificates page</td>
<td>Delete a Trusted Partner Certificate</td>
</tr>
</tbody>
</table>

You can import, view, and delete trusted partner certificates by using:

• The Identity Cloud Service console
• SCIM-based APIs

In the following sections, you learn how to manage trusted partner certificates by using the Identity Cloud Service console.
For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Trusted Partner Certificates

In this topic, you learn about trusted partners and trusted partner certificates.

A trusted partner is any application or organization, remote to Oracle Identity Cloud Service, that communicates with Oracle Identity Cloud Service.

Oracle Identity Cloud Service uses identity propagation to communicate with a trusted partner. During identity propagation, a front-end Oracle Identity Management product, such as Oracle Access Manager, challenges a user and authenticates the user's credentials.

After the user's identity is validated, a token is generated. This token is used in place of a password to prove that the user is who he or she claims to be. The asserted identity is then passed into Oracle Identity Cloud Service. Because the identity has already been established, Oracle Identity Cloud Service trusts that it is a valid user identity, and can use it, as required.

For example, Oracle Identity Cloud Service receives a user assertion from Oracle Access Manager. As a result, a user can use Oracle Access Manager to log in to a portal associated with a trusted partner. This portal takes the user to the Home page of an order management system. The Home page displays the orders the user made from the order management system.

The first step in establishing a trusted partner is to determine the partner's role in the trust relationship. A trusted partner can be a source site (one that generates an SSO assertion) or a destination site (one that consumes an SSO assertion).

Currently, trusted partners generate SSO assertions that Oracle Identity Cloud Service consumes.

To ensure that the assertions are transmitted to Oracle Identity Cloud Service securely, the information contained in the assertions is encrypted in X.509 digital certificates. These certificates are known as trusted partner certificates.

Oracle Identity Cloud Service uses trusted partner certificates that have Distinguished Encoding Rules (DER) file extensions.

Import a Trusted Partner Certificate

You can use Oracle Identity Cloud Service to import a trusted partner certificate. To import the certificate, use a Distinguished Encoding Rules (DER) file.

See Understand Trusted Partner Certificates for more information about trusted partner certificates.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Partner Settings.

2. In the Trusted Partner Certificates page, click Import.

3. In the Import window:
   a. In the Alias field, enter an alias for the trusted partner certificate (for example, TPcert1).
The certificate that you import is an authorization certificate for the trusted partner. It contains a keystore. The keystore is used to authenticate and encrypt the data for the trusted partner for security purposes. A keystore entry is identified by an alias.

b. To locate and select the DER file that contains the trusted partner certificate to import, click Browse.

c. Verify that the path and name of the DER file you selected appear in the Certificate field.

d. Click Import.

View Details About a Trusted Partner Certificate

After importing a trusted partner certificate into Oracle Identity Cloud Service, you can view details about it.

By default, you can see the alias, SHA-1 and SHA-256 thumbprints, start date, and end date for each certificate that you import into Oracle Identity Cloud Service. You can see either the abbreviated version of a certificate (the thumbprint) or the entire certificate.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Partner Settings.

2. In the Trusted Partner Certificates page, verify that you see the following information about the imported trusted partner certificate:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The alias for the trusted partner certificate. See Import a Trusted Partner Certificate for more information about the certificate alias.</td>
</tr>
<tr>
<td>SHA-1 Thumbprint</td>
<td>A hash value computed over the complete certificate, which contains all its fields, including the signature. If SHA-1 is used as the algorithm to encrypt the certificate, then the encrypted value appears in this column. Otherwise, the column is empty.</td>
</tr>
<tr>
<td>SHA-256 Thumbprint</td>
<td>If SHA-256 is used as the algorithm to encrypt the certificate, then the encrypted value appears in this column. Otherwise, the column is empty.</td>
</tr>
<tr>
<td>Certificate Start Date</td>
<td>The date and time after which Oracle Identity Cloud Service can use the certificate to authenticate the trusted partner.</td>
</tr>
<tr>
<td>Certificate End Date</td>
<td>The date and time after which Oracle Identity Cloud Service can no longer use the certificate to authenticate the trusted partner.</td>
</tr>
</tbody>
</table>

3. You can view the entire trusted partner certificate, as opposed to the certificate’s thumbprint. To do so, select the certificate and click View. After viewing the certificate, click OK.
Delete a Trusted Partner Certificate

You can use Oracle Identity Cloud Service to remove a trusted partner certificate.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Partner Settings**.
2. In the **Trusted Partner Certificates** page, click the certificate that you want to remove, and click **Delete**.
3. In the **Confirmation** window, click **OK**.
Customize Oracle Identity Cloud Service Notifications

Learn how to customize notifications for Oracle Identity Cloud Service users and administrators.

Topics:
• Typical Workflow for Customizing Oracle Identity Cloud Service Notifications
• Understand the Types of Notifications
• Understand How to Customize Notifications
• Activate Notifications
• Select Notifications
• Specify Recipients for Notifications
• Modify Notification Templates
• Verify Notifications
• Deactivate Notifications

Typical Workflow for Customizing Oracle Identity Cloud Service Notifications

With the notification feature in Oracle Identity Cloud Service, you can customize and use notifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the types of notifications.</td>
<td>You can learn about the types of Oracle Identity Cloud Service notifications that you can customize for users and administrators.</td>
<td>Understand the Types of Notifications</td>
</tr>
<tr>
<td>Understand how to customize notifications.</td>
<td>You can examine a workflow that illustrates how to customize notifications in Oracle Identity Cloud Service.</td>
<td>Understand How to Customize Notifications</td>
</tr>
<tr>
<td>Activate notifications.</td>
<td>You can activate notifications using the Notifications page.</td>
<td>Activate Notifications</td>
</tr>
<tr>
<td>Select notifications.</td>
<td>You can select notifications using the Notifications page.</td>
<td>Select Notifications</td>
</tr>
<tr>
<td>Specify recipients for notifications.</td>
<td>You can specify recipients for notifications using the Notifications page.</td>
<td>Specify Recipients for Notifications</td>
</tr>
</tbody>
</table>
### Understand the Types of Notifications

You can customize and use notifications by using:
- The Identity Cloud Service console
- SCIM-based APIs

In this section, you learn how to customize notifications by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

#### About User Notifications

Learn about the various user notifications available in Oracle Identity Cloud Service.

The following user notifications are available in Oracle Identity Cloud Service:

---

**Table: Notification Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify notification templates.</td>
<td>You can modify notification templates using the Notifications page.</td>
<td>Modify Notification Templates</td>
</tr>
<tr>
<td>Verify notifications.</td>
<td>You can verify the customizations that you make to Oracle Identity Cloud Service notification templates.</td>
<td>Verify Notifications</td>
</tr>
<tr>
<td>Deactivate notifications.</td>
<td>You can deactivate notifications using the Notifications page.</td>
<td>Deactivate Notifications</td>
</tr>
</tbody>
</table>

---

**Tip:**

In addition to customizing notifications for other Oracle Identity Cloud Services users and administrators, you can also view and act on email notifications that require your attention. To access these notifications, click Notifications in the upper-right corner of the Console. See Get Started with Oracle Identity Cloud Service.

**Topics:**

- About User Notifications
- About Administrator Notifications
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>A user is notified that an administrator created an account for the user. The notification contains a link that the user clicks to activate the account.</td>
</tr>
<tr>
<td>Self-Registration Email Verification</td>
<td>After a user creates an account successfully through the self-registration process, this notification is sent to the user to verify the user's email address.</td>
</tr>
<tr>
<td>Welcome Federated SSO User</td>
<td>A federated SSO user is notified that an administrator created an account for the user. The notification contains a link that the user clicks to activate the account.</td>
</tr>
<tr>
<td>Welcome Delegated Authentication User</td>
<td>A user whose authentication is delegated is notified that an administrator created an account for the user. The notification contains a link that the user clicks to activate the account.</td>
</tr>
<tr>
<td>Resend Welcome</td>
<td>If a user doesn't activate the account using the link provided in the Welcome notification, then the administrator can send this notification. The user is notified again that the administrator created the account for the user. The notification contains a link that the user clicks to activate the account.</td>
</tr>
<tr>
<td>Resend Welcome To Delegated Authentication User</td>
<td>If a user whose authentication is delegated doesn't activate the account using the link provided in the Welcome Delegated Authentication User notification, then the administrator can send this notification. The user is notified again that the administrator created the account for the user. The notification contains a link that the user clicks to activate the account.</td>
</tr>
<tr>
<td>Password Recovery Request</td>
<td>This notification is sent to a user if the user requests a password reset. This notification contains a URL that the user clicks to be redirected to the Password Reset page. The user provides a password as part of the password recovery process. After the activation process is complete, the user is logged in automatically.</td>
</tr>
<tr>
<td>Recovery Email Verification</td>
<td>After a user changes their password recovery email address, this notification is sent to the user to verify the address.</td>
</tr>
<tr>
<td>Primary Email Verification</td>
<td>After a user changes their primary email address, this notification is sent to the user to verify the address.</td>
</tr>
<tr>
<td>Secondary Email Verification</td>
<td>After a user changes their secondary email address, this notification is sent to the user to verify the address.</td>
</tr>
<tr>
<td>Password Change</td>
<td>This notification is sent to the user to inform the user that the password was changed successfully. This event is initiated by the user.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Reset</td>
<td>This notification is sent to the user to inform the user that the password was reset successfully. This event is initiated by the user.</td>
</tr>
<tr>
<td>Password Has Been Changed by an Administrator to a Known Value</td>
<td>This notification is sent to users when the administrator changes the passwords for users to a known value. This notification is used for testing purposes only. Both the administrator and the users know the common password.</td>
</tr>
<tr>
<td>Admin Requesting a Password Reset on Behalf of a User</td>
<td>This notification is sent to a user if the administrator initiates changing the password for the user. The system creates a randomly generated value for the password. If the administrator initiates resetting the password for the user, then a notification is sent to the user along with a URL where the user can reset the password.</td>
</tr>
<tr>
<td>User Activation</td>
<td>A user is notified that an administrator activated the user's account. The notification contains a link that the user clicks to log in to the account.</td>
</tr>
<tr>
<td>User De-activation</td>
<td>A user is notified that an administrator deactivated the user's account.</td>
</tr>
<tr>
<td>User Account Locked</td>
<td>This notification is sent to a user if the user account is locked because the user was unsuccessful in logging in after a consecutive number of attempts. This notification contains a link that the user can click to unlock the account.</td>
</tr>
<tr>
<td>Exceeded Maximum Number of Account Recovery Attempts</td>
<td>After a user exceeds the maximum number of attempts to reset their password to recover their account, this notification is sent to the user's primary email address.</td>
</tr>
<tr>
<td>User Account Unlocked</td>
<td>This notification is sent to a user after the user's account is unlocked. This occurs after the user accesses the link in the User Locked notification to unlock the account.</td>
</tr>
<tr>
<td>User Profile Updated by Administrator</td>
<td>An administrator can update a user's profile by changing attribute values associated with the user's account. A notification is sent to the user. A user can modify their profile and receive the same notification. The user accesses the My Profile page to see the modifications made to the profile. The changes appear in a different foreground or background color.</td>
</tr>
<tr>
<td>User Profile Replaced by Administrator</td>
<td>An administrator can replace attribute values of a user's profile. A notification is sent to the user. A user can replace attribute values of their profile and receive the same notification. The user accesses the My Profile page to see the attribute value replacements made to the profile. The changes appear in a different foreground or background color.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
Device Enrollment Request to Enable 2-Step Verification | This notification contains instructions and links about how to download the Oracle Mobile Authenticator app. It also has an enrollment URL. After the user downloads the app, the user taps the enrollment URL to configure the user account in the app.

2-Step Verification User Account Locked | This notification is sent to a user if the user account is locked because of unusual activity detected on the account as part of the two-step verification process.

2-Step Verification Federated SSO User Account Locked | This notification is sent to a federated SSO user if the user account is locked because of unusual activity detected on the account as part of the two-step verification process.

2-Step Bypass Code Verification | This notification contains a bypass code that is generated by the administrator or user. The user can use this bypass code to complete the two-step verification process.

Enable Kerberos Authentication Request | This notification is sent to a user who's assigned to a Kerberos application for the first time. By clicking the link in the notification, the user logs into Oracle Identity Cloud Service, which enables generation of long-term keys. This is a prerequisite for Kerberos authentication. The user can then use the principal name provided in the notification and the Oracle Identity Cloud Service password to access the Kerberos application to perform authentication to applications that support it.

New Access Request Submitted | This notification is sent to a user after they submit an access request.

Access Request Fulfilled | This notification is sent to a user after their access request has been fulfilled.

2-Step Email One-Time Passcode Verification | This notification contains a one-time passcode (OTP) that's sent to a user. The user uses this OTP to complete 2-Step Verification.

New Device Login Detected with Your Account | If an attempt is made to log in to a user's account from a device, IP address, or web browser, and Oracle Identity Cloud Service doesn't recognize that the device, address, or browser is associated with the account, then this notification is sent to the user. The notification contains a link that the user can click to reset their SSO password in case the user doesn't recognize the login attempt.

### About Administrator Notifications

Learn about the various administrator notifications available in Oracle Identity Cloud Service.

The following administrator notifications are available in Oracle Identity Cloud Service:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Has Been Started</td>
<td>An administrator is notified that a job for importing or exporting Oracle Identity Cloud Service groups, users, or application roles, or for resetting passwords for all Oracle Identity Cloud Service users, has been started.</td>
</tr>
<tr>
<td>Job Has Been Canceled</td>
<td>An administrator is notified that a job for importing or exporting Oracle Identity Cloud Service groups, users, or application roles, or for resetting passwords for all Oracle Identity Cloud Service users, has been canceled.</td>
</tr>
<tr>
<td>Job Is Complete</td>
<td>An administrator is notified that a job for importing or exporting Oracle Identity Cloud Service groups, users, or application roles, or for resetting passwords for all Oracle Identity Cloud Service users, is complete.</td>
</tr>
<tr>
<td>Job Has Failed</td>
<td>An administrator is notified that a job for importing or exporting Oracle Identity Cloud Service groups, users, or application roles, or for resetting passwords for all Oracle Identity Cloud Service users, has failed.</td>
</tr>
<tr>
<td>Quota Limit Exceeded</td>
<td>This notification is sent to an administrator when the administrator has exceeded the allowed resource quota for the Oracle Identity Cloud Service instance. To increase the quota limit, upgrade to Oracle Identity Cloud Service Basic or Oracle Identity Cloud Service Standard.</td>
</tr>
<tr>
<td>From Email Domain Validation Initiated</td>
<td>An administrator is notified that validation of the email domain that's entered in the email address in the From Email Address field on the Notifications page has been initiated, and a validation email will be sent to the postmaster account of this domain.</td>
</tr>
<tr>
<td>Email Address Validation Initiated for From Email Address</td>
<td>An administrator is notified that validation of the email address that's entered in the From Email Address field on the Notifications page has been initiated, and a validation email will be sent to this email address.</td>
</tr>
</tbody>
</table>

**Note:**
The Job Has Been Started, Job Has Been Canceled, Job is Complete, and Job Has Failed administrator notifications contain a link. Clicking the link for each notification takes the administrator to the Jobs Status page of the console where the administrator can view details about the job.

**Understand How to Customize Notifications**

Oracle Identity Cloud Service provides you with email templates for user and administrator notifications.

See About User Notifications for a listing of these notification templates.
You can tailor the recipients and content of these templates to meet the business and security requirements for your enterprise applications.

The following workflow illustrates how to customize notifications in Oracle Identity Cloud Service:

1. **Activate Notifications.** By activating notifications, you enable Oracle Identity Cloud Service to send notifications to users and administrators. See [Activate Notifications](#).

2. **Select Notifications.** After activating notifications in Oracle Identity Cloud Service, you can select notifications to customize. See [Select Notifications](#).

3. **Specify Recipients for Notifications.** After activating and selecting notifications, you can configure Oracle Identity Cloud Service to send the notifications either to all Oracle Identity Cloud Service users or to a limited number of recipients (for testing purposes). See [Specify Recipients for Notifications](#).

4. **Modify Notification Templates.** After activating and selecting notifications, and specifying their recipients, you can modify the notification templates that you selected. See [Modify Notification Templates](#).

5. **Verify Notifications.** You can verify the customizations that you made to the Oracle Identity Cloud Service notification templates you selected. See [Verify Notifications](#).

6. **Deactivate Notifications.** By deactivating notifications, you prevent Oracle Identity Cloud Service from sending notifications to users and administrators. See [Deactivate Notifications](#).

You can access the [Customizing the Service infographic](#) to see how to customize notifications.

---

### Activate Notifications

By activating notifications, you enable Oracle Identity Cloud Service to send notifications to users and administrators.

To activate notifications, you must be assigned to either the identity domain administrator role or the security administrator role. See [Add or Remove a User Account from an Administrator Role](#).

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Notifications**.

2. Turn on the **Status** switch.

3. To send a validation email to the postmaster account of the email's domain, click **Domain**. After the domain is verified, any email address from the domain is valid.

   OR

   To send a validation email to the email address that you enter in the **From Email Address** field, click **Email**. Unlike the **Domain** option, a validation is initiated for every email address even though they’re from the same domain.

4. In the **From Email Address** field, enter the email address that will appear in the **From Email** field for all notifications.

5. Click **Save**.

   If you selected **Domain** in step 2, then an email notification will be sent to the postmaster to verify the email address and validate the domain associated with the
address. Otherwise, if you selected Email, then a validation email will be sent to the email address that you entered in the From Email Address field.

6. In the Confirmation window, click OK.

7. If you see a Pending Domain Verification or Pending Email Verification status, then click Check Status.

   Oracle Identity Cloud Service checks whether verification is done to the email address through the email sent to the postmaster or email account. If it's verified, then the status changes from Pending Domain Verification to Domain Verified or from Pending Email Verification to Email Verified. If it's not verified, then the status remains as Pending Domain Verification or Pending Email Verification.

8. If the email address isn't verified, then access the notification that's sent to the email address you provided, click the verification link in the notification, and click Check Status again. The status will change to Email Verified.

OR

9. If the domain isn't verified, then contact the postmaster of your company so that the postmaster can verify the domain associated with the email address.

Select Notifications

After activating notifications in Oracle Identity Cloud Service, you can select notifications to customize.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Notifications.

2. Click Configure.

   On this tab, you see a "master list" of user and administrator notifications that you can select.

3. Select the check box for each notification that you want to customize.

4. Click Save.

5. In the Confirmation window, click OK.

Specify Recipients for Notifications

After activating and selecting notifications, you can configure Oracle Identity Cloud Service to send the notifications either to all Oracle Identity Cloud Service users or to a limited number of recipients (for testing purposes).

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Notifications.

2. Click Recipients.

3. Set the Limited Recipients List switch.

   • To send the notifications you selected to all Oracle Identity Cloud Service users, turn the switch Off.

   • To send the notifications to a limited number of recipients, turn the switch On. In the Testing Email Addresses text area, enter the email addresses of the users who will receive the notifications. Use commas to separate email addresses.
4. Click **Save**.
5. In the **Confirmation** window, click **OK**.

# Modify Notification Templates

After activating and selecting notifications, and specifying their recipients, you can modify the notification templates that you selected. To meet the business and security requirements for your enterprise applications, tailor the content of these notifications.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Notifications**.
2. Click **Email Templates**.

**Tip:**

The notification templates that appear in the **Email Templates** tab reflect the selections you made in the **Configure** tab. See **Select Notifications**.

3. Expand a notification template by clicking the right-arrow button that’s associated with the template.
4. To modify a notification template, use the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Select the language for the notification. To see a preview of the notification in the language you select, click <strong>View</strong> and access the <strong>Email Body</strong> text area.</td>
</tr>
<tr>
<td>Encoding</td>
<td>Verify that UTF-8 appears as the character encoding for the notification (for security, encryption, and backward-compatibility purposes). This character encoding can encode all possible characters of the notification, or code points, in Unicode.</td>
</tr>
</tbody>
</table>

**Important:**

When adding or changing a variable in an email template, ensure that you use the correct syntax. For example, to use the variable `user.displayName`, the correct syntax is `${user.displayName}`.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Email</td>
<td>Verify that the email address for this field matches the email address you entered in the From Email Address field. This field is the email address that will appear in the From Email field for all notifications. If you haven’t verified the domain or the email address, then this value will be the previously validated email address or email address from the previously validated domain. As soon as the domain or the email address is validated (the status changes from Pending Domain Validation or Pending Email Verification to Domain Verified or Email Verified), then the verified email address will appear in the From Email Address field for all notifications.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter or provide variables for content that appears in the Subject field of the email notification.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Email Body          | The content of the notification template. In this text area, you can customize the content to meet your needs. In addition to a customization toolbar, Oracle Identity Cloud Service provides you with variables to use. These variables are replaced with values specific to your business at runtime. They are:  
  - $(account.emailID): The email address of the user's account from which an attempt is made to log in using a device, IP address, or web browser that Oracle Identity Cloud Service doesn't recognize.  
  - $(actorDisplayName): The identity domain administrator's email address  
  - $(admin.resource.name): The name of the Kerberos application  
  - $(authentication.targetApp): The name of the Microsoft Active Directory domain that contains the account of the user who's authenticating into Oracle Identity Cloud Service  
  - $(bypasscode.expiry): The time (in minutes) before a bypass code expires  
  - $(bypasscode.usage): How many times a bypass code can be used  
  - $(bypasscode.value): The bypass code that the user or administrator generates for use as part of the 2-Step Verification process  
  - $(companyName): The name of the company that will appear in the notification  

Note: When you use the $(companyName) variable, be sure to add your company name to the Company Name field in the Branding page. If you don't, then your company's details won't appear in email notifications, SMS notifications, or in the Oracle Mobile Authenticator (OMA) app when a user completes MFA enrollment. See Customize the Sign In Page for more information about populating the Company Name field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${contactEmails}</code></td>
<td>The system administrator's email address</td>
</tr>
<tr>
<td><code>${date}</code></td>
<td>The date associated with the action of the notification (for example, resetting a password)</td>
</tr>
<tr>
<td><code>${device.ipAddress}</code></td>
<td>The IP address from which an attempt is made to log in to a user's account, but which Oracle Identity Cloud Service doesn't recognize.</td>
</tr>
<tr>
<td><code>${device.enrollmentURL}</code></td>
<td>The configuration URL containing parameters used to configure the Oracle Mobile Authenticator app</td>
</tr>
<tr>
<td><code>${domain}</code></td>
<td>The realm (or domain) that contains the Kerberos application</td>
</tr>
<tr>
<td><code>${email}</code></td>
<td>The email address that appears in the From Email Address field</td>
</tr>
<tr>
<td><code>${emailId}</code></td>
<td>The user's email address</td>
</tr>
<tr>
<td><code>${footerImage}</code></td>
<td>The image that will appear in the footer region of the notification</td>
</tr>
<tr>
<td><code>${headerImage}</code></td>
<td>The image that will appear in the header region of the notification</td>
</tr>
<tr>
<td><code>${homePageRedirectUrl}</code></td>
<td>The redirect URL for the notification that can be used if the link in the notification doesn't work. This URL redirects users to the Home page of Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td><code>${job.displayName}</code></td>
<td>The display name of the job that's started, canceled, completed, or failed</td>
</tr>
<tr>
<td><code>${job.historyId}</code></td>
<td>The ID number of the job that's started, canceled, completed, or failed</td>
</tr>
<tr>
<td><code>${kerberos.principalName}</code></td>
<td>The Kerberos principal name that the user uses to access the Kerberos application to perform authentication to applications that support it</td>
</tr>
<tr>
<td><code>${linkExpirationTime}</code></td>
<td>A date-and-time stamp, after which the link in the notification will be expired</td>
</tr>
<tr>
<td><code>${masked_UID}</code></td>
<td>The account of the user who requests a one-time passcode (OTP) to enroll in 2–Step Verification.</td>
</tr>
<tr>
<td><code>${OTP}</code></td>
<td>The one-time passcode (OTP) that's sent to a user for the user to complete 2–Step Verification.</td>
</tr>
<tr>
<td><code>${quota.limit}</code></td>
<td>The allowable quota limit for the resource type. If an administrator can create 500,000 user accounts, then 500,000 represents the quota limit.</td>
</tr>
<tr>
<td><code>${quota.resourceType}</code></td>
<td>The classification type of the Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Cloud Service entity (or resource) for which there is a quota limit (for example, users)</td>
</tr>
<tr>
<td></td>
<td>• ${quota.usage}: Records of the resource type that were created. If an administrator created 600,000 accounts, then 600,000 represents the quota usage.</td>
</tr>
<tr>
<td></td>
<td>• ${redirectUrl}: The redirect URL for the notification that can be used if the link in the notification doesn’t work</td>
</tr>
<tr>
<td></td>
<td>• ${request.createdOn}: The date and time that the request was created</td>
</tr>
<tr>
<td></td>
<td>• ${request.requestedItem}: The groups or applications to which a user is requesting access</td>
</tr>
<tr>
<td></td>
<td>• ${request.requesteeDisplayName}: The display name of the user who submitted a request for access to groups or applications</td>
</tr>
<tr>
<td></td>
<td>• ${tenantName}: The name of the identity domain (or tenant)</td>
</tr>
<tr>
<td></td>
<td>• ${time}: The time associated with the action of the notification</td>
</tr>
<tr>
<td></td>
<td>• ${user.displayName}: The user’s first and last name (or display name)</td>
</tr>
<tr>
<td></td>
<td>• ${user.userName}: The user’s username</td>
</tr>
<tr>
<td></td>
<td>• ${userToken}: A token that Oracle Identity Cloud Service uses to identify the user</td>
</tr>
<tr>
<td></td>
<td>• ${validity}: The amount of time (in minutes), after which the OTP will no longer be valid. As a result, the user can’t use it to enroll in 2–Step Verification.</td>
</tr>
</tbody>
</table>

**Tip:**

To undo the changes that you make to a notification template, click **Cancel**. If you click **Cancel**, then all your changes are lost.

5. Click **Save**.
6. In the **Confirmation** window, click **OK**.

**Verify Notifications**

You can verify the customizations that you made to the Oracle Identity Cloud Service notification templates you selected. Oracle recommends that you first test the customizations by sending the notifications to a limited number of recipients.

See **Specify Recipients for Notifications**.

To verify your notification customizations, use the following table.
<table>
<thead>
<tr>
<th>Notification</th>
<th>Action (Administrator)</th>
<th>Action (User)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Create an account for a user.</td>
<td>Complete the self-registration process to create a user account.</td>
</tr>
<tr>
<td>Self-Registration Email Verification</td>
<td></td>
<td>Confirms email in the Self-Registration Email Verification notification.</td>
</tr>
<tr>
<td>Welcome Self-Registration User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome Federated SSO User</td>
<td>Create an account for a federated SSO user.</td>
<td></td>
</tr>
<tr>
<td>Welcome Delegated Authentication User</td>
<td>Create an account for a user whose authentication is delegated.</td>
<td></td>
</tr>
<tr>
<td>Resend Welcome</td>
<td>Resend Invitation to user.</td>
<td>Receive another notification that the administrator resent the Welcome notification.</td>
</tr>
<tr>
<td>Resend Welcome To Delegated Authentication User</td>
<td>Resend Invitation to user authenticated by other than Oracle Identity Cloud Service.</td>
<td>Receive another notification that the administrator resent the Welcome notification for the user whose authentication is delegated.</td>
</tr>
<tr>
<td>Password Recovery Request</td>
<td></td>
<td>Request a password reset.</td>
</tr>
<tr>
<td>Recovery Email Verification</td>
<td>Create an account for a user and provide a password recovery email address for the user in the Recovery Email field.</td>
<td>Change the password recovery email address.</td>
</tr>
<tr>
<td>Primary Email Verification</td>
<td>Create an account for a user and provide a primary email address for the user in the Email field.</td>
<td>Change the primary email address.</td>
</tr>
<tr>
<td>Secondary Email Verification</td>
<td>Create an account for a user and provide a secondary email address for the user in the Email field.</td>
<td>Change the secondary email address.</td>
</tr>
<tr>
<td>Recovery Email Update</td>
<td>Updates Recovery Email field.</td>
<td></td>
</tr>
<tr>
<td>Primary Email Update</td>
<td>Updates Email field.</td>
<td></td>
</tr>
<tr>
<td>Secondary Email Update</td>
<td>Updates any secondary Email field.</td>
<td></td>
</tr>
<tr>
<td>Password Change</td>
<td></td>
<td>Change the password.</td>
</tr>
<tr>
<td>Password Reset</td>
<td></td>
<td>Reset the password.</td>
</tr>
<tr>
<td>Password Has Been Changed by an Administrator to a Known Value</td>
<td>Change the password for a user to a known value.</td>
<td></td>
</tr>
<tr>
<td>Admin Requesting a Password Reset on Behalf of a User</td>
<td>Initiate changing a user’s password.</td>
<td></td>
</tr>
<tr>
<td>User Activation</td>
<td>Activate a user’s account.</td>
<td></td>
</tr>
<tr>
<td>User De-activation</td>
<td>Deactivate a user’s account.</td>
<td></td>
</tr>
<tr>
<td>Notification</td>
<td>Action (Administrator)</td>
<td>Action (User)</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Account Locked</td>
<td>Lock the account by logging in to Oracle Identity Cloud Service unsuccessfully for a</td>
<td>Exceed the maximum number of attempts to reset your password to recover your</td>
</tr>
<tr>
<td></td>
<td>consecutive number of attempts.</td>
<td>account.</td>
</tr>
<tr>
<td>Exceeded Maximum Number of Account Recovery Attempts</td>
<td>Exceed the maximum number of attempts to reset your password to recover your account.</td>
<td></td>
</tr>
<tr>
<td>User Account Unlocked</td>
<td>Unlock the account.</td>
<td></td>
</tr>
<tr>
<td>User Profile Updated by Administrator</td>
<td>Update the user's profile.</td>
<td>Update the profile.</td>
</tr>
<tr>
<td>User Profile Replaced by Administrator</td>
<td>Replace attribute values of the user's profile.</td>
<td>Replace attribute values of the profile.</td>
</tr>
<tr>
<td>Device Enrollment Request to Enable 2-Step Verification</td>
<td>Select the Mobile App option during enrollment and click the Email option to send the</td>
<td></td>
</tr>
<tr>
<td>2-Step Verification User Account Locked</td>
<td>Perform unusual activity on the account, such as entering an OTP incorrectly too many</td>
<td>Perform unusual activity on the account, such as entering an OTP incorrectly</td>
</tr>
<tr>
<td></td>
<td>times, an SMS text code incorrectly too many times, or using an untrusted device to</td>
<td>too many times, an SMS text code incorrectly too many times, or using an</td>
</tr>
<tr>
<td></td>
<td>perform 2–Step Verification.</td>
<td>untrusted device to perform 2–Step Verification.</td>
</tr>
<tr>
<td>2-Step Verification Federated SSO User Account Locked</td>
<td>Perform unusual activity on the account, such as entering an OTP incorrectly too many</td>
<td></td>
</tr>
<tr>
<td></td>
<td>times, an SMS text code incorrectly too many times, or using an untrusted device to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>perform 2–Step Verification.</td>
<td></td>
</tr>
<tr>
<td>2-Step Bypass Code Verification</td>
<td>Generate a bypass code and click the Email option.</td>
<td>Generate a bypass code and click the Email option.</td>
</tr>
<tr>
<td>Enable Kerberos Authentication Request</td>
<td>Log in to Oracle Identity Cloud Service. Use the Kerberos principal name provided in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the notification and the Oracle Identity Cloud Service password for the Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>application.</td>
<td></td>
</tr>
<tr>
<td>New Access Request Submitted</td>
<td>Request access to groups or applications from the Catalog.</td>
<td>Request access to groups or applications from the Catalog.</td>
</tr>
<tr>
<td>Access Request Fulfilled</td>
<td>Request access to groups or applications from the Catalog.</td>
<td></td>
</tr>
<tr>
<td>2–Step Email One-Time Passcode Verification</td>
<td>Enroll in 2–Step Verification by using a mobile number as an authentication method.</td>
<td></td>
</tr>
</tbody>
</table>
### Deactivate Notifications

You prevent Oracle Identity Cloud Service from sending notifications to users and administrators by deactivating notifications.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Notifications.

2. Turn Off the Status switch.

3. Click Save.

4. In the Confirmation window, click OK.
15

Manage Oracle Identity Cloud Service Password Policies

Learn how to manage password policies for Oracle Identity Cloud Service.

Topics

• Typical Workflow for Managing Oracle Identity Cloud Service Password Policies
• Understand the Types of Password Policies
• Understand the Criteria for Password Policies
• Set the Password Policy for Your Identity Domain
• Test a Password Policy
• Modify the Custom Password Policy
• Evaluate Password Policies

Typical Workflow for Managing Oracle Identity Cloud Service Password Policies

With the password management feature in Oracle Identity Cloud Service, you can perform tasks such as setting, testing, modifying, and evaluating password policies.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the types of password policies.</td>
<td>You can learn about password policies, including the three types of policies: Simple, Standard, and Custom.</td>
<td>Understand the Types of Password Policies</td>
</tr>
<tr>
<td>Understand the criteria for password policies.</td>
<td>You can learn about criteria for Simple, Standard, and Custom password policies.</td>
<td>Understand the Criteria for Password Policies</td>
</tr>
<tr>
<td>Set the password policy for your identity domain.</td>
<td>You can set the password policy for your identity domain using the Password Policy page.</td>
<td>Set the Password Policy for Your Identity Domain</td>
</tr>
<tr>
<td>Test a password policy.</td>
<td>You can test the criteria for a password policy using the Password Policy page.</td>
<td>Test a Password Policy</td>
</tr>
<tr>
<td>Modify the Custom password policy.</td>
<td>You can modify the Custom password policy using the Password Policy page.</td>
<td>Modify the Custom Password Policy</td>
</tr>
<tr>
<td>Evaluate password policies.</td>
<td>You can evaluate the Simple, Standard, or Custom password policy that you set for your identity domain.</td>
<td>Evaluate Password Policies</td>
</tr>
</tbody>
</table>
You can set, test, modify, and evaluate Simple, Standard, and Custom password policies by using:

- The Identity Cloud Service console
- SCIM-based APIs

In this section, you learn how to manage password policies by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand the Types of Password Policies

A password policy that you set in Oracle Identity Cloud Service is applicable for all users in an identity domain.

When a user is created or when a user changes their password, Oracle Identity Cloud Service validates the password that's provided against the password policy to ensure that it meets the criteria for the policy. When a user logs in for the first time to change the password, or resets the password at any time, the password policy is evaluated.

There are three types of password policies in Oracle Identity Cloud Service:

**Simple**
Used for your developer services, trial Cloud services, and demos when you don't want to customize a policy for them. You can't modify this type of password policy.

**Standard**
Used when you don't want to use the Oracle-recommended password policy for your enterprise applications. You can't modify this type of password policy.

**Custom**
Used to tailor the strength of your password policy to meet the business and security requirements for your enterprise applications. As an administrator, it's your responsibility to make the minimal requirements of the Custom password policy strong.

Understand the Criteria for Password Policies

You can use Simple, Standard, or Custom password policies in Oracle Identity Cloud Service. The default settings for Simple, Standard, or Custom password policies are:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Simple</th>
<th>Standard</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length (characters)</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Maximum length (characters)</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>Password expires after (days)</td>
<td>Never</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>User account is locked (after consecutive, unsuccessful attempts)</td>
<td>20</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
### Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Simple</th>
<th>Standard</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can use previous passwords</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Alphabetic characters (minimum)</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Numeric characters (minimum)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Lowercase characters (minimum)</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Uppercase characters (minimum)</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Can contain the user's first name</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can contain the user's last name</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can contain the user's user name</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can contain a whitespace character</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

You can't modify the Simple or Standard password policy. You can modify the Custom password policy. See Modify the Custom Password Policy to learn how to tailor the strength of this password policy to meet the business and security requirements for your enterprise applications.

---

### Set the Password Policy for Your Identity Domain

The password policy that you set applies to all users in your identity domain.

To set the password policy for your identity domain, you must be assigned to either the identity domain administrator role or the security administrator role. See Add or Remove a User Account from an Administrator Role.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Password Policy**.
2. Click **Change Your Password Policy**.
3. Click the button that represents the type of policy that you want to set for your identity domain (**Simple**, **Standard**, or **Custom**).
4. Click **Save**.
5. In the **Save Password Policy** dialog box, select the **Force all users to set a new password on their next login** check box.

Do this to ensure that their passwords meet the criteria for the policy before the users can use Oracle Identity Cloud Service.

Otherwise, don't select the **Force all users to set a new password on their next login** check box. The password policy applies to users only when they are created or when they reset their passwords.

6. Complete one of the following actions:
   - To save the updated password policy, click **OK**.
• To reinstate the previously saved password policy, click Cancel.

Test a Password Policy

After setting the password policy for your identity domain, you can test the criteria for the policy to validate that the password policy has been set.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Password Policy.
2. Click Test Your Password Policy.
3. In the New Password field of the Test Your Password Policy dialog box, enter the password that you want to test.
   As the password meets a criterion for the policy, the associated red X mark changes to a green check mark. After all criteria are met, all red X marks appear as green check marks.

Modify the Custom Password Policy

Oracle Identity Cloud Service provides you with a Custom password policy that contains predefined settings. You can tailor the strength of this policy to meet the business and security requirements for your enterprise applications.

See Understand the Criteria for Password Policies for a listing of the predefined settings for the Custom password policy.

You can access the Customizing the Service infographic to see how to customize a password policy in Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Password Policy.
2. Click Change Your Password Policy.
3. Click Custom.
4. To modify the Custom password policy, use the following list:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password length (min size)</td>
<td>How many characters the password must contain</td>
</tr>
</tbody>
</table>

Note:
A password must contain at least one character.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password length (max size)</td>
<td>How many characters are allowed for the password</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>A password can’t exceed 256 characters.</td>
</tr>
<tr>
<td>Expires after (days)</td>
<td>How many days until the password expires</td>
</tr>
<tr>
<td>Account lock threshold</td>
<td>The number of consecutive, unsuccessful login attempts into Oracle Identity Cloud Service after which the user account is locked</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If you enter 0 in the <strong>Account lock threshold</strong> field, then the user’s account will never be locked.</td>
</tr>
<tr>
<td>Enable auto unlock account</td>
<td>To enable users to automatically unlock their accounts in Oracle Identity Cloud Service after a configured time.</td>
</tr>
<tr>
<td>Auto unlock account after (minutes)</td>
<td>The amount of time (in minutes), after which Oracle Identity Cloud Service will unlock an account automatically. You can set a value ranging between 5 minutes and 24 hours.</td>
</tr>
<tr>
<td>Previous passwords remembered</td>
<td>How many unique new passwords a user must use before an old password can be reused</td>
</tr>
<tr>
<td>Alphabetic (min)</td>
<td>How many alphabetic characters the password must contain</td>
</tr>
<tr>
<td>Numeric (min)</td>
<td>How many numeric characters the password must contain</td>
</tr>
<tr>
<td>Special (min)</td>
<td>How many special characters the password must contain</td>
</tr>
<tr>
<td>Lowercase (min)</td>
<td>How many lowercase characters the password must contain</td>
</tr>
<tr>
<td>Uppercase (min)</td>
<td>How many uppercase characters the password must contain</td>
</tr>
<tr>
<td>Unique (min)</td>
<td>How many unique characters a password must contain. Increasing the number of unique characters in a password can increase password strength by avoiding repetitive sequences that are easily guessed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Repeated (max)</td>
<td>How many repeated characters are allowed for the password. This rule limits the use of repeating characters in a password. This value provides extra security by preventing users from specifying passwords that are easy to guess, such as the same character repeated several times.</td>
</tr>
<tr>
<td>Starts with (Alphabetic character)</td>
<td>To force the first character of the password to be an alphanumeric character, select this check box.</td>
</tr>
<tr>
<td>Required Characters</td>
<td>To activate the text field to the right of the check box, select the check box. Any alphanumeric or special characters that you enter into this field, separated by commas, are required characters for the password.</td>
</tr>
<tr>
<td>User attributes (The user’s first name)</td>
<td>To prevent the user’s first name from being used as all or part of the password, select this check box.</td>
</tr>
<tr>
<td>User attributes (The user’s last name)</td>
<td>To prevent the user’s last name from being used as all or part of the password, select this check box.</td>
</tr>
<tr>
<td>User attributes (The user name)</td>
<td>To prevent the user’s user name from being used as all or part of the password, select this check box.</td>
</tr>
<tr>
<td>Characters not allowed</td>
<td>To activate the text field to the right of the check box, select the check box. Any alphanumeric or special characters that you enter into this field, separated by commas, are characters that aren't allowed for the password.</td>
</tr>
<tr>
<td>Whitespace Character</td>
<td>To prevent whitespace characters from being used as part of the password, select this check box. A whitespace character is a character that represents horizontal space in Oracle Identity Cloud Service. For example, for the display name of John Smith, the space between the first name of John and the last name of Smith is a whitespace character.</td>
</tr>
</tbody>
</table>
| Restricted Words              | If you select this check box, then you can screen all passwords against the following words:  
  Password,Qwerty,BaseBall,Dragon,Monkey,LetMeIn,Abc,Mustang,Access,Shadow,Mast er,Michael,Superman,BatMan,Trustno,Welc ome,Fusion,Oracle,Orcl,ILoveYou,PaaS,Ad min,Administrator,Cloud,Princess,Azerty,Gu est  
  Oracle Identity Cloud Service will reject any passwords that match the words in the list.                                                                 |

5. Click Save.

6. In the Save Password Policy dialog box, to force all users in your identity domain to set a new password upon their next login, select the **Force all users to set a new password on their next login** check box.
Otherwise, don't select the **Force all users to set a new password on their next login** check box. The password policy applies to users only when they are created or when they reset their passwords.

7. Click **OK**.

---

**Tip:**

To reinstate the previously saved password policy, click **Cancel**. If you click **Cancel**, then all your changes will be lost.

---

**Evaluate Password Policies**

At any time, you can evaluate your current password policy.

You can evaluate the Simple, Standard, or Custom password policy that you set for your identity domain when:

- Users register themselves with Oracle Identity Cloud Service
- Users reset their passwords
- An administrator manually sets or changes a user's password

See **Managing Profile Information** for more information about evaluating password policies.
Brand the Oracle Identity Cloud Service Interface

Learn how to customize the Oracle Identity Cloud Service web-based interface.

Topics

• Typical Workflow for Branding the Oracle Identity Cloud Service Interface
• Customize the Sign In Page
• Brand the Consoles
• Brand Notification Templates

Typical Workflow for Branding the Oracle Identity Cloud Service Interface

With the customization feature in Oracle Identity Cloud Service, you can perform tasks such as customizing the Sign In page. You can brand the Identity Cloud Service console, My Profile console, My Apps page, Catalog page, 2-Step Verification page, and notification templates by adding logos to them.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the Sign In page.</td>
<td>You can customize the Sign In page using the Branding page.</td>
<td>Customize the Sign In Page</td>
</tr>
<tr>
<td>Brand the consoles.</td>
<td>You can brand the Identity Cloud Service console, My Profile console, My Apps page, Catalog page, and 2-Step Verification page by adding a logo to them using the Branding page.</td>
<td>Brand the Consoles</td>
</tr>
<tr>
<td>Brand notification templates.</td>
<td>You can brand notification templates by adding logos to them using the Branding page.</td>
<td>Brand Notification Templates</td>
</tr>
</tbody>
</table>

You can access the Customizing the Service infographic to see how to customize the Oracle Identity Cloud Service interface.

You can customize the Oracle Identity Cloud Service interface by using:

• The Identity Cloud Service console
• SCIM-based APIs

In the following sections, you learn how to customize the interface by using the Identity Cloud Service console.
Customize the Sign In Page

When starting the UI, the user sees the Sign In page. You can customize this page by:

- Modifying the language of the text in the page
- Branding the page so that it displays the company name and logo
- Adding login text to the page. This text provides additional information that the user requires to log in to Oracle Identity Cloud Service.

You can preview your customizations before saving them. This way, you can ensure that they meet your business requirements.

To customize the Sign In page, use the Branding page in the Identity Cloud Service console. To open the Branding page, you must be assigned to either the identity domain administrator role or the security administrator role. See Add or Remove a User Account from an Administrator Role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Branding.
2. Because you want to customize the Sign In page, click Custom Branding.
3. Click Translation, and then select the language of the text for the Sign In page and the country for your identity domain. If you want English to be the text for the Sign In page, and your identity domain is located in the United States, then select English (United States).

![Important:](image)

Make sure the language that you specify for the Sign In page matches the default language of your web browser.

4. In the Company Name field, enter the name of the company for the Sign In page.
5. In the Login Text field, enter and format the login text for the page.
6. In the Desktop Logo or the Mobile Device Logo region of the Sign In Page pane, click Upload.
7. Select the company logo that appears in the Sign In page when the user accesses the page through a web browser or mobile device.

![Tip:](image)

Make sure that your logo has a GIF, JPEG, or PNG file extension, does not exceed 200 pixels for the height or width, and has a maximum file size of 300 KB.

8. Click Preview Sign In.
Brand the Consoles

You can brand the Identity Cloud Service console and the My Profile console to display the company logo in the header regions of the consoles. You can preview your customizations before saving them. This way, you can ensure that they meet your business requirements.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Branding.
2. In the side navigation bar, click Branding.
3. If Oracle Branding (default) is selected, then click Custom Branding.
4. In the Desktop Logo or the Mobile Device Logo region of the Console pane, click Upload.
5. Select the company logo that will appear in the header region of both the Identity Cloud Service console and the My Profile console when the user accesses the consoles using a web browser or mobile device.

   **Tip:**

   Make sure that your logo has a GIF, JPEG, or PNG file extension, does not exceed 200 pixels for the height or width, and has a maximum file size of 300 KB.

6. Click Preview Console.

   A web page opens that displays a preview of the logo you added.

7. Verify that the logo appears properly.
8. Reduce the size of the preview web page so that the dimensions of the page resemble the dimensions of a mobile device.
9. Verify that the logo appears properly again.
10. Click Save.
11. In the Confirmation window, click Yes.

Brand Notification Templates

You can brand notification templates to display a logo in the header and footer regions of the templates.
1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Branding**.

2. If **Oracle Branding (default)** is selected, then click **Custom Branding**.

3. In the **Header Logo** pane or the **Footer Logo** pane, click **Upload**.

4. Select the logo that will appear in the header region or footer region for all notifications.

   **Tip:**
   Make sure that your logo has a GIF, JPEG, or PNG file extension, does not exceed 200 pixels for the height or width, and has a maximum file size of 300 KB.

5. Click **Save**.

6. In the **Confirmation** window, click **Yes**.
Manage Provisioning Bridges for Oracle Identity Cloud Service

Learn how to manage Provisioning Bridges for Oracle Identity Cloud Service.

Topics:
- Typical Workflow for Managing Provisioning Bridges for Oracle Identity Cloud Service
- Understand the Provisioning Bridge
- Why Use the Provisioning Bridge?
- Create a Provisioning Bridge
- Start a Provisioning Bridge
- View Details About a Provisioning Bridge
- Activate and Deactivate Provisioning Bridges
- Modify a Provisioning Bridge
- Stop a Provisioning Bridge
- Remove Provisioning Bridges
- Manage Log Files for a Provisioning Bridge

Important:
The Provisioning Bridge feature is in early access. Contact Oracle Support to activate it.

Typical Workflow for Managing Provisioning Bridges for Oracle Identity Cloud Service

With the Provisioning Bridge feature in Oracle Identity Cloud Service, you can create, manage, and remove Provisioning Bridges.
In the following sections, you learn how to use the Identity Cloud Service console to create, manage, and remove Provisioning Bridges.

**Understand the Provisioning Bridge**

The Provisioning Bridge provides a link between your on-premises apps and Oracle Identity Cloud Service. Through synchronization, account data that's created and updated directly on the apps is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. As a result, any changes to these records will be transferred into Oracle Identity Cloud Service. So, if a
user is deleted in one of your apps, then this change will be propagated into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between your apps and Oracle Identity Cloud Service.

Suppose you're using an on-premises app such Oracle Internet Directory as an authoritative source for your company's users and groups. This app lies within your company's firewall. For a Provisioning Bridge to communicate with on-premises apps such as Oracle Internet Directory, it must leverage Identity Connector Framework (ICF) connectors to access the associated apps. As a result, the Provisioning Bridge can poll the on-premises apps for changes to users and groups in the apps, and synchronize these changes with Oracle Identity Cloud Service. You can configure a Provisioning Bridge so that Oracle Identity Cloud Service can synchronize users and groups from one or multiple apps.

**Figure 17-1  Directory Synchronization**

Both the Provisioning Bridges and your on-premises apps are in your Microsoft Windows or generic environment. A generic environment consists of any machine that has Java 8 installed on it and supports Bash shell.

Each Provisioning Bridge uses a client network to access the on-premises apps with which you want to synchronize Oracle Identity Cloud Service users and groups. Because Oracle Identity Cloud Service is an Oracle Cloud service, it's in an Oracle environment.
The Synchronize Users from Oracle Internet Directory to Oracle Identity Cloud Service video shows you how to configure on-premises apps such as Oracle Internet Directory so that the Provisioning Bridge can use the associated ICF connectors to poll the apps for changes to users and groups in the apps, and synchronize these changes with Oracle Identity Cloud Service.

Certified Components

With the Provisioning Bridge, Oracle Identity Cloud Service can connect to your on-premises apps.

The following table lists the certified versions for Oracle Identity Cloud Service, the versions of the on-premises apps with which Oracle Identity Cloud Service will synchronize by using Provisioning Bridges, and the features of these apps that the bridges support.

<table>
<thead>
<tr>
<th>Oracle Identity Cloud Service</th>
<th>On-Premises App</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.2.1</td>
<td>Oracle Internet Directory 12c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PS3</td>
<td>Authoritative synchronization</td>
</tr>
</tbody>
</table>

Statuses

There are two statuses for a Provisioning Bridge client:

- **Started**: The Provisioning Bridge started successfully. See [Start a Provisioning Bridge](#).
- **Stopped**: The Provisioning Bridge stopped unexpectedly or the identity domain administrator or security administrator stopped it. See [Stop a Provisioning Bridge](#).

There are also two statuses for a Provisioning Bridge:

- **Active**: The Provisioning Bridge is installed, started, and activated. It's available to poll the apps to which the Provisioning Bridge is assigned for changes to users.
and groups in the apps, and synchronize these changes with Oracle Identity Cloud Service. See Activate Provisioning Bridges.

- Inactive: The Provisioning Bridge is installed and configured, but it's deactivated. It's not available to retrieve users and groups from the apps to which the Provisioning Bridge is assigned. For performance reasons, this is done. See Deactivate Provisioning Bridges.

### Why Use the Provisioning Bridge?

Most customers have Microsoft Active Directory (AD) as their central directory service. These customers also use AD as their network directory. This directory is where all of their workstations are connected to and from where they manage their users.

In addition to AD, customers use an enterprise LDAP to centralize all of their user identities. So, a customer uses AD to manage their employees, but in the centralized LDAP, the customer manages their partners, consumers, and any other users with which the customer has relationships.

For these reasons, it's imperative that Oracle Identity Cloud Service can integrate with both AD and an enterprise LDAP (for example, Oracle Internet Directory).

By using Oracle Identity Cloud Service, customers can control when they will migrate their directory-based applications to the cloud. In the interim, they can use one of the following:

- **AD Bridge**: This bridge provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Each minute, the bridge polls AD for any changes to these records and brings these changes into Oracle Identity Cloud Service. So, if a user is deleted in AD, then this change will be propagated into Oracle Identity Cloud Service. As a result, the state of each record is synchronized between AD and Oracle Identity Cloud Service. After the user is synchronized from AD to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, then these changes are propagated to AD through the AD Bridge. See Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service.

- **Provisioning Bridge**: This bridge provides a link between your enterprise LDAP (such as Oracle Internet Directory) and Oracle Identity Cloud Service. Through synchronization, account data that's created and updated directly on the LDAP is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. As a result, any changes to these records will be transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between the LDAP and Oracle Identity Cloud Service.

This chapter focuses on using the Provisioning Bridge to synchronize users and groups from an enterprise LDAP (such as Oracle Internet Directory) to Oracle Identity Cloud Service.
Create a Provisioning Bridge

By creating a Provisioning Bridge, you establish a link between Oracle Identity Cloud Service and your on-premises apps.

To create this bridge, you must:

• Use the Identity Cloud Service console to add the bridge
• Install the client for the bridge

To add a Provisioning Bridge, you must be assigned to either the identity domain administrator role or the security administrator role. See Add or Remove a User Account from an Administrator Role for more information about assigning administrator roles to users.

After adding the Provisioning Bridge, you install the client for the bridge on a Microsoft Windows or generic machine. A generic machine has Java 8 installed on it and supports Bash shell.

Installing the client for the Provisioning Bridge includes providing administrative credentials for Oracle Identity Cloud Service, including the URL for the Oracle Identity Cloud Service identity domain, Client ID, and Client Secret. The Provisioning Bridge requires these credentials to access Oracle Identity Cloud Service as an administrator.

Prerequisites

Part of creating a Provisioning Bridge is installing the client for the bridge. On the machine where you're installing this client, you must have:

• Java 8 installed
• Administrative rights to access the client network that the Provisioning Bridge uses to communicate with the apps that you want to monitor
• Permissions to run the scripts that are used to install and start the Provisioning Bridge
• Permissions to create, manage, and execute commands in the folders associated with the machine where you'll install the client for the Provisioning Bridge
• Permissions to manage log files associated with the Provisioning Bridge
• The ability to communicate with both the Oracle Identity Cloud Service server and the servers associated with the target apps (for example, the Oracle Internet Directory server)
• Low network latency with these target servers

Create a Provisioning Bridge

In this procedure, you'll:

• Use the Identity Cloud Service console to add a Provisioning Bridge
• Install the client for this bridge on a Windows or generic machine. A generic machine has Java 8 installed on it and supports Bash shell.
1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.

2. If this is the first bridge you’re creating, then click **Add a Provisioning Bridge**. Otherwise, click **Add**.

3. In the **Name** and **Description** fields of the **Add Provisioning Bridge** page, enter a name and descriptive information for the Provisioning Bridge. Then, click **Save**.

   A new page appears for the Provisioning Bridge. The name of this page is the name you provided for the bridge in this step. By default, this Provisioning Bridge is deactivated. See **Activate Provisioning Bridges** to learn how to activate it.

   This page contains three tabs:

   - **Details**: This tab contains high-level information about the Provisioning Bridge.
   - **Apps**: This tab displays the apps to which the Provisioning Bridge will poll for changes to users and groups in the apps, and synchronize these changes into Oracle Identity Cloud Service. See **Assign a Provisioning Bridge to Apps**.
   - **Connectors**: After you install the client for the Provisioning Bridge and start the bridge, this tab displays the connectors that the bridge uses to communicate with the apps. You can learn more about this tab in **Start a Provisioning Bridge**.


   The Identity Cloud Service URL contains the name and port number for your Oracle Identity Cloud Service identity domain. The Client ID and Client Secret are used by the Provisioning Bridge to access Oracle Identity Cloud Service as an administrator.

   **Note:**

   The Client Secret is encrypted (for security purposes). To see the Secret in clear text, click **Show Secret**. To regenerate the Secret for the bridge, click **Regenerate**.

5. Click the **Downloads** link (because you want to download the client for the Provisioning Bridge).

6. In the **Downloads** page, click **Download** to the right of the **Identity Cloud Service Provisioning Bridge** client.

   Oracle Identity Cloud Service downloads the client for the Provisioning Bridge.

7. Verify that a **Success** status appears to the right of the **Identity Cloud Service Provisioning Bridge** client.

8. Launch the Windows or generic machine where you want to install the client for the Provisioning Bridge.
Important:

Make sure that you have administrative rights for this machine. Also, this machine will communicate with the client network that the Provisioning Bridge uses to access the apps that you want to monitor.

9. On this machine, create a folder, and then unzip the file that you downloaded in step 6 of this procedure into this folder. This zipped file contains the client that you are to install for the Provisioning Bridge.

After you unzip the file, the following folders are created:

- **bin**: This folder contains the `crossplatform.jar` file. This file is used by the installer to install, start, and stop the Provisioning Bridge.

- **bundle_home**: This folder contains the connector JAR files that Oracle ships with the bridge. These files are used by the bridge to communicate with the apps. For version 19.2.1 of Oracle Identity Cloud Service, this folder has one jar file: `ldap-1.0.jar`.

- **conf**: This folder contains two properties files:
  - `BridgeRuntimeConfigurations.properties`: This file contains properties associated with the Provisioning Bridge communicating with Oracle Identity Cloud Service and the target apps. Oracle strongly recommends that you don't modify the contents of this file.
  - `log4j.properties`: This file contains properties associated with logging operations that are performed by the Provisioning Bridge. See Manage Log Files for a Provisioning Bridge.

- **logs**: This is the default folder is where all log files for the Provisioning Bridge are stored. You can change this folder and path by modifying the `log4j.properties` file. See Manage Log Files for a Provisioning Bridge.

You'll also see three files:

- **startup.bat**: Use this file to launch the client for the Provisioning Bridge on a Windows (.bat) machine.

- **startup.sh**: Use this file to launch the client on a generic (.sh) machine.

- **FileInfo.json**: This file contains version information about the zipped file that you downloaded. Oracle strongly recommends that you don't modify the contents of this file.

Tip:

While you're installing the client, Oracle Identity Cloud Service generates log files for the Provisioning Bridge automatically, and stores them in the `logs` folder.

10. If you're installing the Provisioning Bridge on a generic machine, then open a Terminal window, navigate to the folder that you created in step 9, and run the `./startup.sh install` command.

OR
If you’re installing the Provisioning Bridge on a Windows machine, then open Windows Explorer, navigate to the folder that you created in step 9, and double-click the startup.bat file.

11. At the **Enter a password for Oracle Wallet** prompt, enter your Oracle Wallet password. The wallet is a file that's used to store sensitive information such as the Identity Cloud Service URL, Client ID, and Client Secret for Oracle Identity Cloud Service securely.

12. At the **Re-enter your password** prompt, enter this password again.

**Note:**

After you install the Provisioning Bridge, a wallet folder is created, and the Oracle Wallet you created is stored in this folder. This way, when you start the Provisioning Bridge, instead of providing the Identity Cloud Service URL, Client ID, and Client Secret for Oracle Identity Cloud Service, you only have to supply the password you provided for your Oracle Wallet.

**Important:**

There’s no mechanism to recover your Oracle Wallet password if you forget it. If this happens, then delete the wallet folder and install the Provisioning Bridge again.

13. At the **Enter the Identity Cloud Service URL, Enter the Client ID, and Enter the Client Secret** prompts, enter the Identity Cloud Service URL, Client ID, and Client Secret for Oracle Identity Cloud Service.

**Tip:**

These credentials appear on the [Provisioning_Bridge_Name] page of the Identity Cloud Service console.

14. For the following prompts:

   - **Enter the address for the proxy server**
   - **Enter the port number of the proxy server**
   - **Enter the name of the administrator who can connect to the proxy server**
   - **Enter the password of the administrator who can connect to the proxy server**

   a. If your organization has a firewall in place and requires communication to be handled using an HTTP Proxy Server, then enter the full path (or address) of the proxy server, the port number reserved for this server, and the administrator credentials for connecting to the server.

   b. If your organization doesn’t require communication to be handled using an HTTP Proxy Server, then press **Enter** after each prompt to skip the prompt.

The bridge attempts to connect to the Oracle Identity Cloud Service server.
If a connection can be established, then information about the Provisioning Bridge you created appears. This information includes the name, description, version number, Identity Cloud Service URL of the identity domain, and the locations of the `log4j.properties` file and `bundle_home` folder.

Otherwise, you'll receive an error message, indicating that you entered an incorrect Identity Cloud Service URL, Client ID, or Client Secret. Modify the incorrect values, and try again. If the problem persists, then delete the Oracle Wallet you created, and repeat steps 10-14 of this procedure.

**Start a Provisioning Bridge**

To start a Provisioning Bridge on a Windows or generic machine, you must first start the client for the bridge. Then, use the Identity Cloud Service console to access the Provisioning Bridge to verify that:

- The Provisioning Bridge is started
- The connectors appear that the Provisioning Bridge uses to poll the associated apps for changes to users and groups in the apps, and synchronize these changes into Oracle Identity Cloud Service

**Start the Provisioning Bridge on a Generic Machine**

A generic machine has Java 8 installed on it and supports bash shell. For this type of machine, you can start the Provisioning Bridge in two modes:

- **normal:** The bridge starts in a Terminal window.
- **background:** The bridge starts as a process in the background in a Terminal window.

**Important:**

You can't start multiple Provisioning Bridges with the same configuration information. If you want to start another Provisioning Bridge, then use the Provisioning Bridges page to create a new bridge, and use the newly generated Client ID and Secret for Oracle Identity Cloud Service to start the bridge.

**Start in Normal Mode**

Start the Provisioning Bridge in normal mode.

1. Launch the generic machine where you installed the client for the Provisioning Bridge.

**Important:**

Make sure that you have administrative rights for this machine. Also, this machine will communicate with the client network that the Provisioning Bridge uses to access the apps that you want to monitor.
2. In a Terminal window, navigate to the folder you created that contains the files for the Provisioning Bridge. You created this folder in Create a Provisioning Bridge.

3. At the prompt, enter ./startup.sh normal.

4. At the Enter your password for Oracle Wallet prompt, enter the password for Oracle Wallet that you created in Create a Provisioning Bridge.

The Provisioning Bridge attempts to connect to the Oracle Identity Cloud Service server.

5. Verify that you see the The Provisioning Bridge is started. status message. A connection is established between the Provisioning Bridge and the Oracle Identity Cloud Service server.

6. Important: Make sure that you keep this Terminal window open. If you close it, then you'll stop the Provisioning Bridge.

7. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Provisioning Bridges.

8. Verify that the Provisioning Bridge that you created in Create a Provisioning Bridge has a status of Started.

9. Click this Provisioning Bridge, and then click the Connectors tab.

9. Verify that you see the names and versions of the connectors that are used by the Provisioning Bridge to communicate with the associated apps. For version 19.2.1 of Oracle Identity Cloud Service, you should see one row, displaying version 1.0 of the LDAP Connector.

Start in Background Mode

Start the Provisioning Bridge in background mode.

1. Launch the generic machine where you installed the client for the Provisioning Bridge.

2. Important: Make sure that you have administrative rights for this machine. Also, this machine will communicate with the client network that the Provisioning Bridge uses to access the apps that you want to monitor.

3. In a Terminal window, navigate to the folder you created that contains the files for the Provisioning Bridge. You created this folder in Create a Provisioning Bridge.

4. At the prompt, enter ./startup.sh background.

5. At the Enter your password for Oracle Wallet prompt, enter the password for Oracle Wallet that you created in Create a Provisioning Bridge.

The Provisioning Bridge attempts to connect to the Oracle Identity Cloud Service server.
5. Verify that you see the status message. A connection is established between the Provisioning Bridge and the Oracle Identity Cloud Service server.

Note:
If you want to stop the Provisioning Bridge, then use the process ID to kill the process. You can also use this ID to check if the process is running properly, or if there are any errors associated with the process.

6. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Provisioning Bridges.

7. Verify that the Provisioning Bridge that you created in Create a Provisioning Bridge has a status of Started.

8. Click this Provisioning Bridge, and then click the Connectors tab.

9. Verify that you see the names and versions of the connectors that are used by the Provisioning Bridge to communicate with the associated apps. For version 19.2.1 of Oracle Identity Cloud Service, you should see one row, displaying version 1.0 of the LDAP Connector.

Start the Provisioning Bridge on a Windows Machine

In this procedure, you'll start the Provisioning Bridge on a Windows machine.

Important:
You can't start multiple Provisioning Bridges with the same configuration information. If you want to start another Provisioning Bridge, then use the Provisioning Bridges page to create a new bridge, and use the newly generated Client ID and Secret for Oracle Identity Cloud Service to start the bridge.

1. Launch the Windows machine where you installed the client for the Provisioning Bridge.

Important:
Make sure that you have administrative rights for this machine. Also, this machine will communicate with the client network that the Provisioning Bridge uses to access the apps that you want to monitor.

2. Open Windows Explorer, and then navigate to the folder you created that contains the files for the Provisioning Bridge. You created this folder in Create a Provisioning Bridge.

3. Double-click the startup.bat file.
4. At the **Enter your password for Oracle Wallet** prompt of the Command window, enter the password for Oracle Wallet that you created in Create a Provisioning Bridge.

The Provisioning Bridge attempts to connect to the Oracle Identity Cloud Service server.

5. **Verify that you see the** The Provisioning Bridge is started. **status message.** A connection is established between the Provisioning Bridge and the Oracle Identity Cloud Service server.

**Important:**
Make sure that you keep this Command window open. If you close it, then you'll stop the Provisioning Bridge.

6. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.

7. **Verify that the Provisioning Bridge that you created in Create a Provisioning Bridge** has a status of **Started**.

8. Click this Provisioning Bridge, and then click the **Connectors** tab.

9. **Verify that you see the names and versions of the connectors that are used by the Provisioning Bridge to communicate with the associated apps.** For version 19.2.1 of Oracle Identity Cloud Service, you should see one row, displaying version **1.0** of the LDAP Connector.

**View Details About a Provisioning Bridge**

By default, in the **Provisioning Bridges** page, you can see the name, description, and statuses for each Provisioning Bridge.

You can also see other information about a Provisioning Bridge, such as its Identity Cloud Service URL, version number, Client ID, and Client Secret, any apps assigned to the bridge, and any connectors that are used by the bridge to communicate between the apps and Oracle Identity Cloud Service.

**Note:**
See Create a Provisioning Bridge for more information about the Provisioning Bridge’s Identity Cloud Service URL, Client ID, and Client Secret.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.

2. Click the bridge about which you want to view additional information.

3. Click **Details**.

In this tab, you see information about the Provisioning Bridge, including its name, description, Identity Cloud Service URL, version number, and Client ID. By clicking
Show Secret, you can see the Client Secret for the Provisioning Bridge in clear text. By clicking Regenerate, you can regenerate the Secret for this bridge.

4. Click Apps.

In this tab, you can see a list of apps assigned to the Provisioning Bridge. You can assign additional apps to this bridge or change the bridge associated with the apps. See Assign a Provisioning Bridge to Apps and Change the Provisioning Bridge Assigned to Apps.

Note:

For load-balancing purposes, Oracle suggests that you don't assign more than 10 apps to a Provisioning Bridge. To maintain more apps, create another Provisioning Bridge.

5. Click Connectors.

In this tab, you can see any connectors that the Provisioning Bridge uses to communicate with the apps. See Start a Provisioning Bridge.

Activate and Deactivate Provisioning Bridges

You can use Oracle Identity Cloud Service to activate and deactivate Provisioning Bridges.

- Activating a Provisioning Bridge enables the link between Oracle Identity Cloud Service and your on-premises apps such as Oracle Internet Directory. The Provisioning Bridge can use connectors to poll the corresponding apps for changes to users and groups in the apps, and synchronize these changes into Oracle Identity Cloud Service.

- Deactivating a Provisioning Bridge disables the link between Oracle Identity Cloud Service and your on-premises apps such as Oracle Internet Directory. The Provisioning Bridge can't use connectors to poll the associated apps for changes to users and groups in the apps, and synchronize these changes into Oracle Identity Cloud Service.

Note:

Oracle recommends that you deactivate a Provisioning Bridge before stopping the bridge or performing any maintenance activity on the machine where the client for the bridge is installed.

Activate Provisioning Bridges

You can use Oracle Identity Cloud Service to activate a single Provisioning Bridge. For efficiency purposes, you can also activate multiple Provisioning Bridges simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Provisioning Bridges.

2. Select the check box for each Provisioning Bridge that you want to activate.
3. Click **Activate**.
4. In the **Confirmation** window, click **OK**.

   The status of each Provisioning Bridge you selected changes from **Inactive** to **Active**.

### Deactivate Provisioning Bridges

You can use Oracle Identity Cloud Service to deactivate either a single Provisioning Bridge or multiple Provisioning Bridges simultaneously (for efficiency purposes).

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.
2. Select the check box for each Provisioning Bridge that you want to deactivate.
3. Click **Deactivate**.
4. In the **Confirmation** window, click **OK**.

   The status of each Provisioning Bridge you selected changes from **Active** to **Inactive**.

### Modify a Provisioning Bridge

You can change the following items for a Provisioning Bridge:

- The name, description, and Client Secret of the bridge
- The apps to which the bridge is assigned

**Note:**

You can also change the folder where all log files for the Provisioning Bridge are stored and the log level for these log files. See **Manage Log Files for a Provisioning Bridge**.

### Modify a Provisioning Bridge

You can use the **Provisioning Bridges** page to modify a Provisioning Bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.
2. Click the Provisioning Bridge that you want to modify.
3. Click **Details**.
   a. To edit the name or descriptive information about the Provisioning Bridge, enter the modifications in the **Name** or **Description** fields.
   b. To regenerate the Client Secret for this bridge, click **Regenerate**.
Note:

If you have activated this Provisioning Bridge, then you can’t regenerate a Client Secret for it because the bridge is using this Secret to access Oracle Identity Cloud Service as an administrator.

To regenerate the Client Secret for this Provisioning Bridge, you must first deactivate the bridge, and then stop it. See Deactivate Provisioning Bridges and Stop a Provisioning Bridge.

If you regenerate the Client Secret for a Provisioning Bridge, then you must delete the wallet folder and recreate the Oracle Wallet that you made in Create a Provisioning Bridge so that the wallet contains the regenerated Secret.

c. Click Save.
d. In the Confirmation window, click OK.

Assign a Provisioning Bridge to Apps

After creating a Provisioning Bridge, you can assign it to on-premises apps in the App Catalog. Because this bridge serves as a provisioning and synchronizing agent between Oracle Identity Cloud Service and your apps, the bridge can poll for changes to users or groups in the apps and synchronize those changes into Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
2. Click the App Catalog app to which you want to assign a Provisioning Bridge.

Note:
For version 19.2.1 of Oracle Identity Cloud Service, you can assign the Provisioning Bridge to the Oracle Internet Directory app only. Also, see the Synchronize Users from Oracle Internet Directory to Oracle Identity Cloud Service video to learn more about configuring this app.

3. Click Deactivate.
4. In the Confirmation window, click OK.

Note:
You must deactivate the app so that you can modify it by assigning a Provisioning Bridge to it.

5. Click Provisioning.
6. Turn on the Enable Provisioning switch.
7. From the Associate with Provisioning Bridge list, select the Provisioning Bridge that you want to assign to this app.
8. Click **Save**.

9. Click **Activate**.

10. In the **Confirmation** window, click **OK**.

**Note:**

If the Provisioning Bridge has an inactive status, then activate it. See **Activate Provisioning Bridges**.

11. Repeat steps 1-10 for each app to which you want to assign the Provisioning Bridge.

12. In the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.

13. Click the Provisioning Bridge that you assigned to apps, and then click the **Apps** tab.

14. Verify that you see each app to which you assigned the Provisioning Bridge.

### Change the Provisioning Bridge Assigned to Apps

Only one Provisioning Bridge can be assigned to an app at any time. If you want to assign another bridge to the app, then you must replace the bridge that's already associated with the app with the designated Provisioning Bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Applications**.

2. Click the App Catalog app to which you want to assign another Provisioning Bridge.

**Note:**

For version 19.2.1 of Oracle Identity Cloud Service, you can assign a different Provisioning Bridge to the Oracle Internet Directory app only.

3. Click **Deactivate**.

4. In the **Confirmation** window, click **OK**.

**Note:**

You must deactivate the app so that you can modify it by changing the Provisioning Bridge assigned to it.
5. Click **Provisioning**.
6. Turn on the **Enable Provisioning** switch.
7. From the **Associate with Provisioning Bridge** list, select a different Provisioning Bridge than the one that’s assigned to this app.
8. Click **Save**.
9. Click **Activate**.
10. In the **Confirmation** window, click **OK**.

**Note:**

By activating this app, the other Provisioning Bridge that you selected for it can be used to poll the app for changes to users and groups in the app, and synchronize these changes into Oracle Identity Cloud Service.

11. Repeat steps 1-10 for each app to which you want to assign a different Provisioning Bridge.
12. In the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.
13. Click the Provisioning Bridge that you unassigned from the apps, and then click the **Apps** tab.
14. Verify that you no longer see these apps in the tab.

---

### Stop a Provisioning Bridge

You can stop a Provisioning Bridge that’s running on a Windows or generic machine.

**Important:**

If you stop a Provisioning Bridge, then you must wait three minutes to restart the bridge. Also, before you stop a Provisioning Bridge, you must deactivate it. See Deactivate Provisioning Bridges.

Use the following table to guide you on how to stop a Provisioning Bridge.

<table>
<thead>
<tr>
<th>Machine</th>
<th>Mode</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic</td>
<td>normal</td>
<td>Close the Terminal window or press Ctrl + C.</td>
</tr>
</tbody>
</table>
At the prompt of the Terminal window, kill the process by entering `kill -9 [Process_ID]`.

**Note:**

Because you started the Provisioning Bridge in `background` mode, even if you close the Terminal window, the bridge continues to run. For this reason, you must kill the process to stop the Provisioning Bridge.

**Tip:**

If you don't know the process ID, then run the following command: `ps -ef | grep CrossPlatformBridgeRunner`.

To verify that you stopped the Provisioning Bridge, complete the following steps:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Provisioning Bridges**.
2. Verify that the Provisioning Bridge that you stopped has a status of **Stopped**.

**Note:**

If you still see a status of **Started** for the Provisioning Bridge, then wait three minutes, and click **Refresh**.
Remove Provisioning Bridges

You can remove unused Provisioning Bridges from Oracle Identity Cloud Service. You can remove either a single Provisioning Bridge or multiple bridges.

**Important:**

Before you remove any Provisioning Bridges, make sure that you:

- Deactivate the Provisioning Bridges. See Deactivate Provisioning Bridges.
- Assign different Provisioning Bridges to apps. See Change the Provisioning Bridge Assigned to Apps.
- Stop the Provisioning Bridges. See Stop a Provisioning Bridge.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Provisioning Bridges.
2. Select the check box for each Provisioning Bridge that you want to remove.
3. Click Remove.
4. In the Confirmation window, click OK.

Manage Log Files for a Provisioning Bridge

After you install and start a Provisioning Bridge, you may want to access the log files for troubleshooting purposes. You can locate these files in the `logs` folder.

The `logs` folder is contained in the directory that you created when you unzipped the file for the Identity Cloud Service Provisioning Bridge client in Create a Provisioning Bridge.

You can change the folder path where all log files for the Provisioning Bridge are stored and the log level for these log files. To do this, you modify the `log4j.properties` file.

The `log4j.properties` file is located in the `conf` folder of the directory that you created when you unzipped the file for the Identity Cloud Service Provisioning Bridge client, and contains properties associated with logging operations that are performed by the Provisioning Bridge.

1. Navigate to the `conf` folder.
2. Using a text editor, open the `log4j.properties` file.
3. In the file, locate the following line of code: `property.baseLocation = ./logs/`
4. Change the value of the `property.baseLocation` parameter to the folder path where you want all log files for the Provisioning Bridge to be stored.
5. Locate the following line of code: `filter.threshold.level = error`
6. Change the value of the `filter.threshold.level` parameter to one of the following log levels:

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Capture all events</td>
</tr>
<tr>
<td>debug</td>
<td>Capture fine-grained informational events that are most useful to debug the Provisioning Bridge</td>
</tr>
<tr>
<td>error</td>
<td>Capture error events that might still allow the Provisioning Bridge to continue running</td>
</tr>
<tr>
<td>info</td>
<td>Capture informational events that highlight the progress of the Provisioning Bridge at a coarse-grained level</td>
</tr>
</tbody>
</table>

7. Save and close the `log4j.properties` file.

Note:

You must stop the Provisioning Bridge and restart it for the changes you made to the `log4j.properties` file to take effect. Also, after you stop the Provisioning Bridge, you must wait three minutes to restart it.
Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service

Learn how to manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service.

Topics

• Typical Workflow for Managing Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service
• About the Microsoft Active Directory (AD) Bridge
• Why Use the Microsoft Active Directory (AD) Bridge?
• Set Permissions for Your Microsoft Active Directory (AD) Account
• Create a Microsoft Active Directory (AD) Bridge
• Configure a Microsoft Active Directory (AD) Bridge
• Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge
• Run a Microsoft Active Directory (AD) Bridge
• View Details About a Microsoft Active Directory (AD) Bridge
• Activate and Deactivate Microsoft Active Directory (AD) Bridges
• Modify a Microsoft Active Directory (AD) Bridge
• Remove a Microsoft Active Directory (AD) Bridge
• Understand Best Practices for the Microsoft Active Directory (AD) Bridge

Typical Workflow for Managing Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service

With the Microsoft Active Directory (AD) Bridge feature in Oracle Identity Cloud Service, you can create, manage, and remove AD Bridges.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the AD Bridge.</td>
<td>You can receive an overview of the AD Bridge for Oracle Identity Cloud Service. You can also learn why you should use the AD Bridge, and how it's used to synchronize users and groups between AD and Oracle Identity Cloud Service.</td>
<td>About the Microsoft Active Directory (AD) Bridge Why Use the Microsoft Active Directory (AD) Bridge?</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Set permissions for your AD account.</td>
<td>Before creating an AD Bridge, you must set permissions for your AD domain administrator account. You must set these permissions so that you can install the bridge and configure delegated authentication for it.</td>
<td>Set Permissions for Your Microsoft Active Directory (AD) Account</td>
</tr>
<tr>
<td>Create an AD Bridge.</td>
<td>You can create an AD Bridge using the Directory Integrations page and the client for the bridge.</td>
<td>Create a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Configure an AD Bridge.</td>
<td>You can configure an AD Bridge using the Directory Integrations page.</td>
<td>Configure a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Define attribute mappings for an AD Bridge.</td>
<td>You can define attribute mappings for an AD Bridge using the Directory Integrations page.</td>
<td>Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Run an AD Bridge.</td>
<td>You can run an AD Bridge manually or view a synchronization log about the bridge being run using the Directory Integrations page.</td>
<td>Run a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>View details about an AD Bridge.</td>
<td>You can view details about an AD Bridge using the Directory Integrations page.</td>
<td>View Details About a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Activate and deactivate AD Bridges.</td>
<td>You can activate and deactivate AD Bridges using the Directory Integrations page.</td>
<td>Activate and Deactivate Microsoft Active Directory (AD) Bridges</td>
</tr>
<tr>
<td>Modify an AD Bridge.</td>
<td>You can modify an AD Bridge using the Directory Integrations page.</td>
<td>Modify a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Remove an AD Bridge.</td>
<td>You can remove an AD Bridge using the Directory Integrations page and the client for the bridge.</td>
<td>Remove a Microsoft Active Directory (AD) Bridge</td>
</tr>
<tr>
<td>Understand best practices for the AD Bridge.</td>
<td>You can learn about best practices for creating, managing, and maintaining the AD Bridge.</td>
<td>Understand Best Practices for the Microsoft Active Directory (AD) Bridge</td>
</tr>
</tbody>
</table>

You can create, manage, and remove AD Bridges by using:

- The Identity Cloud Service console
- SCIM-based APIs

In the following sections, you learn how to manage AD Bridges by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.
About the Microsoft Active Directory (AD) Bridge

The Microsoft Active Directory (AD) Bridge provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service.

**Topics:**
- Understand the Microsoft Active Directory (AD) Bridge
- Certified Components
- Statuses
- Hardware Requirements

Understand the Microsoft Active Directory (AD) Bridge

The Microsoft Active Directory (AD) Bridge provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Each minute, the AD Bridge polls AD for any changes to these records and brings these changes into Oracle Identity Cloud Service. So, if a user is deleted in AD, then this change will be propagated into Oracle Identity Cloud Service. Because of this synchronization, the state of each record is synchronized between AD and Oracle Identity Cloud Service.

After users are synchronized from AD to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, then these changes are propagated to AD through the AD Bridge.

**Note:**
The AD organizational units (OUs) contain the users and groups that are imported into Oracle Identity Cloud Service.

You can configure Oracle Identity Cloud Service to synchronize with one or multiple AD domains by installing an AD Bridge for each domain.

**Note:**
You must install the AD Bridge on the machine that's attached to the Microsoft Active Directory domain for auto discovery. You don't have to install the bridge on the domain controller.
In the diagram above, Clarence Saladna (CSALADNA) is a user who's been synchronized from AD to Oracle Identity Cloud Service through the AD Bridge. In Oracle Identity Cloud Service, an administrator deactivates Clarence's account because he's on vacation. Also, because Clarence received a promotion, he has a new job title of Director and belongs to different groups that are associated with his new role, including the Executive and Management groups. The AD Bridge can be used to propagate these changes to AD.

Both the AD Bridges and your AD enterprise directory structure are in your Microsoft Windows environment (for example, Microsoft Windows 2003). Because Oracle Identity Cloud Service is an Oracle Cloud service, it's in an Oracle environment.
**Certified Components**

With the Microsoft Active Directory (AD) Bridge, Oracle Identity Cloud Service can connect to your AD enterprise directory structure.

The following table lists the certified versions for Oracle Identity Cloud Service, AD, your operating system, and the Microsoft .NET software framework (which is required for the AD Bridge to run).

<table>
<thead>
<tr>
<th>Oracle Identity Cloud Service</th>
<th>AD</th>
<th>64-Bit</th>
<th>Operating System</th>
<th>.NET Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.2.1</td>
<td>Microsoft Windows Server 2008</td>
<td>Yes</td>
<td>Windows 7 or later</td>
<td>Version 4.6+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 or later</td>
<td></td>
</tr>
<tr>
<td>19.2.1</td>
<td>Microsoft Windows Server 2008 R2</td>
<td>Yes</td>
<td>Windows 7 or later</td>
<td>Version 4.6+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 or later</td>
<td></td>
</tr>
<tr>
<td>19.2.1</td>
<td>Microsoft Windows Server 2012</td>
<td>Yes</td>
<td>Windows 7 or later</td>
<td>Version 4.6+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 or later</td>
<td></td>
</tr>
</tbody>
</table>
### Statuses

Learn about the various statuses for Microsoft Active Directory (AD) and the AD Bridge.

There are two statuses for the AD domain with which the AD Bridge is communicating:

- **Partially Configured**: The AD Bridge is installed, but it's not configured to communicate with either the AD domain or Oracle Identity Cloud Service.
- **Configured**: The AD Bridge is installed and configured, and available to synchronize with the AD domain.

There are three statuses for the AD Bridge:

- **Active**: The AD Bridge is installed and configured, and available to synchronize with AD to retrieve user accounts and groups.
- **Inactive**: The AD Bridge is installed and configured, but it's not available to synchronize with AD. For performance reasons, this is done.
- **Unreachable**: The AD Bridge is installed and configured. However, one of the following conditions has occurred:
  - The back-end service used to establish communication between Oracle Identity Cloud Service and AD is stopped.
  - The Oracle Identity Cloud Service administrator uninstalled the client associated with the AD Bridge, but the bridge couldn't be removed from the Directory Integrations page of the Identity Cloud Service console because the client can't connect to the Oracle Identity Cloud Service server. Oracle Identity Cloud Service can't use the bridge to communicate with AD. See Remove a Microsoft Active Directory (AD) Bridge.
  - The administrator regenerated the Client Secret for the AD Bridge, and then uninstalled the client for the bridge.

### Hardware Requirements

Learn about the minimum hardware requirements for setting up the Microsoft Active Directory (AD) Bridge.

The minimum hardware requirements are, as follows:

- 1 GB of RAM
- 1 GB of disk space
Why Use the Microsoft Active Directory (AD) Bridge?

Learn about why you should use the Microsoft Active Directory (AD) Bridge.

Most customers have AD as their central directory service. These customers also use AD as their network directory. This directory is where all of their workstations are connected to and from where they manage their users.

In addition to AD, customers use an enterprise LDAP to centralize all of their user identities. So, a customer uses AD to manage their employees, but in the centralized LDAP, the customer manages their partners, consumers, and any other users with which the customer has relationships.

For these reasons, it's imperative that Oracle Identity Cloud Service can integrate with both AD and an enterprise LDAP (for example, Oracle Internet Directory).

By using Oracle Identity Cloud Service, customers can control when they will migrate their directory-based applications to the cloud. In the interim, they can use one of the following:

- **AD Bridge**: This bridge provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Each minute, the bridge polls AD for any changes to these records and brings these changes into Oracle Identity Cloud Service. So, if a user is deleted in AD, then this change will be propagated into Oracle Identity Cloud Service. As a result, the state of each record is synchronized between AD and Oracle Identity Cloud Service. After the user is synchronized from AD to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, then these changes are propagated to AD through the AD Bridge.

- **Provisioning Bridge**: This bridge provides a link between your enterprise LDAP (such as Oracle Internet Directory) and Oracle Identity Cloud Service. Through synchronization, account data that's created and updated directly on the LDAP is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. As a result, any changes to these records will be transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between the LDAP and Oracle Identity Cloud Service. See Manage Provisioning Bridges for Oracle Identity Cloud Service.

This chapter focuses on using the AD Bridge to synchronize users and groups between AD and Oracle Identity Cloud Service.

Set Permissions for Your Microsoft Active Directory (AD) Account

You use your Microsoft Active Directory (AD) domain administrator account to create an AD Bridge. Before creating this bridge, you must set permissions for your account. You must set these permissions so that you can install the bridge and configure delegated authentication for it.
With delegated authentication, Oracle Identity Cloud Service identity domain administrators and security administrators don't have to synchronize user passwords between AD and Oracle Identity Cloud Service. Users can use their AD passwords to sign in to Oracle Identity Cloud Service to access resources and applications protected by Oracle Identity Cloud Service.

See Understand Delegated Authentication for more information about delegated authentication.

Topics:

- Set Permissions to Synchronize Users, Groups, and Group Membership
- Set Permissions to Propagate Changes to Microsoft Active Directory
- Set Permissions for Delegated Authentication

Set Permissions to Synchronize Users, Groups, and Group Membership

You set permissions for your Active Directory Bridge service account so that you can synchronize users, groups, or OUs between Microsoft Active Directory (AD) and Oracle Identity Cloud Service

1. Use your domain administrator credentials to sign in to the machine that contains your AD server.
2. Open a command window.
3. Set the **Generic Read** permissions for the users, groups, and organizational units (OU) in the AD domain that you want to import into Oracle Identity Cloud Service:

   ```
   dsacls <AD_Domain_Name> /I:T /g "<AD_Domain_Name>\<User/Group_Name>:GR"
   ```

**Note:**

- `<AD_Domain_Name>` is the name of the domain that you're associating with Oracle Identity Cloud Service and `<User/Group_Name>` is the username of your domain administrator account.
- `/I:T`: This parameter specifies the objects to which you are applying the permissions. T is the default, which means you can propagate inheritable permissions to this object and child objects down to one level only.
- `/g`: This parameter grants the permissions that you specify to the user or group. For example, `/g {<user> | <group>}::<permissions>`.
- `<permissions>`: This parameter specifies the type of permissions that you are applying.
  - **GR**: Generic Read
  - **GW**: Generic Write
  - **LC**: List the child objects of the object
  - **RP**: Read Property
4. Set the **List Children** and **Read** properties for the **cn=Deleted Objects** container with inheritance. This container is also in the AD domain that you're associating with Oracle Identity Cloud Service.

```bash
dsacls "cn=deleted objects,<AD_Domain_Name>" /takeOwnership
dsacls "cn=deleted objects,<AD_Domain_Name>" /I:T /g "<AD_Domain_Name>\<User/Group_Name>:LCRP"
```

**Note:**

If you don't have the above permissions, then the AD Bridge won't be able to synchronize deleted users, groups, or OUs between AD and Oracle Identity Cloud Service. This will cause inconsistencies between AD and Oracle Identity Cloud Service.

### Set Permissions to Propagate Changes to Microsoft Active Directory

You set permissions for your Active Directory Bridge service account so that you can propagate changes you have done in Oracle Identity Cloud Service to Microsoft Active Directory (AD) through the AD Bridge.

1. Use your domain administrator credentials to sign in to the machine that contains your AD server.
2. Open a command window.
3. Set the **Generic Write** permission for the users, groups, and organizational units (OU) in the AD domain, if you want to propagate the changes you have done in Oracle Identity Cloud Service to Active Directory.

```bash
dsacls <AD_Domain_Name> /I:T /g "<AD_Domain_Name>\<User/Group_Name>:GW"
```

### Set Permissions for Delegated Authentication

You set permissions for your Microsoft Active Directory (AD) domain administrator account so that you can configure delegated authentication for the AD Bridge.

1. Open **Active Directory Users and Computers**.
2. Right-click the user, group, or organizational unit (OU) that you want to delegate, and then click **Delegate Control**.
3. On the **Delegation of Control** wizard, click **Next**, and then click **Add**.
4. On the **Select Users, Computers, or Groups** dialog box, in the text area, enter the user name or group name that needs to be granted permissions to configure delegated authentication.
5. Click **Check Names** to verify that the user or group has been created in AD. If it hasn't been created, then create it.
6. Click **OK**, and then click **Next**.
7. Select the **Delegate the following common tasks** option, and then select **Reset user passwords and force password change at next logon**.
8. Click **Next**, and then click **Finish**.
The next steps explain how to set specific permissions to lock and unlock user accounts.

9. Right-click on the newly modified user or group, and select **Properties**.

10. Select the **Security** tab, click **Advanced**.

11. On the Advanced Security Settings, click **Add**.

12. On the Permission Entry wizard, click **Select a principal**, and enter the same user name or group name that has been granted reset permission.

13. Click **OK**.

14. In the **Applies to** field, select **Descendant User objects**.

   The list of permissions allowed for the user account (Principal) displays.

15. Scroll down and enable **Read lockoutTime**, and **Write lockoutTime**.

16. Click **OK** and continue to click **OK** until the end of the setup.

   The user account now has permissions to change passwords for all the user objects present in the high-level context.

---

Create a Microsoft Active Directory (AD) Bridge

To create a Microsoft Active Directory (AD) Bridge that provides a link between your AD enterprise directory structure and Oracle Identity Cloud Service, you must be assigned to either the identity domain administrator role or the security administrator role. You must also have administrative rights to access the AD domain that you want to monitor by using the bridge.

Part of creating the AD Bridge is providing administrative credentials for both AD and Oracle Identity Cloud Service. The bridge requires these credentials to communicate with AD and Oracle Identity Cloud Service as an administrator.

See [Add or Remove a User Account from an Administrator Role](#) for more information about assigning administrator roles to users.
The AD account used to install the AD Bridge should have the following permissions:

- **Generic Read** for the users and groups in the AD domain that you want to import into Oracle Identity Cloud Service
- **Generic Read** for all organizational units (OUs) in the domain
- **Generic Read** for the `cn=Configuration` container in the domain
- The `List Children` and `Read` properties for the `cn=Deleted Objects` container with inheritance

If this account is also used to configure delegated authentication for the AD Bridge, then the account should have the following permissions:

- **Change Password**
- **Reset Password**
- **Read pwdLastSet**
- **Write pwdLastSet**
- **Read lockoutTime**
- **Write lockoutTime**

See [Set Permissions for Your Microsoft Active Directory (AD) Account](#).

You can access the [Managing Security Settings](#) infographic to see how to create an AD Bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Directory Integrations**.
2. If this is the first AD Bridge you’re creating, then click **Add a Microsoft Active Directory Bridge**. Otherwise, click **Add**.
3. In the **Install Bridge** page, make a note of the Identity Cloud Service URL, Client ID, and Client Secret.
   
   The Identity Cloud Service URL contains the name and port number for your Oracle Identity Cloud Service identity domain. The Client ID and Client Secret are used by the AD Bridge to access Oracle Identity Cloud Service as an administrator.

   **Note:**
   
   The Client Secret is encrypted (for security purposes). To see the Secret in clear text, click **Show Secret**. To regenerate the Secret for the AD Bridge, click **Regenerate**.

4. Click **Download**.
   
   Oracle Identity Cloud Service downloads the client for the AD Bridge.
5. To install the client for the AD Bridge, double-click the `ad-id-bridge.exe` file. The Welcome to AD Bridge Installer window appears.

6. In the Language Selection area, select the language that you want to use to install the client for the AD Bridge, and then click OK. The Identity Cloud Service Microsoft Active Directory Bridge Installer appears.

7. If the Open File — Security Warning dialog box appears, then click Run. Otherwise, go to step 8.

8. In the Welcome dialog box, click Next.

9. In the Destination Folder dialog box, choose one of the following install choices:
   - To install the client in the default directory, click Next.
   - To select another directory to install the client:
     a. Click Browse.
     b. In the Browse For Folder dialog box, select the directory where Oracle Identity Cloud Service will install the client.
     c. Click OK.
     d. Click Next.

10. In the Specify Proxy Server dialog box:
    a. If your organization has a firewall in place and requires communication to be handled using an HTTP Proxy Server, then select Use Proxy Server. If you select this check box, then provide the full path (or address) of the proxy server and the administrator credentials for connecting to the proxy server.
    b. If your organization doesn't require communication to be handled using an HTTP Proxy Server, then don't select Use Proxy Server.
    c. Click Next.

11. In the Specify Identity Cloud Service Credentials dialog box:
    a. Provide the Cloud Service URL, Client ID, and Client Secret.
Tip:
These credentials appear on the Install Bridge page of the Identity Cloud Service console.

b. Click Test.

The AD Bridge attempts to connect to the Oracle Identity Cloud Service server.

If a connection can be established, then a Connection Successful! confirmation message appears.

Otherwise, you'll receive an error message, indicating that you entered an incorrect Cloud Service URL, Client ID, or Client Secret. Modify the incorrect values, and click Test again.

c. Click Next.

12. In the Specify Microsoft Active Directory Credentials dialog box, provide the following connection details to the AD server:

a. Username: The AD account that the AD Bridge uses to access the AD server.

b. Password: The password for the AD account.

c. Use SSL: If you're connecting to the server via an SSL connection, then leave this check box selected. Otherwise, deselect it.

Note:
Oracle recommends that you keep the Use SSL check box selected because this results in a faster and more-secure connection. After you select or deselect this check box, and install the client for the AD Bridge, you can't modify this setting.

d. Click Test.

The AD Bridge attempts to connect to the AD server.

If a connection can be established, then a Connection Successful! confirmation message appears.

Otherwise, you'll receive an error message, indicating that:

• You entered an incorrect username or password. Modify the incorrect values, and click Test again.

• You're attempting to connect to the AD server via an SSL connection, but the certificate for the server isn't trusted. Make sure that this certificate is valid, and is present in the trust store of your machine. Then, click Test again.

e. Click Next.

13. In the Summary dialog box, click Close.


The AD Bridge that you created for the AD domain appears with a status of Partially Configured. The bridge is created, but not configured. See Configure a
Configure a Microsoft Active Directory (AD) Bridge

After creating a Microsoft Active Directory (AD) Bridge, you configure it by:

• Selecting the AD organizational units (OUs) and groups with which you want Oracle Identity Cloud Service to synchronize using the AD Bridge. The OUs contain the users that you want to import into Oracle Identity Cloud Service. By synchronizing with AD, the bridge can transfer new, updated, or deleted user or group records into Oracle Identity Cloud Service.

• Specifying whether, after a user or group is synchronized from AD to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, these changes will be propagated to AD.

• Scheduling how often you want Oracle Identity Cloud Service to use the AD Bridge to import users and groups from AD.

• Defining custom attribute mappings between AD and Oracle Identity Cloud Service.

• Specifying whether users can use their Oracle Identity Cloud Service or AD passwords, or their federated accounts, to authenticate into Oracle Identity Cloud Service to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console, the Identity Cloud Service console, or any apps assigned to the users.

You can access the Managing Security Settings infographic to see how to configure an AD Bridge.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.

2. Click the AD Bridge that you want to configure.

3. In the Configure the Microsoft Active Directory Domain page, configure the AD domain to listen for changes to users or groups in AD and import those changes into Oracle Identity Cloud Service.

a. In the Select organizational units (OUs) for users and Select organizational units (OUs) for groups panes:
i. Select the **Include Hierarchy** check box. If you select a parent OU, then all children OUs will be selected. The OUs contain the users and groups that you want to import into Oracle Identity Cloud Service.

OR

Deselect the check box. If you select a parent OU, then children OUs won’t be selected.

ii. Select the check box for each OU that contains users or groups with which you want Oracle Identity Cloud Service to synchronize using the AD Bridge.

---

**Note:**

If you don’t see any OUs for users or groups in the **Select organizational units (OUs) for users** and **Select organizational units (OUs) for groups** panes, then refresh your web browser.

To force a full synchronization between AD and Oracle Identity Cloud Service, deselect all check boxes for selected user or group OUs, click **Save**, and then in the **Save Configuration Changes?** dialog box, click **OK**. Then, click **Import** to import the users and groups from AD.

iii. Optional. In the **Filter** text box, enter a custom filter to search for user or group OUs. For example, entering `(sn=Smith)` will return all users with the last name of Smith. Or, enter `(department=IT)` to return the IT group.
Tip:

- To select all users or groups, select the Include Hierarchy check box, and then select the top-most check box in each pane.
- In the Filter text box, you can't enter more than 4,000 characters.
- The wildcard character * is allowed, except when the AD Attribute is a DN attribute. For more information about AD filters, click here.
- You can use the Filter text box to synchronize users from AD to Oracle Identity Cloud Service based on their group memberships rather than their OUs. To do this, don't select the check boxes for the OUs. Instead, in the Filter text box, provide the custom group membership filters.
- If there's a mismatch between the number of users or groups you're expecting to be transferred into Oracle Identity Cloud Service and how many users or groups are actually imported, then use Active Directory Users and Computers to test the custom filter in AD to verify that the users and groups brought into Oracle Identity Cloud Service are correct.
- The names of the users that you want to import into Oracle Identity Cloud Service must contain at least three characters. The names of the groups that you want to import into Oracle Identity Cloud Service must contain at least five characters.
- The telephone numbers of the users that you want to import must meet the requirements of the RFC 3966 specification.

b. In the Supported Operations area, choose which operations for Oracle Identity Cloud Service users or groups will be propagated to AD:

- If you activate or deactivate Oracle Identity Cloud Service users, and you want these user activation status changes to be reflected in AD, then select the Activate/Deactivate Users check box. Otherwise, leave this check box deselected.

- If you edit attribute values for Oracle Identity Cloud Service users, and you want these modifications to be passed to AD, then select the Update Users Attributes check box. Otherwise, leave this check box deselected.

- If you change the groups to which Oracle Identity Cloud Service users belong, and you want these group membership changes to be propagated to AD, then select the Update Groups check box. Otherwise, leave this check box deselected.

c. In the Set import frequency area, schedule how often, in hours and minutes, you want Oracle Identity Cloud Service to use the AD Bridge to import users and groups from AD.
Important:

During an incremental synchronization cycle, if there are more than 100,000 group membership changes in Microsoft Active Directory, then the synchronization cycle might take more than one hour. Microsoft Active Directory needs this time to process the change logs.

d. In the **Configure Attribute Mappings** area, click **Edit Attribute Mappings** to define custom attribute mappings between AD and Oracle Identity Cloud Service. See Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge. Otherwise, go to step e.

e. In the **Authentication Settings** area, select **Enable local authentication** if you want users to use their Oracle Identity Cloud Service or their AD passwords to authenticate into Oracle Identity Cloud Service to access Oracle Identity Cloud Service-protected resources.

If you select this option, then configure delegated authentication for this AD Bridge. By activating delegated authentication, users transferred into Oracle Identity Cloud Service through the bridge will use their AD passwords to sign in to Oracle Identity Cloud Service. By deactivating delegated authentication, users must use their Oracle Identity Cloud Service passwords to authenticate into Oracle Identity Cloud Service. See Configure Delegated Authentication in Oracle Identity Cloud Service for more information about configuring delegated authentication for an AD Bridge.

Also, if you select **Enable local authentication**, then keep **Don't send Welcome Notifications** deselected to have Oracle Identity Cloud Service notify users by email that they must activate the Oracle Identity Cloud Service accounts that are created for them.

Otherwise, if you don't want users to be notified that Oracle Identity Cloud Service created accounts for them, then select the **Don't send Welcome Notifications** check box.

If you want users to use their federated accounts to authenticate into Oracle Identity Cloud Service, then select **Enable federated authentication**.

Note:

If you select this option, then configure SSO through the **Identity Providers** page. See Activate and Deactivate an Identity Provider.

Important:

By selecting **Enable federated authentication**, any user accounts that are transferred into Oracle Identity Cloud Service through the AD Bridge are classified as federated accounts. For referential integrity purposes, you can't deactivate, remove, or change the status of these user accounts to nonfederated.

f. Click **Save**.
4. In the **Confirmation** window, click **OK**.

The status of the AD Bridge changes from **Partially Configured** to **Configured**.
The bridge is created and configured.

---

**Important:**

Before you use the AD Bridge to import any AD user accounts into Oracle Identity Cloud Service, enable the **Password Never Expires** option for the accounts in AD. Otherwise, the passwords for the accounts will expire. If this occurs, then you can change the passwords. See Microsoft Active Directory (AD) Bridge Limitations in Known Issues for Oracle Identity Cloud Service.

---

**Note:**

If you use the AD Bridge to import a group into Oracle Identity Cloud Service, and then delete the group in Oracle Identity Cloud Service, you can re-establish a link between the group in AD and the group in Oracle Identity Cloud Service. To do so:

a. In the **Select organizational units (OUs) for groups** pane, clear the check box for the designated group, and click **Save**.

b. Select the check box for the group, and click **Save** again.

c. Run the AD Bridge to synchronize the group between Oracle Identity Cloud Service and AD immediately. See **Run a Microsoft Active Directory (AD) Bridge**.

---

**Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge**

By default, when you create a Microsoft Active Directory (AD) Bridge, attribute mappings are defined between AD and Oracle Identity Cloud Service. Attribute mappings enable the AD Bridge to pass values associated with user accounts between AD and Oracle Identity Cloud Service.

You can map attributes in two different ways: inbound and outbound. Inbound mappings allow you to map attributes from AD to Oracle Identity Cloud Service. Outbound mappings allow you to map any changes in Oracle Identity Cloud Service attributes to AD attributes.

For example, when you run the AD Bridge, the bridge can use the `givenName - First Name` mapping to transfer the first name of the user account from the **First name** field on the **General** tab of the **Properties** window of AD to the **First Name** field on the **Details** tab of the **Users** page of Oracle Identity Cloud Service. Similarly, you can perform an outbound mapping so that when you make any change to the first name of the user account in Oracle Identity Cloud Service, this change is reflected in AD. See **Run a Microsoft Active Directory (AD) Bridge**.
In addition to the predefined attribute mappings, you can define custom attribute mappings between AD and Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Directory Integrations**.
2. Click the AD Bridge for which you want to define custom attribute mappings.
3. Click **Configuration**.
4. In the **Configure Attribute Mappings** area, click **Edit Attribute Mappings**. In the **Edit Attribute Mappings** window, two tabs appear:
   - **Microsoft Active Directory to Identity cloud**: This tab contains inbound attribute mappings from AD to Oracle Identity Cloud Service.
   - **Identity cloud to Microsoft Active Directory**: This tab contains outbound attribute mappings from Oracle Identity Cloud Service to AD.
5. If you want to define inbound attribute mappings, then click the **Microsoft Active Directory to Identity cloud** tab. Otherwise, go to step 9.
   You'll see predefined inbound mappings from AD to Oracle Identity Cloud Service. These mappings include:

<table>
<thead>
<tr>
<th>List of predefined attributes</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sAMAccountName</td>
<td>Yes</td>
<td>The user's user name.</td>
</tr>
<tr>
<td>givenName</td>
<td>No</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>sn</td>
<td>Yes</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>middleName</td>
<td>No</td>
<td>The user's middle name.</td>
</tr>
<tr>
<td>displayName</td>
<td>No</td>
<td>The user's display name.</td>
</tr>
<tr>
<td>title</td>
<td>No</td>
<td>The user's job title.</td>
</tr>
<tr>
<td>preferredLanguage</td>
<td>No</td>
<td>The user's preferred language (for example, English).</td>
</tr>
<tr>
<td>localeID</td>
<td>No</td>
<td>The user's language and region (locale).</td>
</tr>
<tr>
<td>mail</td>
<td>Yes</td>
<td>The user's email address.</td>
</tr>
<tr>
<td>telephonenumber</td>
<td>No</td>
<td>The user's telephone number.</td>
</tr>
<tr>
<td>homePhone</td>
<td>No</td>
<td>The user's home telephone number.</td>
</tr>
<tr>
<td>mobile</td>
<td>No</td>
<td>The user's mobile telephone number.</td>
</tr>
<tr>
<td>postalAddress</td>
<td>No</td>
<td>The user's postal address.</td>
</tr>
<tr>
<td>streetAddress</td>
<td>No</td>
<td>The user's street address.</td>
</tr>
<tr>
<td>l</td>
<td>No</td>
<td>The user's work location.</td>
</tr>
<tr>
<td>st</td>
<td>No</td>
<td>The state of the user's work address.</td>
</tr>
<tr>
<td>postalCode</td>
<td>No</td>
<td>The zip code of the user's work address.</td>
</tr>
<tr>
<td>c</td>
<td>No</td>
<td>The country of the user's work address.</td>
</tr>
<tr>
<td>usercertificate</td>
<td>No</td>
<td>This multi-valued attribute contains the DER-encoded X509v3 certificates issued to the user.</td>
</tr>
<tr>
<td>userAccountControl</td>
<td>Yes</td>
<td>Specifies flags that control behavior for the user, such as whether the user has an <strong>Active</strong> or <strong>Inactive</strong> status, or whether the user's account is locked.</td>
</tr>
</tbody>
</table>

6. Click **Add Row** because you want to define an inbound attribute mapping from AD to Oracle Identity Cloud Service.
7. In the Directory User Attributes column, enter or select the name of the AD attribute that contains a value which you want to transfer into Oracle Identity Cloud Service.

8. In the Oracle Identity Cloud Service User Attributes column, enter or select the name of the Oracle Identity Cloud Service attribute that will contain the value transferred from AD.

9. If you want to define outbound attribute mappings, then click the Identity cloud to Microsoft Active Directory tab. Otherwise, go to step 13.

You'll see predefined outbound mappings from Oracle Identity Cloud Service to AD. These mappings include:

<table>
<thead>
<tr>
<th>List of predefined attributes</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>No</td>
<td>The user's user name.</td>
</tr>
<tr>
<td>Display Name</td>
<td>No</td>
<td>The user's display name.</td>
</tr>
<tr>
<td>Work Email</td>
<td>No</td>
<td>The user's work-related email address.</td>
</tr>
<tr>
<td>First name</td>
<td>No</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>No</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>No</td>
<td>The user's middle name.</td>
</tr>
<tr>
<td>Title</td>
<td>No</td>
<td>The user's job title.</td>
</tr>
<tr>
<td>Locale</td>
<td>No</td>
<td>The user's language and region (locale)</td>
</tr>
<tr>
<td>Preferred Language</td>
<td>No</td>
<td>The user's preferred language (for example, English).</td>
</tr>
<tr>
<td>Work Phone number</td>
<td>No</td>
<td>The user's work-related telephone number.</td>
</tr>
<tr>
<td>Mobile Phone number</td>
<td>No</td>
<td>The user's mobile telephone number.</td>
</tr>
<tr>
<td>Work Address Formatted</td>
<td>No</td>
<td>The user's work-related postal address.</td>
</tr>
<tr>
<td>Work Street Address</td>
<td>No</td>
<td>The user's street address.</td>
</tr>
<tr>
<td>Work Locality</td>
<td>No</td>
<td>The user's work location.</td>
</tr>
<tr>
<td>Work Address Region</td>
<td>No</td>
<td>The state or region of the user's work address.</td>
</tr>
<tr>
<td>Work Address Zip Code</td>
<td>No</td>
<td>The zip code of the user's work address.</td>
</tr>
<tr>
<td>Work Address Country</td>
<td>No</td>
<td>The country of the user's work address.</td>
</tr>
<tr>
<td>Home Phone number</td>
<td>No</td>
<td>The user's home telephone number.</td>
</tr>
</tbody>
</table>

10. Click Add Row because you want to define an outbound attribute mapping from Oracle Identity Cloud Service to AD.

11. In the Oracle Identity Cloud Service User Attributes column, enter or select the name of the Oracle Identity Cloud Service attribute that contains a value which you want to transfer into AD.

12. In the Directory User Attributes column, enter or select the name of the AD attribute that will contain the value transferred from Oracle Identity Cloud Service.

13. Click Save.
Run a Microsoft Active Directory (AD) Bridge

You can run a Microsoft Active Directory (AD) Bridge to synchronize Oracle Identity Cloud Service with AD immediately.

As part of configuring an AD Bridge, you specified how often, in hours and minutes, you want Oracle Identity Cloud Service to use the bridge to import users and groups from AD. You're synchronizing Oracle Identity Cloud Service with your AD enterprise directory structure.

When the interval you specified elapses, Oracle Identity Cloud Service synchronizes with the directory structure so that any new, updated, or deleted user or group records are transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between AD and Oracle Identity Cloud Service.

For security purposes, you may want to import users and groups from AD immediately. There are two types of imports that you can run:

- **Full import**: The AD Bridge polls AD and retrieves data associated with all user and groups that you selected in the Select organizational units (OUs) for users and Select organizational units (OUs) for groups panes of the Configuration tab for the bridge. This data represents users and groups that were created, modified, or removed in AD. As a best practice, Oracle recommends that you perform a full import the first time you run the AD Bridge. See Configure a Microsoft Active Directory (AD) Bridge for more information about the Configuration tab.

- **Incremental import**: Similar to a full import, but for this type of import, the AD Bridge polls AD and retrieves only user and group data that changed since you last used the AD Bridge to import users and groups into Oracle Identity Cloud Service.

By running the AD Bridge, you can propagate changes for Oracle Identity Cloud Service users in AD. After users are imported into Oracle Identity Cloud Service through the bridge, if you activate or deactivate a user, modify the user’s attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, then these changes will be reflected in AD.

You can also use the AD Bridge to view a synchronization log of the communication between Oracle Identity Cloud Service and AD.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.
2. Click the AD Bridge that you want to use to import users and groups from AD.
3. Click Configuration.
4. In the Configuration tab:
   a. In the Select organizational units (OUs) for users and Select organizational units (OUs) for groups panes, select the check box for each OU that contains users or groups that you want to import.
   b. In the Supported Operations area, select check boxes to enable Oracle Identity Cloud Service to propagate a user's activation status, attribute values, or group memberships to AD. See Configure a Microsoft Active Directory (AD) Bridge for more information about the Supported Operations area.
c. Click **Save**.
   The AD Bridge propagates any changes to an Oracle Identity Cloud Service user’s activation status, attribute values, or group memberships to AD.

5. In the **Confirmation** window, click **OK**.

6. Click **Import**.

7. In the **Import Type** window, choose whether you want to run an incremental import or a full import, and then click **OK**.

   Oracle Identity Cloud Service imports the users and groups from AD.

    **Note:**
    
    Based on how many users and groups you’re importing, the job may take several minutes or even hours.

8. Click the **Import** tab. The status of the job Oracle Identity Cloud Service uses to import users and groups from AD is **Running**. After all users and groups are imported, the status changes to **Success**.

   Also, on this tab, you'll see a synchronization log of all traffic that occurs between Oracle Identity Cloud Service and AD for the current import job that ran. This includes the start date and time, and completion date and time, for the import job, how many users and groups were imported from AD successfully, and how many users and groups couldn't be imported.

    **Note:**
    
    If you don't see the status change after a few minutes, then click **Refresh**. Also, if the status of the job is **Failed**, then an error occurred while the AD Bridge was transferring users and groups from AD to Oracle Identity Cloud Service. See [Troubleshooting Oracle Identity Cloud Service](#).

---

**View Details About a Microsoft Active Directory (AD) Bridge**

By default, you can see the domain name and status for each Microsoft Active Directory (AD) Bridge.

You might want to see other information about the AD Bridge, such as its configuration information, attribute mappings, and a synchronization log of the communication between Oracle Identity Cloud Service and AD.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Directory Integrations**.

2. Click the AD Bridge about which you want to see more information.

   • To view configuration information about the AD Bridge, click the **Configuration** tab. See [Configure a Microsoft Active Directory (AD) Bridge](#).
Activate and Deactivate Microsoft Active Directory (AD) Bridges

You can use Oracle Identity Cloud Service to activate and deactivate Microsoft Active Directory (AD) Bridges:

- **Deactivate**: Disable the link between your AD enterprise directory structure and Oracle Identity Cloud Service.
- **Activate**: Enable the link between Oracle Identity Cloud Service and AD.

### Activate a Microsoft Active Directory (AD) Bridge

You can use Oracle Identity Cloud Service to activate a single Microsoft Active Directory (AD) Bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Directory Integrations**.

2. Click the **Action** menu to the right of the domain that contains the AD Bridge that you want to activate.

3. Select **Activate**.

4. In the **Confirmation** window, click **OK**.

   By activating the domain, you’re activating the AD Bridge associated with the domain. The status of the bridge changes from **Inactive** to **Active**.

### Deactivate a Microsoft Active Directory (AD) Bridge

You can use Oracle Identity Cloud Service to deactivate a single Microsoft Active Directory (AD) Bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Directory Integrations**.

2. Click the **Action** menu to the right of the domain that contains the AD Bridge that you want to deactivate.

3. Select **Deactivate**.

4. In the **Confirmation** window, click **OK**.

   By deactivating the domain, you’re deactivating the AD Bridge associated with the domain. The status of the bridge changes from **Active** to **Inactive**.
Activate All Microsoft Active Directory (AD) Bridges

For efficiency purposes, you can use Oracle Identity Cloud Service to activate all Microsoft Active Directory (AD) Bridges simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.
2. Click Activate All.
3. In the Confirmation window, click OK.
   By activating all domains, you're activating the AD Bridge associated with each domain. The status of each bridge changes from Inactive to Active.

Deactivate All Microsoft Active Directory (AD) Bridges

For security purposes, you can use Oracle Identity Cloud Service to deactivate all Microsoft Active Directory (AD) Bridges simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.
2. Click Deactivate All.
3. In the Confirmation window, click OK.
   By deactivating all domains, you're deactivating the AD Bridge associated with each domain. The status of each bridge changes from Active to Inactive.

Modify a Microsoft Active Directory (AD) Bridge

You can change the following items for a Microsoft Active Directory (AD) Bridge:

- The AD users and groups that you want Oracle Identity Cloud Service to import using the AD Bridge.
- Whether, after a user or group is synchronized from AD to Oracle Identity Cloud Service, if you activate or deactivate a user, modify the user's attribute values, or change the group memberships for the user in Oracle Identity Cloud Service, these changes will be propagated to AD.
- How often you want Oracle Identity Cloud Service to use the AD Bridge to import users and groups from AD.
- The predefined and custom attribute mappings defined between AD and Oracle Identity Cloud Service.
- Whether users can use their AD or their Oracle Identity Cloud Service passwords, or their federated accounts, to sign in to Oracle Identity Cloud Service to access resources protected by Oracle Identity Cloud Service, such as the My Profile console, Identity Cloud Service console, and apps assigned to the users.
Note:

You can upgrade the client for the AD Bridge. By doing this, you can install the latest client without removing the existing client that's installed.

To upgrade the client, download it and follow the instructions in Create a Microsoft Active Directory (AD) Bridge. When you see the Specify Identity Cloud Service Credentials or the Specify Microsoft Active Directory Credentials dialog boxes, the client will use the credentials you provided in the previous installation. For this reason, the values are greyed out so they can't be edited.

Modify a Microsoft Active Directory (AD) Bridge

You can use the Directory Integrations page to modify a Microsoft Active Directory (AD) Bridge.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.
2. Click the AD Bridge that you want to modify.
3. To edit configuration information about the AD Bridge, go to step 4. Otherwise, go to step 5.
4. Click Configuration.
   a. In the Select organizational units (OUs) for users and Select organizational units (OUs) for groups panes, select or deselect check boxes to enable or prevent Oracle Identity Cloud Service from importing users and groups using the AD Bridge.
      See Configure a Microsoft Active Directory (AD) Bridge for more information about the Select organizational units (OUs) for users and Select organizational units (OUs) for groups panes.
   b. In the Supported Operations area, select or deselect check boxes to enable or prevent Oracle Identity Cloud Service from propagating changes for a user's activation status, attribute values, or group memberships to AD.
      See Configure a Microsoft Active Directory (AD) Bridge for more information about the Supported Operations area.
   c. In the Set import frequency area, change how often you want Oracle Identity Cloud Service to use the AD Bridge to import users and groups from AD.
   d. In the Configure Attribute Mappings area, click Edit Attribute Mappings. The Edit Attribute Mappings window opens and two tabs appear:
      • Microsoft Active Directory to Identity cloud: In this tab, you can modify inbound attribute mappings from AD to Oracle Identity Cloud Service.
      • Identity cloud to Microsoft Active Directory: Use this tab to modify outbound attribute mappings from Oracle Identity Cloud Service to AD.
   i. Click the Microsoft Active Directory to Identity cloud or Identity cloud to Microsoft Active Directory tab.
ii. In the Directory User Attributes and Oracle Identity Cloud Service User Attributes columns, change the AD or Oracle Identity Cloud Service attribute used for the predefined or custom attribute mapping.

iii. To remove an attribute mapping, click the X button to the right of the mapping.

**Note:**
Inbound attribute mappings with asterisks in the Microsoft Active Directory to Identity cloud tab are required by the AD Bridge to pass values associated with AD user accounts into Oracle Identity Cloud Service so that the accounts can be created in Oracle Identity Cloud Service. You can't delete these mappings.

iv. Click Save to close the Edit Attribute Mappings window.

See Define Attribute Mappings for a Microsoft Active Directory (AD) Bridge for more information about the Directory User Attributes and Oracle Identity Cloud Service User Attributes columns of the Microsoft Active Directory to Identity cloud and Identity cloud to Microsoft Active Directory tabs of the Edit Attribute Mappings window.

e. In the Authentication Settings area, select the Enable local authentication option if you want users to use their Oracle Identity Cloud Service or their AD passwords to sign in to Oracle Identity Cloud Service to access Oracle Identity Cloud Service-protected resources.

   If you select this option, then configure delegated authentication for the AD Bridge. See Configure a Microsoft Active Directory (AD) Bridge.

   If you select Enable local authentication, then select or deselect Don't send Welcome Notifications to enable or prevent Oracle Identity Cloud Service from notifying users by email that they must activate the Oracle Identity Cloud Service accounts that are created for them.

   Otherwise, select Enable federated authentication to have users use their federated accounts to sign in to Oracle Identity Cloud Service.

f. Click Save.

g. In the Confirmation window, click OK.

See Configure a Microsoft Active Directory (AD) Bridge for more information about the areas of the Configuration tab.

Remove a Microsoft Active Directory (AD) Bridge

You can use Oracle Identity Cloud Service to remove a Microsoft Active Directory (AD) Bridge.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.

2. Click the Action menu to the right of the domain that contains the AD Bridge that you want to remove.
3. Select **Remove**.

4. In the **Confirmation** window, click **OK**.

   By removing the domain, you’re removing the AD Bridge associated with the domain. To ensure that your bridge is deleted cleanly and completely, you must delete the client associated with the bridge.

5. Double-click the **ad-id-bridge.exe** file.

   The **Identity Cloud Service Microsoft Active Directory Bridge Installer** appears.

6. In the **Welcome** dialog box, click **Next**.

7. In the **Removal Completed** dialog box, click **Close**.

### Important:

If you can't remove the client for the AD Bridge or the bridge still appears in the **Directory Integrations** page, then complete the following steps:

1. Run the following CURL command to obtain the Client ID that you used to install the client for the AD Bridge:

   ```
   curl -X GET \
   <Identity_Cloud_Service_URL>/admin/v1/IdentityAgents \
   -H 'Authorization: Bearer <access_token>
   ```

   Where **<Identity_Cloud_Service_URL>** is a placeholder for the Identity Cloud Service URL that you used to install the client for the bridge, and **<access_token>** is a placeholder for the access token that contains the authorization credentials that are required to obtain the Client ID.

   See the Oracle Identity Cloud Service: First REST API Call tutorial to learn how to get this access token.

   A list of AD Bridge clients that are installed for your identity domain appears.

2. From this list, find the Client ID of the AD Bridge that you want to remove.

3. Run the following CURL command to remove the client for the AD Bridge:

   ```
   curl -X DELETE \
   <Identity_Cloud_Service_URL>/admin/v1/IdentityAgents/ <Client_ID> \
   -H 'Authorization: Bearer <access_token>
   ```

   Where **<Client_ID>** represents the ID of the client for the AD Bridge that you want to remove.

   A 204 (No Content) response appears, signifying that you removed the client for the bridge.
Understand Best Practices for the Microsoft Active Directory (AD) Bridge

This section contains best practices to:

- Create and Manage Log Files for the Microsoft Active Directory (AD) Bridge
- Maintain the Microsoft Active Directory (AD) Bridge

By implementing these best practices, the Microsoft Active Directory (AD) Bridge will run optimally.

Create and Manage Log Files for the Microsoft Active Directory (AD) Bridge

After you install and configure the Microsoft Active Directory (AD) Bridge, you may want to access the log files for troubleshooting purposes. You can locate these files in the %ProgramData%\Oracle\IDBridge\logs directory.

To modify the log level of the log files for the AD Bridge:

1. Navigate to the %ProgramFiles%\Oracle\IDBridge directory.
2. Using a text editor, open the log4net.config file.
3. In the file, locate the following line of code: <level value="info" />
4. Change the value of the level value parameter to one of the following log levels:

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Capture all events.</td>
</tr>
<tr>
<td>debug</td>
<td>Capture fine-grained informational events that are most useful to debug the AD Bridge.</td>
</tr>
<tr>
<td>error</td>
<td>Capture error events that might still allow the AD Bridge to continue running.</td>
</tr>
<tr>
<td>fatal</td>
<td>Capture severe error events that will result in the AD Bridge no longer running.</td>
</tr>
<tr>
<td>info</td>
<td>Capture informational events that highlight the progress of the AD Bridge at a coarse-grained level.</td>
</tr>
<tr>
<td>off</td>
<td>Turn off logging.</td>
</tr>
<tr>
<td>trace</td>
<td>Capture finer-grained informational events than the debug log level.</td>
</tr>
<tr>
<td>warn</td>
<td>Capture potentially harmful situations to the AD Bridge.</td>
</tr>
</tbody>
</table>

5. Save and close the log4net.config file.
Maintain the Microsoft Active Directory (AD) Bridge

Maintaining the Microsoft Active Directory (AD) Bridge includes transferring the bridge to another machine and restarting the bridge.

Topics:
- Transfer the Microsoft Active Directory (AD) Bridge
- Restart the Microsoft Active Directory (AD) Bridge

Transfer the Microsoft Active Directory (AD) Bridge

After you have setup a Microsoft Active Directory (AD) Bridge, you can transfer that bridge to another machine.

1. From the original machine, access the Control Panel, and uninstall the client for the AD Bridge.
2. On the other machine, install the client. See Create a Microsoft Active Directory (AD) Bridge.
3. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Directory Integrations.
4. Verify that the AD Bridge appears in the other machine with an Active status. This bridge can now be used to synchronize with your AD enterprise directory structure.

Restart the Microsoft Active Directory (AD) Bridge

If the Microsoft Active Directory (AD) Bridge stops unexpectedly, then you can restart it.

1. Click Start.
2. In the text box, enter Services, and then press Enter.

The Services window appears. This window contains a utility that's used to manage daemon processes within the Windows OS. These processes include the back-end service that's used to establish communication between Oracle Identity Cloud Service and AD.
3. Click Services (Local), click the Standard tab, scroll down the list of services, right-click Identity Cloud Service Microsoft Active Directory Bridge Service, and then click Start.

4. Verify that Running appears as the status for the service.
Manage Oracle Identity Cloud Service Session Settings

Learn how to manage your default session settings for Oracle Identity Cloud Service.

To manage default identity domain settings, you must be assigned to the identity domain administrator role. See Add or Remove a User Account from an Administrator Role.

Topics:
- Change Session Settings

Change Session Settings

To specify the session expiration and the logout URL for an identity domain, use the Sessions Settings page.

To open this page, you must be assigned the identity domain administrator role or the security administrator role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Session Settings.

2. In the Session Expiry field, enter a duration in minutes.

3. In the Login URL field, enter the URI where you want the user redirected to log in.
   For example, enter /ui/v1/signin.

4. In the Logout URL field, enter a logout URL.
   For example, to redirect the user to the My Profile console, enter /ui/v1/myconsole.

5. In the Error URL field, enter the tenant specific Error page URL to which a user has to be redirected, in case of a failure. This URL is considered when the Application specific Custom Error URL is not specified for an Application.

6. In the Social Linking Callback URL field, enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. This URL is considered when the Application specific Social Linking Callback URL is not specified for an Application.

7. Select the Allow Cross-Origin Resource Sharing (CORS) option to allow client applications that run on one domain to obtain data from another domain.

   CORS creates a way for the browser and the server to interact to determine whether to allow requests to external domains. The CORS standard adds new HTTP headers that allow servers to describe the set of origins that are permitted to read information using a web browser.
8. In the **Allowed CORS Domain Names** box, enter the external domain names that are allowed for CORS operations. Use a comma-delimited list to enter more than one domain, for example: domain1, domain2, domain3.

9. Click **Save**.
Manage Self-Registration Profiles in Oracle Identity Cloud Service

Create self-registration profiles to manage different sets of users, approval policies, and applications. For example, Identity domain administrators can create profiles that allow users to complete self-registration and gain access to specific applications without approval.

Topics

• Typical Workflow for Managing Self-Registration Profiles
• Understand Self-Registration Profiles
• Create Self-Registration Profiles

Typical Workflow for Managing Self-Registration Profiles

To start creating self-registration profiles, first complete the prerequisites in the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create groups.</td>
<td>Create the groups that you want to use for self-registration.</td>
<td>Manage Oracle Identity Cloud Service Groups</td>
</tr>
<tr>
<td>Review self-registration</td>
<td>Review the self-registration email templates and make any necessary changes</td>
<td>Typical Workflow for Customizing Oracle Identity Cloud</td>
</tr>
<tr>
<td>notification templates.</td>
<td></td>
<td>Service Notifications</td>
</tr>
</tbody>
</table>

Once you have completed the prerequisites, complete the tasks in the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Self-Registration</td>
<td>Add your customized header and footer logos, determine your allowed email</td>
<td>Create Self-Registration Profiles</td>
</tr>
<tr>
<td>Profiles</td>
<td>domains, and add header, footer, success, and user consent text.</td>
<td></td>
</tr>
<tr>
<td>Activate the profile.</td>
<td>By default, a profile is created in inactive state. Activate the profile</td>
<td>Create Self-Registration Profiles</td>
</tr>
<tr>
<td>Construct a self-registration</td>
<td>Construct a self-registration URL to be sent to the users.</td>
<td>Create Self-Registration Profiles</td>
</tr>
<tr>
<td>URL.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Understand Self-Registration Profiles

Self-registration profiles give you the flexibility to define different mechanisms for users to register with an application.

Using self-registration profiles, you can:

- Create a self-registration **consumer flow** that allows users to create an account in a verified state. Use the REST API for Oracle Identity Cloud Service to turn off the `activationEmailRequired` option. The user can then directly log in to Oracle Identity Cloud Service using a user name and password to authenticate. See Self Registration Profiles REST Endpoints.

- Create a self-registration **partner flow** that allows users to create an account in an unverified state. Use the REST API for Oracle Identity Cloud Service to turn on the `activationEmailRequired` option so that a user receives a link in the welcome email to verify the user. Once the user clicks this link, the user's state is changed to verified and the user can log in to Oracle Identity Cloud Service. See Self Registration Profiles REST Endpoints.

- Specify whether users are prompted and must accept a user consent before self-registering.

- Assign groups to a profile so that users are assigned to all the groups that are part of that profile.

- Specify the domains allowed when accessing the self-registration process. Only users with these specific domains are allowed to register.

- Customize the self-registration login page with your header and footer logos.

- Customize the header, footer, success, and user consent text.

- Delete profiles using the REST API. See REST API for Oracle Identity Cloud Service.

Create Self-Registration Profiles

To manage self-registration for different sets of users, approval policies, and applications, create self-registration profiles.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then **Self Registration**.
2. Click **Add Profile**.
3. Complete the **Details** section.
   - Enter a unique **Profile Name**.
   - To require a user to accept the terms of use during self-registration, turn on the **User Consent Required** option.
   - To hide the terms of use from the user during self-registration, turn off the **User Consent Required** option.
   - To add groups to the profile, click **Add** in the **Assign to Group** section.
   - Add the domains allowed during the self-registration process in the **Allowed Email Domains** field.
4. Upload footer and header logos or keep the default logos.

5. Complete the **Self-Registration Content** section.
   - Enter the **Registration Page Name** that you want to appear as a link on your customized login page.
   - Add header, footer, and success text or keep the default values.
   - If you have turned on the **User Consent Required** option, enter the text in the **User Consent Text** field.

   **Tip:**
   Click **Cancel** to discard your changes and return to the **Manage Self-Registration Profiles** page. Currently, you can only delete profiles using the REST API.

6. Click **Save**.
   The **Profile ID** that you need for the self-registration link is created.

7. On the **Manage Self-Registration Profiles** page, use the action menu to activate the profile.

   Next, you must construct a self-registration URL. Click the profile that you created and use the **Profile ID** to construct a URL exactly like the following: https://[instancename.idcs.internal.oracle.com:port]/ui/v1/signup?profileid=[ProfileID]

   If the URL is not constructed properly, you receive an error stating that your profile was not found. Verify that the syntax of the URL is correct.

   This URL gives the user access to the self-registration page. After the user completes self-registration and clicks **Submit**, they are presented with a success page. The user must then click the link **Click here to continue** to go to the **My Apps** page in Oracle identity Cloud Service. If the user does not click the link within 1 hour, the token expires and user is presented with the **Login** page.
Download Oracle Identity Cloud Service SDKs and Applications

This section describes how to understand, download, and use Oracle Identity Cloud Service software development kits (SDKs) and applications.

Topics:

• Typical Workflow for Downloading Oracle Identity Cloud Service SDKs and Applications
• Understand Oracle Identity Cloud Service SDKs and Applications
• Download Oracle Identity Cloud Service SDKs and Applications
• Use Oracle Identity Cloud Service SDKs and Applications

Typical Workflow for Downloading Oracle Identity Cloud Service SDKs and Applications

With the download feature in Oracle Identity Cloud Service, you can perform tasks such as downloading software development kits (SDKs) and applications.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand Oracle Identity Cloud Service SDKs and applications.</td>
<td>You can learn about SDKs, including how they're used to develop custom mobile and Web applications to authenticate and integrate them with Oracle Identity Cloud Service. You can learn about a Java application known as the Oracle E-Business Suite (EBS) Asserter, including how it's used to integrate Oracle E-Business Suite with Oracle Identity Cloud Service. You can learn about the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM), including how it's used to integrate your Linux environment with Oracle Identity Cloud Service to perform end user authentication with first and second factor authentication. You can learn about an admin client known as the Secure Form Fill Client, including how it's used to configure Secure Form Fill for your applications. You can learn about the Identity Cloud Service Provisioning Bridge, including how it's used to install, start, and stop the client for the Provisioning Bridge. The Provisioning Bridge provides a link between your on-premises apps and Oracle Identity Cloud Service. You can learn about the Identity Cloud Service Device Fingerprint Utility, including how it's used to enable the <strong>Access for an unknown device</strong> event of Adaptive Security for a custom sign-in page.</td>
<td>Understand Oracle Identity Cloud Service SDKs and Applications</td>
</tr>
<tr>
<td>Download Oracle Identity Cloud Service SDKs and applications.</td>
<td>You can download SDKs, the EBS Asserter, the Linux PAM, the Secure Form Fill Client, the client for the Provisioning Bridge, and the Identity Cloud Service Device Fingerprint Utility using the <a href="#">Downloads page</a>.</td>
<td>Download Oracle Identity Cloud Service SDKs and Applications</td>
</tr>
</tbody>
</table>
Use Oracle Identity Cloud Service SDKs and applications.

You can access documentation, Oracle-by-Example (OBE) tutorials, and videos to learn how to use SDKs, the EBS Asserter, the Linux PAM, the Secure Form Fill Client, the Provisioning Bridge, and the Identity Cloud Service Device Fingerprint Utility.

You can download SDKs and applications by:

- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to download SDKs and applications by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Oracle Identity Cloud Service SDKs and Applications

You're an identity domain administrator or security administrator who wants to enable mobile and Web applications to authenticate with Oracle Identity Cloud Service. To do this, you use one of the options below.

You may want to integrate your Oracle E-Business Suite environment with Oracle Identity Cloud Service for authentication and password management purposes. To do this, you use a lightweight Java application known as the Oracle E-Business Suite (EBS) Asserter.

You may want to integrate your Linux environment with Oracle Identity Cloud Service to perform end user authentication with first and second factor authentication. To do this, you use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM).

If your web application supports header based authentication, then use App Gateway to protect access to your application. App Gateway acts as a reserve proxy protecting web applications by restricting unauthorized network access to them. These applications are called Enterprise Applications in Oracle Identity Cloud Service.

Oracle Identity Cloud Service can be used to provide single sign-on for your applications. These applications can be integrated with Oracle Identity Cloud Service using one of the following options:

- **App Catalog**: The App Catalog contains ready-to-use templates to integrate with most of your cloud-based applications.

- **SAML 2.0**: Use Oracle Identity Cloud Service as an identity provider for applications that support the SAML standard.
• **SDKs**: Use SDKs to develop applications to use the Oracle Identity Cloud Service authentication mechanism.

• **Open ID Connect**: Use Oracle Identity Cloud Service as the authentication server for applications that support the Open ID Connect standard.

• **OAuth 2.0**: Use Oracle Identity Cloud Service as the authorization server for applications that support the OAuth standard.

When none of these methods apply to the applications you need to integrate for authentication, use Secure Form Fill. To help you configure Secure Form Fill for your applications, Oracle Identity Cloud Service provides you with an admin client known as the Secure Form Fill Client.

You may want to establish a link between your on-premises apps and Oracle Identity Cloud Service. To do this, create a Provisioning Bridge. Through synchronization, account data that is created and updated directly on the apps is pulled into Oracle Identity Cloud Service (through the Provisioning Bridge) and stored for the corresponding Oracle Identity Cloud Service users and groups. As a result, any changes to this data will be transferred into Oracle Identity Cloud Service. So, if a user is deleted in one of your apps, then this change will be propagated into Oracle Identity Cloud Service. As a result, the state of each record is synchronized between your apps and Oracle Identity Cloud Service.

Creating a Provisioning Bridge includes using the Identity Cloud Service console to add a bridge, and then installing the client for this bridge.

Adaptive Security is an advanced feature of Oracle Identity Cloud Service that provides strong authentication capabilities for your users, based on their behavior within Oracle Identity Cloud Service, and across multiple heterogeneous on-premises applications and cloud services.

When activated, the Adaptive Security feature can analyze a user's risk profile within Oracle Identity Cloud Service when they sign in to access the service, based on their historical behavior and real-time device context, such as access from unknown devices.

Adaptive Security uses the concept of risk providers to allow administrators to configure various contextual and threat events to be analyzed within Oracle Identity Cloud Service. A default risk provider within Oracle Identity Cloud Service is seeded automatically with a list of supported contextual and threat events, such as **Access from an unknown device**. For this event, if a user accesses Oracle Identity Cloud Service from a device that hasn't been previously used to access the service, then this event (commonly referred to as Device Fingerprinting) is triggered.

Although Oracle Identity Cloud Service has a sign-in page, you may prefer to use your own page. If so, then you can use the Identity Cloud Service Device Fingerprint Utility to enable the **Access for an unknown device** event of Adaptive Security for your custom sign-in page.

Oracle Identity Cloud Service has a centralized location in the Identity Cloud Service console where you can download SDKs, the EBS Asserter, the Secure Form Fill Client, the Linux PAM, the Identity Cloud Service Provisioning Bridge Client, or the Identity Cloud Service Device Fingerprint Utility.

For this version of Oracle Identity Cloud Service, the following SDKs and applications are available:
Identity Cloud Service E-Business Suite Asserter

App Gateway for Identity Cloud Service

Identity Cloud Service Secure Form Fill Client

Identity Cloud Service Provisioning Bridge

Identity Cloud Service Linux Pluggable Authentication Module (PAM)

Identity Cloud Service Device Fingerprint Utility

Identity Cloud Service SDK for Java

Identity Cloud Service SDK for Node.js

Identity Cloud Service SDK for Python

Identity Cloud Service SDK for .NET

Identity Cloud Service SDK for Android

Identity Cloud Service SDK for iOS

Download Oracle Identity Cloud Service SDKs and Applications

You can download software development kits (SDKs) to develop your Web and mobile applications to authenticate and integrate them with Oracle Identity Cloud Service. You can also download the E-Business Suite Asserter to integrate Oracle E-Business Suite with Oracle Identity Cloud Service, the Secure Form Fill Client to configure Secure Form Fill for your applications, the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to integrate your Linux environments with Oracle Identity Cloud Service, the App Gateway binary file to enable you to integrate your enterprise applications with Oracle Identity Cloud Service, the client for the Provisioning Bridge to establish a link between your on-premises apps and Oracle Identity Cloud Service, or the Identity Cloud Service Device Fingerprint Utility to enable the Access for an unknown device event of Adaptive Security for your custom sign-in page.
1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Downloads**.

2. In the **Downloads** page, click **Download** to the right of the SDK or application that you want to download.

3. Verify that a **Success** status appears to the right of the SDK or application that you downloaded.

**Use Oracle Identity Cloud Service SDKs and Applications**

You’re a developer who wants to integrate Web applications with Oracle Identity Cloud Service. Oracle Identity Cloud Service provides you with software development kits (SDKs) that you can use to enable your Java, Node.js, Python, or .NET applications to authenticate with Oracle Identity Cloud Service. For more information about using these SDKs, refer to the following tutorials:

- Learn About Authenticating an Application with Oracle Identity Cloud Service by Using the Java SDK
- Learn About Authenticating an Application with Oracle Identity Cloud Service by Using the Node.js SDK
- Learn about Authenticating an Application with Oracle Identity Cloud Service by Using the Python SDK
- **Use Oracle Identity Cloud Service's Software Development Kit (SDK) for Authentication in .NET Web Applications**

If you're developing mobile applications, and you want to use Oracle Identity Cloud Service as an authentication server, then you can use SDKs to enable your mobile Android or iOS applications to authenticate with Oracle Identity Cloud Service. For more information on using these SDKs, refer to the following documentation:

- Learn About Authenticating an Android Mobile App with Oracle Identity Cloud Service
- Learn About Authenticating an iOS Mobile App with Oracle Identity Cloud Service

If your web application uses header variables to identify the user logged in, then you can use the App Gateway to integrate your application with Oracle Identity Cloud Service for authentication purposes. App Gateway acts as a reserve proxy protecting your application by restricting unauthorized network access to the application or ensuring that the users are authenticated in Oracle Identity Cloud Service before forwarding the request to the application. For more information about using the App Gateway, see **Secure Enterprise Applications with App Gateway**.

If you can't change the source code of your Web application or the application isn't based on headers, then use Oracle Identity Cloud Service's Secure Form Fill. The Secure Form Fill Client helps you map the sign in form for your Web application so Oracle Identity Cloud Service knows how to populate the user's user name and password automatically, and submit the user's credentials to the application's identity store. For more information about using the Secure Form Fill Client, see **Use Secure Form Fill to Authenticate an Application with Oracle Identity Cloud Service**.

You may have to integrate your Oracle E-Business Suite (EBS) environment with other cloud services in single-sign-on (SSO) mode using Oracle Identity Cloud Service. Oracle Identity Cloud Service provides a lightweight Java application known as the EBS Asserter that implements SSO. By using the EBS Asserter, you can integrate Oracle E-Business Suite with Oracle Identity Cloud Service for authentication and
password management purposes. For more information about using the EBS Asserter, refer to one of the following tutorials:

- Learn About Authenticating Oracle E-Business Suite with Oracle Identity Cloud Service Using the E-Business Suite Asserter
- Configure Oracle E-Business Suite to Use Oracle Identity Cloud Service for Single Sign-On (SSO)

You may want to integrate your Linux environment with Oracle Identity Cloud Service to perform end user authentication with first and second factor authentication. Oracle Identity Cloud Service provides a module known as the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM). For more information about using the Linux PAM, see Manage Linux Authentication using the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM).

If you want to establish a link between your on-premises apps and Oracle Identity Cloud Service, then create a Provisioning Bridge. By doing so, you’re synchronizing user and group account data that’s created and updated directly on the apps with Oracle Identity Cloud Service. Any changes to this data will be transferred into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. For more information about using the Provisioning Bridge, see Synchronize Users from Oracle Internet Directory to Oracle Identity Cloud Service.

If you have a custom sign-in page for Oracle Identity Cloud Service and you want to enable the Access for an unknown device event of Adaptive Security for your page, then use the Identity Cloud Service Device Fingerprint Utility. If a user uses your sign-in page to access Oracle Identity Cloud Service from a device that hasn’t been previously used to access the service, then this event is triggered. For more information about using the Identity Cloud Service Device Fingerprint Utility, see Enable the ‘Access for an unknown device’ Event for a Custom Sign-In Page.
Customize Schemas in Oracle Identity Cloud Service

Learn how to add, edit, or delete custom schema attributes in Oracle Identity Cloud Service.

Topics:
• Add Custom Schema Attributes
• Edit Custom Schema Attributes

Add Custom Schema Attributes

If you are creating your own user interface, and you do not find a schema attribute that you need in the base Oracle Identity Cloud Service schema attributes, you can add your own custom attribute using the Oracle Identity Cloud Service user interface.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Schema Management.
2. Click the Action menu for the User schema, and then select Edit Schema.
3. Click Add.

**Important:**
Once you create a custom schema attribute, if data exists for that attribute, you cannot delete it.

4. Complete the attribute details.
   • **Display name**: The attribute name that appears in the Attributes page.
   • **Name**: The attribute name that is recognized by the Oracle Identity Cloud Service server.
   • **Description**: Provide further information related to its usage and other details that helps the user identify this attribute.
   • **Data type**: Select **String** for numerical values or **String array** for alpha numeric values.
   • **Min length**: Select the minimum length of the attribute value. Minimum value allowed is 1.
   • **Max length**: Select the maximum length of the attribute value. The maximum allowed value is 4000.
   • **Searchable**: If this check box is selected, then the values for this attribute can be used in searches. If it's not selected, then the values can't be used for searches.
5. Click Save.

The custom attribute is created.

Tip:
Open the custom attribute to find the custom attribute FQN.

Edit Custom Schema Attributes

After you create a custom attribute, you might need to change the custom attribute settings. For example, you might need to adjust the min and max length for the attribute.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Schema Management.

2. Click the Action menu for the User schema, and then select Edit Schema.

3. On the Attributes page, in the Filter attribute type section, choose Custom, and then locate the custom attribute that you want to edit.

4. In the attribute page, you can edit the values of Display name, Description, Min length and Max length of the attribute.

   • To delete the attribute, click the delete button ✗, and then in the Confirmation window, click OK.

   Note:
   If data exists for that attribute, you cannot delete it.

   • To edit the custom attribute, click the Display name of the attribute, make any changes necessary, and then click Save.
Part V
Configure Security Settings

Learn how to configure important security settings.

Chapters

• Manage Terms of Use
• Manage Adaptive Security in Oracle Identity Cloud Service
• Manage Oracle Identity Cloud Service Identity Providers
• Manage Oracle Identity Cloud Service Identity Provider Policies
• Manage Oracle Identity Cloud Service Sign-On Policies
• Manage Oracle Identity Cloud Service Network Perimeters
• Manage Oracle Identity Cloud Service App Gateways
• Manage Account Recovery in Oracle Identity Cloud Service
• Manage Oracle Identity Cloud Service Multi-Factor Authentication Settings
• Manage Oracle Identity Cloud Service OAuth Settings
• Configure Delegated Authentication in Oracle Identity Cloud Service
• Transferring Oracle Identity Cloud Service Configuration Data
Manage Terms of Use

Oracle Identity Cloud Service allows the customer to present disclaimers and acceptable use policies, also known as Terms of Use, to its users. The customer can configure Terms of Use on an application basis and collect consent from users prior to allowing them access to the application. As a domain or security administrator, you can manage Terms of Use and perform the following:

Topics:
- Understand Terms of Use
- Add a Terms of Use
- View Details of Terms of Use
- Modify Terms of Use
- Remove Terms of Use
- Activate and Deactivate Terms of Use

Understand Terms of Use

The Terms of Use are the rules that one must agree to abide in order to access an application.

The Terms of Use feature in Oracle Identity Cloud Service helps customer to set the terms and conditions for the users to access an application, based on the user's consent. This feature allows the identity domain administrator to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service.

In Oracle Identity Cloud Service, you can grant or deny access to the applications based on the consent provided by the user. When the user logs in for the first time, the relevant disclaimers for legal or compliance requirements are displayed. The user has the option of either accepting or denying his consent for accessing that particular application based on the content of the disclaimer. If the user does not provide his consent by accepting the Terms of Use, he will not be allowed to access that particular application. As a domain or security administrator, you can create or customize your disclaimers based on the need and language of your choice.

Add a Terms of Use

You create a Terms of Use that you can map it to an application or to multiple applications. When a user tries to access a particular application, the Terms of Use mapped to that application is presented to the user. When the user accepts the terms of use and provides his consent, he is allowed to access that application.

To create a Terms of Use, perform the following procedure:

1. From the navigation drawer, click **Security** and then click **Terms of Use**.
2. In the Terms of Use screen, click Add.

3. In the Add Terms of Use screen, enter the following details:
   - **Name**: Enter a name for the Terms of Use to easily identify it.
   - **Description**: Enter the description to help understand the purpose and usage of this Terms of Use.
   - **Duration**: Enter the duration for which the Terms of Use consent will be valid. The value can range between 1 and 365 days. Select *Never Expires* if you do not want this Terms of Use to expire.

   Click **Next** to proceed to the Statements screen. A confirmation message is displayed.

4. In the Statements screen, click Add and perform the following:
   - **Language**: A list of supported language is displayed. Select the language in which you want to create the statement for your Terms of Use.
   - **Statement**: Enter or paste the statement content.

   Click **Save**.

5. In the Assign Applications screen, click Add and perform the following:
   - Search and select the application that you want to assign to this Terms of Use. Alternatively you can select multiple applications to assign them with this Terms of Use.

   Click **OK** and the confirmation message is displayed.

6. Click **Finish**.

---

**View Details of Terms of Use**

You can view the details of a particular Terms of Use, like Name, Description, Duration, Statements and the applications that are assigned to the particular Terms of Use.

1. From the navigation drawer, click **Security** and then click **Terms of Use**. The list of Terms of Use that are already created is displayed.

2. Click the required Terms of Use to view the details.

---

**Modify Terms of Use**

You can modify the details of a particular Terms of Use, like Name, Description, Duration, Statements and the applications that are assigned to the particular Terms of Use.

1. From the navigation drawer, click **Security** and then click **Terms of Use**. The list of Terms of Use that are already created is displayed.

2. Click the required Terms of Use to modify the details.
Remove Terms of Use

You can remove the Terms of Use that you do not need.

To remove a particular Terms of Use, perform the following procedure:

1. To modify a Terms of Use, under Security, click Terms of Use and the list of Terms of Use is displayed.
2. Click the name of the required Terms of Use, then click the menu option, and then click Remove.

Note:
Alternatively, you can remove a particular Terms of Use by selecting the check box in front of the Terms of Use name, and then click X Remove.

Activate and Deactivate Terms of Use

Based on your requirement, you can activate or deactivate a particular Terms of Use.

Note:
Every newly created Terms of Use will be in the deactivated state.

To activate or deactivate a particular Terms of Use, perform the following procedure:

1. From the navigation drawer, click Security and then click Terms of Use. A list of Terms of Use is displayed.
2. In the Terms of Use screen, perform the following:
   - **Activate**: Select the check box in front of the Terms of Use name, and then click Activate. Alternatively, you can click the menu option of the particular Terms of Use, and then click Activate.
   - **Deactivate**: Select the check box in front of the Terms of Use name, and then click Deactivate. Alternatively, you can click the menu option of the particular Terms of Use, and then click Deactivate.
Manage Adaptive Security in Oracle Identity Cloud Service

This section describes how to manage Adaptive Security in Oracle Identity Cloud Service.

Topics:

• Typical Workflow for Managing Adaptive Security in Oracle Identity Cloud Service
• Understand Adaptive Security
• Why Use Adaptive Security?
• Activate and Deactivate Adaptive Security
• Understand Risk Providers
• Configure Oracle Identity Cloud Service Risk Events
• View Details About a Risk Provider
• Add a Third-Party Risk Provider
• Activate and Deactivate Risk Providers
• Modify a Third-Party Risk Provider
• Remove a Third-Party Risk Provider

Typical Workflow for Managing Adaptive Security in Oracle Identity Cloud Service

With the Adaptive Security feature in Oracle Identity Cloud Service, you can perform tasks such as managing Adaptive Security and risk providers.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand Adaptive Security and risk providers.</td>
<td>You can learn about Adaptive Security, and how it’s used to provide strong authentication capabilities for your users, based on their behavior within Oracle Identity Cloud Service, and across multiple heterogeneous on-premises applications and cloud services. You can also learn why you should use Adaptive Security, and how Adaptive Security uses risk providers to allow administrators to configure various contextual and threat events to be analyzed within Oracle Identity Cloud Service, and also to configure and consume user risk scores from third-party risk providers.</td>
<td>Understand Adaptive Security Why Use Adaptive Security Understand Risk Providers</td>
</tr>
<tr>
<td>Configure Oracle Identity Cloud Service risk events.</td>
<td>You can modify risk events for the risk provider that’s associated with Oracle Identity Cloud Service actions using the Adaptive Security page.</td>
<td>Configure Oracle Identity Cloud Service Risk Events</td>
</tr>
<tr>
<td>View details about a risk provider.</td>
<td>You can view details about a risk provider using the Adaptive Security page.</td>
<td>View Details About a Risk Provider</td>
</tr>
<tr>
<td>Add a third-party risk provider.</td>
<td>You can add a third-party risk provider using the Adaptive Security page.</td>
<td>Add a Third-Party Risk Provider</td>
</tr>
<tr>
<td>Activate and deactivate risk providers.</td>
<td>You can activate and deactivate risk providers using the Adaptive Security page.</td>
<td>Activate and Deactivate Risk Providers</td>
</tr>
<tr>
<td>Modify third-party risk providers.</td>
<td>You can modify third-party risk providers using the Adaptive Security page.</td>
<td>Modify a Third-Party Risk Provider</td>
</tr>
<tr>
<td>Remove a third-party risk provider.</td>
<td>You can remove a third-party risk provider using the Adaptive Security page.</td>
<td>Remove a Third-Party Risk Provider</td>
</tr>
</tbody>
</table>

You can create, manage, and remove Adaptive Security and risk providers by using:

- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage Adaptive Security and risk providers by using the Identity Cloud Service console.
Understand Adaptive Security

Adaptive Security is an advanced feature that provides strong authentication capabilities for your users, based on their behavior within Oracle Identity Cloud Service, and across multiple heterogeneous on-premises applications and cloud services.

When activated, the Adaptive Security feature can analyze a user’s risk profile within Oracle Identity Cloud Service based on their historical behavior, such as too many unsuccessful login attempts and too many unsuccessful MFA attempts, and real-time device context, such as access from unknown devices, impossible travel between locations, and so on. To evaluate the user’s behavior across other systems with which Oracle Identity Cloud Service isn’t directly involved, Adaptive Security allows you to configure your existing risk providers to obtain the user’s risk score from third-party risk providers, such as Symantec CloudSOC Cloud Access Security Broker (CASB). With this enriched context and risk information, Adaptive Security risk profiles each user, and arrives at its own risk score and an overall consolidated risk level (High, Medium, Low) that can be used with Oracle Identity Cloud Service policies to enforce a remediation action, such as allowing or denying the user from accessing Oracle Identity Cloud Service and its protected applications and resources, requiring the user to provide a second factor to authenticate into Oracle Identity Cloud Service, and so on. Administrators can also view how the user’s risk profile trended over a period of time, and drill down to see details associated with each event.

Why Use Adaptive Security?

Users are connected increasingly, accessing their accounts and applications from multiple locations, devices, and channels. Implementing overly restrictive and static controls to secure access (for example, prompting a user for a second factor for every authentication or blocking access to a user when the user is out of their base country) would result in a painful user experience with no overall improvements in security.

Adaptive Security can analyze contextual, risk, and threat information about the user, device, and network, and provide an intelligent, secure, and user-friendly way of providing access to corporate applications and resources. This also reduces the likelihood of online identity theft and fraud, which secures your business applications even if the user’s device or the user’s account password is compromised.

Activate and Deactivate Adaptive Security

You can activate or deactivate the Adaptive Security feature.

- Deactivating Adaptive Security stops Oracle Identity Cloud Service from performing contextual and threat event analytics, and obtaining user risk scores from third-party risk providers.
- Activating Adaptive Security allows Oracle Identity Cloud Service to start evaluating contextual and threat analysis, and obtain user risk scores from the configured third-party risk providers.
Activate Adaptive Security

You can use Oracle Identity Cloud Service to activate Adaptive Security.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Adaptive Security.

Deactivate Adaptive Security

You can use Oracle Identity Cloud Service to deactivate Adaptive Security.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Adaptive Security.

Understand Risk Providers

Adaptive Security uses the concept of risk providers to allow identity domain administrators and security administrators to configure various contextual and threat events to be analyzed within Oracle Identity Cloud Service, and also to configure and consume user risk scores from third-party risk providers.

A default risk provider within Oracle Identity Cloud Service is seeded automatically with a list of supported contextual and threat events, such as too many unsuccessful login attempts, too many unsuccessful MFA attempts, access from unknown devices, access from unfamiliar locations, access from suspicious IP addresses, and impossible travel between locations. Administrators can enable events of interest, and specify weighting or severity for each of these events. The system uses the configured weighting to compute the user’s Oracle Identity Cloud Service risk score.
Example:

Consider a user who logs into Oracle Identity Cloud Service using a new device, say a laptop. Because the device is unknown, the system won’t recognize the device, and will the trigger the **Access from an unknown login device** event and get the weighting from the configuration. There are six events in the risk provider configuration: **Access from an unknown device**, **Too many unsuccessful login attempts**, **Too many unsuccessful MFA attempts**, **Access from suspicious IP addresses**, **Access from an unfamiliar location**, and **Impossible travel between locations**.

The administrator can assign weighting to these events that correspond to those risk ranges. Consider the weighting for each of the risks as follows: low risk range (0-25), medium risk range (26-75) and high risk range (76-100). If the administrator wants to consider the user login from an unknown device to be of low risk, then the administrator sets the weighting for that event to be less than 25. If the administrator wants to consider the same event to be of medium risk, then the administrator sets the weighting for that event to be between 26 and 75. Any value set above 75 for that event is considered as high risk. If the user hits more than one event, then the risk score will be a combination of two weightings and will correspond to whichever risk level the combination points. The user’s risk scores are evaluated continuously and are reduced based on the remediation actions that are taken by the user, such as successful logins and password resets.

Administrators can add additional risk providers to obtain a user’s risk score from the Symantec third-party risk engine. This risk engine provides additional intelligence on the user’s behavior across heterogeneous systems with which Oracle Identity Cloud Service isn’t directly involved.

To provide a consolidated risk profile of the user at any time, Oracle Identity Cloud Service takes the highest level of the risk scores of both the default Oracle Identity Cloud Service risk provider and the configured third-party risk providers, and qualifies the user as a high-risk, medium-risk, or low-risk user. For instance, if a user’s risk score from the default risk provider is within the Low range, but the risk score from a third-party risk provider is within the Medium range, then the user’s consolidated risk level is set to Medium.

Administrators can then use the Oracle Identity Cloud Service risk score, third-party risk score, or consolidated user risk level as conditions that can be used with Oracle Identity Cloud Service sign-on policies to enforce a remediation action, such as allowing or denying the user from accessing Oracle Identity Cloud Service and its protected applications and resources, requiring the user to provide a second factor to authenticate into Oracle Identity Cloud Service, and so on.

**Configure Oracle Identity Cloud Service Risk Events**

You can modify risk events for the risk provider that’s associated with Oracle Identity Cloud Service actions. When this risk provider, known as the default risk provider, is activated, it evaluates the following events that constitute risk-based activity for Oracle Identity Cloud Service users:
• **Access from an unfamiliar location:** If a user accesses Oracle Identity Cloud Service from a location that hasn’t been used previously to access the service, then this event is triggered. Oracle Identity Cloud Service obtains the user’s current access location, using the IP address, and determines if this location has been used previously. If it's a new location, then the service determines the distance between the current access location and the user’s immediately preceding access location. If the distance between these two locations exceeds the value specified in the threshold, then this event is triggered.

• **Access from an unknown device:** If a user accesses Oracle Identity Cloud Service from a device that hasn’t been previously used to access the service, then this event (commonly referred to as Device Fingerprinting) is triggered.

• **Access from suspicious IP addresses:** If the IP address from where the user is accessing Oracle Identity Cloud Service is flagged as suspicious by the integrated IP reputation provider, then this event (commonly referred to as IP reputation) is triggered.

• **Impossible travel between locations:** Oracle Identity Cloud Service obtains the user’s current access location, using the IP address, and calculates the distance between this location and the user’s immediately preceding access location. If it determines that this distance can’t be covered at the speed specified in the threshold, then this event (commonly referred to as geo-velocity) is triggered.

• **Too many unsuccessful login attempts:** If the number of unsuccessful login attempts exceed the value specified for the **Account lock threshold** attribute for the password policy, then this event is triggered.

  **Note:**
  See [Modify the Custom Password Policy](#) to learn how to set the maximum number of unsuccessful logins that the user can attempt in Oracle Identity Cloud Service before they’re locked out of their account.

• **Too many unsuccessful MFA attempts:** If the number of unsuccessful login attempts using the factors configured exceed the value specified for the **Max Unsuccessful MFA attempts** attribute for MFA, then this event is triggered.

  **Note:**
  See [Configure Multi-Factor Authentication Settings](#) to learn how to set the maximum number of unsuccessful MFA logins that the user can attempt in Oracle Identity Cloud Service using their MFA factors before they’re locked out of their account.

  **Note:**
  If an event is disabled, then Oracle Identity Cloud Service won’t use it to generate a risk score that can be used to evaluate risk-based activity for Oracle Identity Cloud Service users. Also, if the default risk provider is deactivated, then the user’s risk score won’t be increased.
Modifying the default risk provider includes:

- Changing the description of the risk provider.
- Setting the Low, Medium, and High risk range for this risk provider.
- Enabling or disabling the individual events for contextual and threat analytics.
- Setting a value (weighting) for each event that corresponds to the risk range for this risk provider. For example, suppose you set the Low risk range for the risk provider to be from 0-10, the Medium risk range to be from 11-80, and the High risk range to be from 81-100. For example, if you set the weighting of the **Access from an unknown device** event to 20, and a low-risk user accesses Oracle Identity Cloud Service with a device that is previously not used which Oracle Identity Cloud Service doesn't recognize, then the user's risk range will change to Medium.

To modify the default risk provider:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Adaptive Security**.
2. In the **Adaptive Security** page, click the **Action** menu to the right of the default risk provider.
3. Select **Edit**. The risk provider opens and displays three panes: **Details**, **Risk Range**, and **Events**. See **Add a Third-Party Risk Provider** for more information about the **Details** and **Risk Range** panes.
4. Change the values that you want to modify in the **Details** and **Risk Range** panes.
5. In the **Events** pane:
   a. Select or deselect a check box to enable or disable the event. By doing so, you're specifying whether Oracle Identity Cloud Service will use this event to generate a risk score that can be used to evaluate risk-based activity for Oracle Identity Cloud Service users.
   
   **Note:**
   
   If you disable all events for the default risk provider, then you can't save it.

   b. If you enabled the **Access from an unfamiliar location** event, then enter or select the distance for the threshold between the user's current location, which hasn't been used to access the service, and the user's preceding access location. If the distance between these two locations exceeds the value that you specify for the threshold, then this event is triggered. After setting the threshold for the distance, specify whether this distance is in miles (mi) or kilometers (km).

   c. If you enabled the **Access from suspicious IP addresses** event, then in the **Excluded IP Addresses** field, enter or select any network perimeters that you want to exclude for this event. User access from IP addresses contained in these network perimeters won't be considered for risk analysis even if they're flagged as suspicious by the integrated IP reputation provider. See **Understand Network Perimeters**.
Oracle Identity Cloud Service scans for malicious IP addresses across 11 categories. These categories are: Windows Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, TOR Proxies, Anonymous Proxies, Reputation, Spam Sources, and Mobile Threats. By doing so, Oracle Identity Cloud Service gains dramatic improvements in security efficacy and efficiency, as the time required to identify IP threats is drastically reduced.

d. If you enabled the **Impossible travel between locations** event, then enter or select the speed for the threshold that Oracle Identity Cloud Service uses to determine whether the distance can be covered between the user's current location and the user's preceding access location. Then, specify whether this speed is in miles per hour (MPH) or kilometers per hour (KPH).

e. Use the slider to set the weighting for each event to **Low**, **Moderate**, **Severe**, or **Critical**.

6. Click **Save**.

7. In the **Confirmation** window, click **OK**.

### View Details About a Risk Provider

By default, you can see the name, company, and activation status of each risk provider you added to Oracle Identity Cloud Service. You can also see other information, such as the risk levels and authentication information associated with the risk provider.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Adaptive Security**.

2. In the **Adaptive Security** page, click the risk provider about which you want to see more information.

   The risk provider opens and displays two panes: **Details** and **Risk Range**. See **Add a Third-Party Risk Provider** for more information about these panes.

   **Note:**

   If you clicked the default risk provider, then you'll see a third pane: **Events**. See **Configure Oracle Identity Cloud Service Risk Events** to learn more about this pane.

### Add a Third-Party Risk Provider

You can add a risk provider to Oracle Identity Cloud Service that can be used to obtain a user's risk score from the Symantec third-party risk engine. This risk score provides additional intelligence on the user's behavior across heterogeneous systems with which Oracle Identity Cloud Service isn't directly involved. Administrators can then use this third-party risk score with Oracle Identity Cloud Service sign-on policies to enforce a remediation action, such as allowing or denying the user from accessing Oracle Identity Cloud Service and its protected applications and resources, requiring the user to provide a second factor to authenticate into Oracle Identity Cloud Service, and so on.

   ![Note:]

   In the Adaptive Security page, Oracle Identity Cloud Service provides you with a default risk provider which can’t be deleted. See Configuring the Default Risk Provider for more information about this risk provider.

2. Click Add. The New Risk Provider page appears.

3. Use the following table to populate the Details pane of the New Risk Provider page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>Select the vendor of the risk provider solution.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the risk provider.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a brief description of the risk provider.</td>
</tr>
<tr>
<td>Endpoint Configuration URL</td>
<td>Enter the risk provider URL that Oracle Identity Cloud Service can use to reach out to obtain the user’s risk score.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>This menu contains two methods that Oracle Identity Cloud Service uses to authenticate against the risk provider: BASIC and TOKEN. If you select BASIC, then the User Name and Password fields appear. Enter the user name and password that Oracle Identity Cloud Service will use to authenticate against the risk provider. If you select TOKEN, then the Scheme and Token fields appear. Enter the name of the authentication scheme and the authentication token that Oracle Identity Cloud Service will use to pass a user’s credentials to the risk provider.</td>
</tr>
<tr>
<td>User Identifier</td>
<td>Select the unique identifier for user accounts that Oracle Identity Cloud Service will use to link the user in the risk provider. This identifier can be either the user name or the primary email address.</td>
</tr>
<tr>
<td>Refresh Rate</td>
<td>Specify how often (in minutes or hours) Oracle Identity Cloud Service will make a call to the risk provider to check for refreshed scores.</td>
</tr>
</tbody>
</table>

4. To check whether the risk provider information is correct, click Validate.

   Verify that you see the The connection to the {risk_provider_name} risk provider has been validated. message.
5. In the Risk Range pane of the Add Risk Provider page, the risk levels configured in the risk provider will be shown automatically, if the provider supports an API to get this information. If the API is not available, then the administrator can specify the risk ranges manually, as configured in the risk provider. This is just to provide a reference to the configured risk ranges in the risk provider and has no significance in the risk calculations.

6. Click Save. The risk provider is added and saved with a deactivated status. See Activate a Risk Provider for more information about activating this risk provider.

### Activate and Deactivate Risk Providers

You can activate or deactivate individual risk providers.

**Note:**

If the default risk provider is deactivated, then none of the events configured in this risk provider will be considered for the user’s risk score analysis. Also, if third-party risk providers are deactivated, risk scores will not be fetched from these risk providers.

In addition to enabling and disabling the Adaptive Security feature, you can activate or deactivate one or more risk providers individually.

**Note:**

A green check mark ✅ indicates an activated risk provider. A red circle with a red line through the circle ❌ indicates a deactivated risk provider.

**Topics:**

- Activate a Risk Provider
- Deactivate a Risk Provider

### Activate a Risk Provider

You can use Oracle Identity Cloud Service to activate a risk provider.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Adaptive Security.
2. In the **Adaptive Security** page, click the **Action** menu  to the right of the risk provider that you want to activate.

3. Select **Activate**.

4. In the **Confirmation** window, click **OK**. The status of the risk provider changes from deactivated ☑️ to activated ✔️.

**Deactivate a Risk Provider**

You can use Oracle Identity Cloud Service to deactivate a risk provider.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Adaptive Security**.

2. In the **Adaptive Security** page, click the **Action** menu  to the right of the risk provider that you want to deactivate.

3. Select **Deactivate**.

4. In the **Confirmation** window, click **OK**. The status of the risk provider changes from activated ✔️ to deactivated ☑️.

**Modify a Third-Party Risk Provider**

After viewing details about, activating, or deactivating a risk provider that you added, you can modify it. Modifying this type of risk provider includes:

- Changing the name or description of the risk provider.
- Editing the endpoint configuration URL, authentication type, or authentication credentials of the risk provider.
- Specifying a different unique identifier for user accounts that the risk provider will use to evaluate risk-based activity for the users.
- Changing how often (in minutes or hours) the risk provider will evaluate risk-based activity for users.
- Modifying the Low, Medium, and High risk range for the risk provider.

To modify a third-party risk provider:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Adaptive Security**.

2. In the **Adaptive Security** page, click the **Action** menu  to the right of the risk provider that you want to modify.

3. Select **Edit**. The risk provider opens and displays two panes: **Details** and **Risk Range**. See **Add a Third-Party Risk Provider** for more information about these panes.

4. Change the values that you want to modify in the **Details** and **Risk Range** panes.

5. Click **Validate**. Verify that you see the **The connection to the {risk_provider_name} risk provider has been validated** message.
Note:
If you receive an error message, then check the values you changed for the Endpoint Configuration URL and Authentication Type fields.

6. Click Save.
7. In the Confirmation window, click OK.

Remove a Third-Party Risk Provider

If a third-party risk provider is no longer needed to provide its user risk score to Oracle Identity Cloud Service, then you can remove it.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Adaptive Security.

2. In the Adaptive Security page, if the risk provider that you want to remove is activated, then deactivate it. See Deactivate a Risk Provider.

3. Click the Action menu to the right of the risk provider that you want to remove.

Note:
Because the default risk provider is associated with Oracle Identity Cloud Service events, such as whether users access Oracle Identity Cloud Service with devices that aren't registered, or users exceed the number of consecutive, unsuccessful login attempts into Oracle Identity Cloud Service allowed, you can't remove this risk provider.

4. Select Edit.
5. Click Delete.
Manage Oracle Identity Cloud Service Identity Providers

Learn how to manage identity providers for Oracle Identity Cloud Service.

Topics

- Typical Workflow for Managing Oracle Identity Cloud Service Identity Providers
- Understand Identity Providers
- Add an Identity Provider
- View Details About an Identity Provider
- Activate and Deactivate an Identity Provider
- Test an Identity Provider
- Modify an Identity Provider
- Delete an Identity Provider

Typical Workflow for Managing Oracle Identity Cloud Service Identity Providers

With the identity provider feature in Oracle Identity Cloud Service, you can perform tasks such as adding, managing, and using identity providers.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand identity providers.</td>
<td>Learn about digital certificates, identity providers, and identity provider certificates that Oracle Identity Cloud Service uses.</td>
<td>Understand Identity Providers</td>
</tr>
<tr>
<td>Add an identity provider.</td>
<td>Add an identity provider to your identity domain using the Identity Providers page.</td>
<td>Add an Identity Provider</td>
</tr>
<tr>
<td>View details about an identity provider.</td>
<td>View details about an identity provider using the Identity Providers page.</td>
<td>View Details About an Identity Provider</td>
</tr>
<tr>
<td>Activate and deactivate an identity provider.</td>
<td>Activate and deactivate an identity provider using the Identity Providers page.</td>
<td>Activate and Deactivate an Identity Provider</td>
</tr>
<tr>
<td>Test an identity provider.</td>
<td>Test an identity provider to verify that you can use federated SSO credentials to log in to Oracle Identity Cloud Service through an external website.</td>
<td>Test an Identity Provider</td>
</tr>
</tbody>
</table>
Understand Identity Providers

In this topic, you learn about digital certificates, identity providers, and identity provider certificates that Oracle Identity Cloud Service uses.

- About Digital Certificates
- About Identity Providers

About Digital Certificates

In this topic, you learn about digital certificates that Oracle Identity Cloud Service uses.

A digital certificate is like an electronic passport that allows a person, computer, or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it is issued by an official, trusted agency. The certificate can contain the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it's digitally signed by a root certificate that belongs to a trusted CA. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed.

There are two types of Oracle Identity Cloud Service certificates: certificates for identity providers and certificates for trusted partners. See Understand Trusted Partner Certificates for more information about trusted partner certificates.

About Identity Providers

In this topic, you learn about Identity providers that Oracle Identity Cloud Service uses.
An identity provider, known as an Identity Assertion provider, provides identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service. A service provider is a website such as Oracle Identity Cloud Service that hosts applications. You can enable an identity provider and define one or more service providers. Your users can then access the applications hosted by the service providers directly from the identity provider.

For example, a website can allow users to log in to Oracle Identity Cloud Service with Google credentials. Google acts as the identity provider and Oracle Identity Cloud Service functions as the service provider. Google verifies that the user is an authorized user and returns information to Oracle Identity Cloud Service (for example, the user name and the email address of the user, if the email address differs from the user name).

A user must be authenticated only once. For this example, the user obtains a security token. This security token is then validated by Google so that the user can access Oracle Identity Cloud Service. This method is known as federated single sign-on (SSO), where a single token for the user is trusted across multiple IT systems. The same token can be used to authenticate the user against both the identity provider and the service provider (for this example, Google and Oracle Identity Cloud Service).

Oracle Identity Cloud Service uses identity provider certificates that support several security token types, including Security Assertion Markup Language (SAML) 2.0 and X.509.

### Add an Identity Provider

There are two ways that you can add a SAML 2.0 identity provider in Oracle Identity Cloud Service:

- You can import metadata for the identity provider. Identity provider metadata summarizes the basic information about data associated with the identity provider. This metadata makes finding and working with this data easier.
- You can enter metadata for the identity provider.

If a CRL checking error occurs, see Create a SAML Partner and CRL Validation to resolve the issue.

Oracle Identity Cloud Service provides you with a wizard to add a SAML 2.0 identity provider. This wizard contains six panes:

- **Details**: Provide a name, description, and icon for the SAML identity provider.
- **Configure**: Configure SSO for the identity provider by either importing metadata for it or entering metadata for it.
- **Map**: Map a user's attribute value received from the identity provider to a corresponding attribute value for the user in Oracle Identity Cloud Service.

After providing information in the Map pane of the wizard, Oracle Identity Cloud Service adds and deactivates the identity provider. You may want to export metadata for the identity provider, test it, or activate it. The wizard has the Export, Test, and Activate panes.

- **Export**: Export metadata for Oracle Identity Cloud Service and import this metadata into the identity provider. The identity provider requires this information to communicate with Oracle Identity Cloud Service for authentication purposes.
Tip:
If the identity provider doesn't support importing metadata, then the information for Oracle Identity Cloud Service appears in the Export pane. You can enter this metadata into the identity provider manually.

- **Test**: Test the configuration settings for the identity provider to confirm that the identity provider is working properly. You can use the credentials of the identity provider to log in to Oracle Identity Cloud Service through an external website.
- **Activate**: Activate the identity provider.

Tip:
Suppose you want a user to use their single sign-on (SSO) credentials to authenticate against Oracle Identity Cloud Service, but you want the user to use the password that's provided by the SAML identity provider (instead of their Oracle Identity Cloud Service password). To do this, turn on the **Federated** switch for the user's account. See Edit Attribute Values for the User Account to learn how to turn on or off this switch.

Oracle Identity Cloud Service also provides you with a wizard to add a social identity provider. This wizard contains two panes:

- **Details**: Provide a name, description, and icon for the social identity provider.
- **Configure**: Configure SSO for the identity provider by entering metadata for it.

To add an identity provider, you must be assigned to either the identity domain administrator role or the security administrator role. See Add or Remove a User Account from an Administrator Role.

**Important**:
After you add the identity provider, you must add it to the default identity provider policy. By doing so, it will appear in the Sign In page and can be used by a user who's trying to sign in to Oracle Identity Cloud Service, either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console. See Add an Identity Provider Policy.

**Import Metadata for a SAML Identity Provider**

You can use Oracle Identity Cloud Service to import metadata for a SAML 2.0 identity provider.

If a CRL checking error occurs, see Create a SAML Partner and CRL Validation to resolve the issue.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Identity Providers.
2. Click **Add SAML IDP**. The **Add Identity Provider** wizard appears.

3. Use the following table to populate the **Details** pane of the wizard, and click **Next**:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the identity provider.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter explanatory information about the identity provider.</td>
</tr>
<tr>
<td>Icon</td>
<td>Click <strong>Upload</strong> to add an icon that represents the identity provider.</td>
</tr>
</tbody>
</table>

4. Use the following table to populate the **Configure** pane of the wizard, and click **Next**:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Identity Provider metadata</td>
<td>Click this button because you want to configure SSO for the identity provider by importing metadata for it.</td>
</tr>
<tr>
<td>Metadata</td>
<td>Click <strong>Upload</strong>. Select the XML file that contains the metadata for the identity provider that you want to import.</td>
</tr>
<tr>
<td>Signature Hashing Algorithm</td>
<td>From the menu, select the secure hash algorithm used to encrypt the signing certificate for the identity provider.</td>
</tr>
<tr>
<td></td>
<td>• By default, select the SHA-256 algorithm.</td>
</tr>
<tr>
<td></td>
<td>• If the identity provider doesn't support SHA-256, then select SHA-1.</td>
</tr>
<tr>
<td>Include Signing Certificate</td>
<td>To include a signing certificate with your identity provider, select this check box. The signing certificate is used to verify the</td>
</tr>
<tr>
<td></td>
<td>signature of the messages for the identity provider.</td>
</tr>
<tr>
<td></td>
<td>If you don't want to include a signing certificate with your identity provider, then leave the check box deselected.</td>
</tr>
</tbody>
</table>

5. Use the following table to populate the **Map** pane of the wizard, and click **Next**:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider User Attribute</td>
<td>Select the attribute value received from the identity provider that can be used to uniquely identify the user. You can specify the user ID or another SAML attribute (such as the user's email address).</td>
</tr>
<tr>
<td>Oracle Identity Cloud Service User Attribute</td>
<td>Select the attribute in Oracle Identity Cloud Service to which you are mapping the attribute received from the identity provider.</td>
</tr>
</tbody>
</table>
### Task Description

**Requested NameID Format**
Select the format for mapping the user’s attribute value in the identity provider to the corresponding attribute in Oracle Identity Cloud Service. If you don’t want to provide a format, then select *<None Requested>*.

6. Use the following table to populate or reference the Export pane of the wizard, and click **Next**:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Provider Metadata</strong></td>
<td>To export metadata for Oracle Identity Cloud Service, click <strong>Download</strong>. Then, import this metadata into the identity provider.</td>
</tr>
<tr>
<td><strong>Provider ID</strong></td>
<td>The Uniform Resource Identifier (URI) that uniquely identifies the identity domain. There’s a one-to-one relationship between the provider ID and the identity provider because the provider ID identifies the identity provider uniquely. Because of this relationship, only one identity provider can be defined in Oracle Identity Cloud Service with a given provider ID.</td>
</tr>
<tr>
<td><strong>Assertion Consumer Service URL</strong></td>
<td>The Uniform Resource Locator (URL) of the service that receives and processes assertions from the identity provider.</td>
</tr>
<tr>
<td><strong>Logout Service Endpoint URL</strong></td>
<td>The URL of the service that receives and processes logout requests from the identity provider.</td>
</tr>
<tr>
<td><strong>Logout Service Return URL</strong></td>
<td>The URL of the service that receives and processes logout responses from the identity provider.</td>
</tr>
<tr>
<td><strong>Service Provider Signing Certificate</strong></td>
<td>To download a signing certificate for the identity provider, click <strong>Download</strong>. Select the file that contains the signing certificate. This certificate is used to verify requests and responses signed by Oracle Identity Cloud Service.</td>
</tr>
<tr>
<td><strong>Service Provider Encryption Certificate</strong></td>
<td>To download an encryption certificate for the identity provider, click <strong>Download</strong>. Select the file that contains the encryption certificate. The identity provider can use this certificate to encrypt the assertion.</td>
</tr>
</tbody>
</table>

To get the issuing Oracle Identity Cloud Service root certificate, see **Obtaining the Root CA Certificate from Oracle Identity Cloud Service**.

7. In the **Test** pane of the wizard, click **Test Login** to test the configuration settings for the identity provider.

8. Click **Next**.

9. In the **Activate** pane of the wizard, click **Activate** to activate the identity provider.

10. Click **Finish**.
Enter Metadata for a SAML Identity Provider

You can use Oracle Identity Cloud Service to enter metadata for a SAML 2.0 identity provider.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Identity Providers**.

2. Click **Add SAML IDP**.

3. Populate the **Details** pane of the **Add Identity Provider** wizard and click **Next**. See **Import Metadata for a SAML Identity Provider**.

4. Use the following table to populate the **Configure** pane of the wizard, and click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enter Identity Provider metadata manually</strong></td>
<td>Click this button because you want to configure SSO for the identity provider by entering metadata for it.</td>
</tr>
<tr>
<td><strong>Issuer ID</strong></td>
<td>Enter the ID of the issuer that's used to register the signing certificate for the identity provider. If you upload new metadata for the identity provider, then the <strong>Issuer ID</strong> field will be updated to reflect the new metadata.</td>
</tr>
<tr>
<td><strong>Signing Certificate</strong></td>
<td>To upload a signing certificate for the identity provider, click <strong>Upload</strong>. Select the file that contains the signing certificate.</td>
</tr>
<tr>
<td><strong>Encryption Certificate</strong></td>
<td>To upload an encryption certificate for the identity provider, click <strong>Upload</strong>. Select the file that contains the encryption certificate.</td>
</tr>
<tr>
<td><strong>SSO Service URL</strong></td>
<td>Enter the URL of the SSO authentication service for the identity provider. With this service, users can access multiple Oracle Cloud services without having to provide authentication credentials more than once.</td>
</tr>
<tr>
<td><strong>SSO Service Binding</strong></td>
<td>This menu contains two options for web-based SSO associated with the identity provider: <strong>Redirect</strong> and <strong>POST</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To send an authentication request with the HTTP-Redirect binding, select <strong>Redirect</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To transmit the response associated with the request using the HTTP-POST binding, select <strong>POST</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Global Logout Activated</strong></td>
<td>To activate SAML global logouts between Oracle Identity Cloud Service and the identity provider, select this check box. Otherwise, leave the check box deselected. If you select the check box, then you must enter values for two URLs for the identity provider: logout request and logout response, and specify whether you want Oracle Identity Cloud Service to initiate a logout with a HTTP-Redirect or HTTP-POST binding.</td>
</tr>
<tr>
<td><strong>Logout Request URL</strong></td>
<td>Enter the URL of the service that receives and processes logout requests from the identity provider.</td>
</tr>
<tr>
<td><strong>Logout Response URL</strong></td>
<td>Enter the URL of the service that receives and processes logout responses from the identity provider.</td>
</tr>
<tr>
<td><strong>Logout Binding</strong></td>
<td>This menu contains two options to initiate a logout: <strong>Redirect</strong> and <strong>POST</strong>. To initiate a logout with the HTTP-Redirect binding, select <strong>Redirect</strong>. To initiate a logout using the HTTP-POST binding, select <strong>POST</strong>.</td>
</tr>
<tr>
<td><strong>Signature Hashing Algorithm</strong></td>
<td>Select the SHA-1 or SHA-256 secure hash algorithm used to encrypt the signing certificate for the identity provider. See <strong>Import Metadata for a SAML Identity Provider</strong>.</td>
</tr>
<tr>
<td><strong>Include Signing Certificate</strong></td>
<td>To include a signing certificate with your identity provider, select this check box. If you don't want to include a signing certificate with your identity provider, then leave the check box deselected.</td>
</tr>
</tbody>
</table>

5. Populate the **Map** pane of the **Add Identity Provider** wizard, and click **Next**. See **Import Metadata for a SAML Identity Provider**.

6. Populate or reference the **Export** pane of the **Add Identity Provider** wizard, and click **Next**. See **Import Metadata for a SAML Identity Provider**.

7. In the **Test** pane of the wizard, click **Test Login** to test the configuration settings for the identity provider.

8. Click **Next**.

9. In the **Activate** pane of the wizard, click **Activate** to activate the identity provider.

10. Click **Finish**.

### Create a SAML Partner and CRL Validation

When adding Oracle Identity Cloud Service as a SAML partner in ADFS, you are required to disable CRL validation or to download SAML 2.0 metadata directly from Oracle Identity Cloud Service.

- **For Releases 17.4.4 and Greater**
For Releases 17.4.4 and Greater

Download and use this metadata to create an Oracle Identity Cloud Service SAML Partner in ADFS that is compatible with the ADFS default security settings.

To download the SAML 2.0 metadata, complete the following steps:

1. Go to https://[instancename.idcs.internal.oracle.com:port]/fed/v1/metadata?adfsmode=true and authenticate (if necessary).
2. Use the web browser Save As feature to save your file.
3. Use the ADFS compatible SAML 2.0 metadata when creating or updating the Oracle Identity Cloud Service partner in ADFS.

Add a Social Identity Provider

Administrators can add a social identity provider so that users can log in to Oracle Identity Cloud Service with their social credentials. Administrators can also allow users to self-register in Oracle Identity Cloud Service if they do not already have an account.

When adding an instance of a social identity provider, you can choose from any of the following predefined social identity provider types:

- Facebook
- Google
- LinkedIn
- Microsoft
- OpenID Connect
- Twitter

You can add an instance of an out-of-the-box social identity provider type by using either the Identity Cloud Service console or SCIM-based APIs. In this section, you learn how to add a social identity provider from a predefined type by using the Identity Cloud Service console. For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

A social identity provider uses an access token to access a resource that’s protected by Oracle Identity Cloud Service. This type of token has an expiration date and time. When the access token expires, a refresh token is used to obtain a renewed access token. Unlike access tokens, refresh tokens never expire.

For some social identity provider types (for example, Adobe e-Sign), separate URLs have to be provided for the access token endpoint and the refresh token endpoint. When this occurs, you must specify different URLs.

For more information about how to customize a social identity provider type, or to learn how to provide different URLs for the access token and refresh token endpoints, see REST API for Oracle Identity Cloud Service.

Some cloud services have applications that may have to connect to multiple instances of the same social identity provider. For example, for application A and application B, the Facebook social identity provider can be configured as an identity provider along with distinct configuration settings, such as a Client ID and Secret, social registration settings, and so on. To support such scenarios, Oracle Identity Cloud Service enables
you to add multiple instances of the same social identity provider with different configuration settings for each instance.

After adding multiple instances of a social identity provider, you can choose which instances can be used to sign in to Oracle Identity Cloud Service by using an identity provider policy.

Prerequisites:
1. Read use cases for social login. To learn about social login and use cases pertaining to it, see Understand Social Login.
2. Create an application for the social identity provider; for example, go to the Google developer site to create a Google application.
3. Configure the redirectUrl in the application created in Step 2. The redirectUrl must have the format: https://<IDCS tenant base URL>/oauth2/v1/social/callback.
   At the time of this printing, each social identity provider calls these URLs by a different name. See the following list of the social identity providers and the names that they use for the URLs.
   • Facebook: Valid OAuth redirect URIs
   • Google and LinkedIn: Authorized redirect URL
   • Microsoft: Redirect URLs
   • Twitter: Callback URL
4. Ensure that you retain the Client ID and the Client Secret from the application that you created at the social identity provider. You use this ID and Secret when configuring a social identity provider in Oracle Identity Cloud Service.

To add a social identity provider:
1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Identity Providers.
2. Click Add Social IDP.
3. Choose a social login type.
4. In the Name and Description fields, enter a name and description for the social identity provider, and then click Next.

Note:
The social identity provider name can contain spaces. However, it can't contain special characters.

5. (Optional) For social login type OpenID Connect, upload an application icon, and then click Next.
6. Enter the Client ID and the Client Secret for the social login type.
7. For the OpenID Connect social login type, enter the Discovery Service URL.
   The discovery service URL is used to get authentication endpoints (URLs) to authenticate users for the social login type.
8. Set the Enable Account Linking option.
• To allow users to link to their social accounts, turn on this option.
• To prevent users from linking to their social accounts, turn off this option.

Note:

You can prevent users from linking to their social accounts for security or organizational purposes. For example, if a hacker accesses the user's social account, the hacker can't sign in to Oracle Identity Cloud Service to access resources and applications that are protected by Oracle Identity Cloud Service. Or, the administrator may want users to have separate profiles for their social accounts and Oracle Identity Cloud Service accounts.

9. Click Finish.

The social identity provider is added, but is deactivated by default. To use this provider, you must activate it.

10. To activate the social identity provider:

   a. Click the Action menu to the right of the provider.
   b. Click Activate.
   c. In the Confirmation window, click OK.

11. (Optional) Set the Enable Registration option so that users can register their social identities with Oracle Identity Cloud Service. To set this option, click the Action menu to the right of the social identity provider, click Edit, and then make one of the following choices:

   • To allow users to register their social identities with Oracle Identity Cloud Service, turn on the Enable Registration option.
   • To prevent users from registering their social identities with Oracle Identity Cloud Service, turn off this option.

Important:

After you add and activate the identity provider, you must add it to an identity provider policy. By doing so, it will appear in the Sign In page and can be used by a user who's trying to sign in to Oracle Identity Cloud Service, either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console. See Add an Identity Provider Policy.

If you no longer want to display the identity provider in the Sign In page, then remove the identity provider from all identity provider policies and deactivate the identity provider. See Remove Identity Providers from the Policy and Deactivate an Identity Provider.

12. Click Save, and then click Close.

13. Log in with the social identity provider.
**View Details About an Identity Provider**

By default, you can see the name of each identity provider you added to Oracle Identity Cloud Service.

You can also see other information about the identity provider, such as its configuration settings.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Identity Providers**.

2. In the **Identity Providers** page, click the **Action** menu to the right of the identity provider about which you want to see more information.

3. Select **Edit**.

**Activate and Deactivate an Identity Provider**

You can use Oracle Identity Cloud Service to activate and deactivate an identity provider.

Deactivating an identity provider prevents users from being able to use the identity provider to access their Oracle Cloud services externally from a different login page than the one associated with their local Oracle Cloud account.

Activating an identity provider reinstates users to use the identity provider.

After you activate an identity provider, you can assign the identity provider to an identity provider policy. An identity provider policy allows you to define criteria that Oracle Identity Cloud Service uses to determine whether the identity provider appears for users on the **Sign In** page, either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console.

See **Understand Identity Provider Policies** for more information about identity provider policies, and **Add an Identity Provider Policy** to learn more about assigning identity providers to an identity provider policy.

**Activate an Identity Provider**

You can use Oracle Identity Cloud Service to activate an identity provider.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Identity Providers**.
2. In the **Identity Providers** page, click the **Action** menu to the right of the identity provider that you want to activate.

3. Select **Activate**.

4. In the **Confirmation** window, click **OK**.

**Deactivate an Identity Provider**

You can use Oracle Identity Cloud Service to deactivate an identity provider.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Identity Providers**.

2. In the **Identity Providers** page, click the **Action** menu to the right of the identity provider that you want to deactivate.

3. Select **Deactivate**.

**Test an Identity Provider**

After adding and activating an identity provider, you can test it. You can verify that you can use your federated SSO credentials to log in to Oracle Identity Cloud Service through an external website.

See **Understand Identity Providers** for more information about the external website.

1. If you assigned the identity provider to an identity provider policy, then go to step 2. Otherwise, assign the identity provider to an identity provider policy. See **Assign Identity Providers to the Policy**.

2. Log out of Oracle Identity Cloud Service.

3. In the **Sign In** page, verify that you see a link called `<Identity_Provider_Name>`.

   The `<Identity_Provider_Name>` placeholder represents the name you entered for the identity provider that you created.

   If, for example, you created an identity provider called Google, then the link appears as **Google**.

   See **Add an Identity Provider**.

4. Click the `<Identity_Provider_Name>` link.

5. Log in to the external website with your federated SSO credentials.

   The identity provider evaluates the user's login credentials, verifies that the user is an authorized user, and returns this information to Oracle Identity Cloud Service. The user can access Oracle Identity Cloud Service.

   **Tip:**

   If you no longer want to display the link to the identity provider in the Sign In page, then remove the identity provider from all identity provider policies and deactivate the identity provider. See **Remove Identity Providers from the Policy** and **Deactivate an Identity Provider**.
Modify an Identity Provider

After viewing details about, activating or deactivating, and testing an identity provider, you can modify it.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Identity Providers.

2. In the Identity Providers page, click the Action menu to the right of the identity provider that you want to modify.

3. Select Edit.

   A window that displays configuration settings for the identity provider opens.

4. Click Edit.

5. Modify a configuration setting for the identity provider:
   a. Enter the value in the attribute field (for example, the Name field).
   b. Select the value from the drop-down menu (for example, the Signature Hashing Algorithm menu).
   c. Remove the value from the field (for example, the Encryption Certificate field).

6. After editing the configuration settings for the identity provider, click Save.

Delete an Identity Provider

You can use Oracle Identity Cloud Service to remove an identity provider.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Identity Providers.

2. In the Identity Providers page, if the identity provider that you want to remove is assigned to an identity provider policy, then remove it from the policy. See Remove Identity Providers from the Policy.

3. Click the Action menu to the right of the identity provider that you want to remove.

4. Select Edit.

   A window that displays configuration settings for the identity provider opens.

5. Click Delete.

   Note:

   Deleting a social identity provider removes the user profiles that are linked to that social identity provider. Alternatively, consider deactivating the social identity provider (which does not remove the user profiles) so that users can still see the accounts in My Profile but can't use them to log in.
6. In the **Confirmation** window, click **OK**.
Manage Oracle Identity Cloud Service
Identity Provider Policies

This section describes how to manage Oracle Identity Cloud Service identity provider policies.

Topics:
- Typical Workflow for Managing Oracle Identity Cloud Service Identity Provider Policies
- Understand Identity Provider Policies
- Add an Identity Provider Policy
- View Details About an Identity Provider Policy
- Modify an Identity Provider Policy
- Remove Identity Provider Policies

Typical Workflow for Managing Oracle Identity Cloud Service Identity Provider Policies

With the identity provider policy feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing identity provider policies.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand identity provider policies.</td>
<td>You can learn about identity provider policies, including how they are used to restrict which identity providers appear in the Sign In page.</td>
<td>Understand Identity Provider Policies</td>
</tr>
<tr>
<td>Add an identity provider policy.</td>
<td>You can add an identity provider policy using the Identity Provider Policies page.</td>
<td>Add an Identity Provider Policy</td>
</tr>
<tr>
<td>View details about an identity provider policy.</td>
<td>You can view details about an identity provider policy using the Identity Provider Policies page.</td>
<td>View Details About an Identity Provider Policy</td>
</tr>
<tr>
<td>Modify an identity provider policy.</td>
<td>You can modify an identity provider policy using the Identity Provider Policies page.</td>
<td>Modify an Identity Provider Policy</td>
</tr>
<tr>
<td>Remove identity provider policies.</td>
<td>You can remove identity provider policies using the Identity Provider Policies page.</td>
<td>Remove Identity Provider Policies</td>
</tr>
</tbody>
</table>
You can create, manage, and remove identity provider policies by:

- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage identity provider policies by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Identity Provider Policies

An identity provider policy allows identity domain administrators, security administrators, and application administrators to define which identity providers are visible in the Sign In page either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service.

Oracle Identity Cloud Service also uses identity provider policies to determine whether users authenticate into Oracle Identity Cloud Service through identity providers or with their local credentials.

There are three types of identity providers available with Oracle Identity Cloud Service:

- SAML identity provider: This type of identity provider supports the SAML 2.0 (Security Assertion Markup Language 2.0) standard. You use a SAML identity provider when you want to establish trust between an SAML-compatible identity provider such as Active Directory Federation Services so that users in your organization can access resources protected by Oracle Identity Cloud Service.

  If you want your users to be redirected to a specific SAML identity provider automatically so that they can access an app, then ensure that the identity provider policy associated with the app has only the SAML identity provider assigned to it. If multiple identity providers are assigned to the identity provider policy, then users will be prompted to select one of the identity providers from the Sign In page.

- Social identity provider: By linking an Oracle Identity Cloud Service user account to a user's social accounts, the user can access Oracle Identity Cloud Service using their social credentials, such as Facebook, Google, LinkedIn, Microsoft, and Twitter.

- Local identity provider (Local IDP): Authentication into Oracle Identity Cloud Service happens locally by the user providing their credentials (user name and password) in the Sign In page.

The identity provider policy allows you to configure whether local authentication will be displayed in the Sign In page for the user.

Suppose you've created several social identity providers and SAML identity providers, and you want to configure which of these identity providers will appear in the Sign In page when the user attempts to authenticate into Oracle Identity Cloud Service using a particular app. Without identity provider policies, you couldn't configure this. So, if you had all of these SAML and social identity providers activated and set to appear in the Sign In page, they would all be displayed.

Oracle Identity Cloud Service provides you with a default identity provider policy that has a local identity provider (Local IDP) assigned to it. This way, at the bare minimum, users can authenticate into Oracle Identity Cloud Service with their user names and
passwords. However, you can build upon this default policy by assigning other identity providers to it. Both the My Profile console and the Identity Cloud Service console use the identity providers that are assigned to the default identity provider policy.

In addition to the default identity provider policy, you can create identity provider policies and associate them with specific apps. Suppose you have multiple apps and you want to assign different identity providers to each app. For example, you may have two apps, and you want users to authenticate into Oracle Identity Cloud Service from Facebook or Linkedin. So, you can have one identity provider policy specifically for one app and the Facebook social identity provider, and another identity provider policy exclusively for the second app and the Linkedin social identity provider.

Oracle Identity Cloud Service displays a maximum of four identity providers on the Sign In page. If you assign more than four identity providers to an identity provider policy, then a View all link appears on the page. Click the link and all identity providers associated with the policy appear.

Add an Identity Provider Policy

Oracle Identity Cloud Service provides you with a wizard to add an identity provider policy. As a result, you define criteria that Oracle Identity Cloud Service uses to determine which identity providers appear for users on the Sign In page when they are accessing particular apps.

This wizard contains three panes:

- **Details**: Provide the name and description for the policy.
- **Identity Providers**: Assign or remove identity providers for this policy.
- **Apps**: Assign or remove apps for this policy.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click IDP Policies. The Identity Provider Policies page appears.

   **Tip:**

   In the Identity Provider Policies page, Oracle Identity Cloud Service provides you with a default identity provider policy. See Understand Identity Provider Policies for more information about this policy.

2. Click Add. The Add Identity Provider Policy wizard appears.

3. In the Details pane of the wizard, enter the name of the policy in the Policy Name field. Then, click Next.

   After providing information in the Details pane and clicking Next, Oracle Identity Cloud Service adds the identity provider policy.

   You may want to assign or remove identity providers or apps for this policy. To do this, the wizard has the Identity Providers and Apps panes.

4. In the Identity Providers pane of the wizard, click Assign to assign identity providers to this policy.
5. In the **Assign Identity Providers** window, select the check box for each identity provider that you want to assign to the policy. Then, click **OK**.

**Note:**
You may have added incorrect identity providers to this policy inadvertently. If so, then you can remove them. To do so, select the check box for each identity provider that you want to remove, click **Remove**, and then click **OK** from the confirmation window.

6. In the **Identity Providers** pane, click **Next**.
7. In the **Apps** pane of the wizard, click **Assign** to assign apps to this policy.
8. In the **Assign Apps** window, select the check box for each app that you want to assign to the policy. Then, click **OK**.

**Note:**
You can remove apps from the policy by selecting the check box for each app that you want to remove, clicking **Remove**, and then clicking **OK** from the confirmation window.

9. Click **Finish**.

### View Details About an Identity Provider Policy

By default, you can see the name of each identity provider policy you added to Oracle Identity Cloud Service. You can also see other information about the policy, such as the identity providers and apps assigned to the policy.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **IDP Policies**.
2. In the **Identity Provider Policies** page, click the identity provider policy about which you want to see more information. The policy opens and displays three tabs: **Details**, **Identity Providers**, and **Apps**.
3. To view high-level information about the identity provider policy, such as the policy name, click **Details**.
4. To view identity providers or apps assigned to the policy, click **Identity Providers** or **Apps**, respectively.

### Modify an Identity Provider Policy

After viewing details about an identity provider policy, you can modify it. Modifying an identity provider policy in Oracle Identity Cloud Service includes:

- Changing the name of the policy
- Assigning identity providers and apps to the policy
- Removing identity providers and apps from the policy
To modify an identity provider policy:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click IDP Policies.

2. In the Identity Provider Policies page, click the identity provider policy that you want to modify.

The policy opens and displays three tabs: Details, Identity Providers, and Apps. See View Details About an Identity Provider Policy for more information about these tabs.

**Change the Policy Name**

You can change the name of an identity provider policy.

1. Click the Details tab.

2. In the Policy Name field, enter the new name of the identity provider policy.

3. Click Save.

**Assign Identity Providers to the Policy**

You can assign identity providers to an identity provider policy. These identity providers will appear in the Sign In page, and a user can use them to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console.

1. Click the Identity Providers tab.

2. Click Assign.

3. In the Assign Identity Providers window, select the check box for each identity provider that you want to assign to the policy. Then, click OK.

**Remove Identity Providers from the Policy**

You can remove identity providers from an identity provider policy. These identity providers will no longer appear in the Sign In page, and a user can't use them to access Oracle Identity Cloud Service-protected resources, such as the My Profile console or the Identity Cloud Service console.

1. Click the Identity Providers tab.

2. Select the check box for each identity provider that you want to remove from the policy.

3. Click Remove.

4. In the Confirmation window, click OK.

**Assign Apps to the Policy**

You can assign apps to an identity provider policy. When a user attempts to authenticate into Oracle Identity Cloud Service through the apps, the only identity providers that appear in the Sign In page are the ones you assigned to the policy.

1. Click the Apps tab.
2. Click **Assign**.
3. In the **Assign Apps** window, select the check box for each app that you want to assign to the policy. Then, click **OK**.

### Remove Apps from the Policy

You can remove apps from an identity provider policy. A user who uses these apps can no longer authenticate into Oracle Identity Cloud Service by using the identity providers assigned to the policy.

1. Click the **Apps** tab.
2. Select the check box for each app that you want to remove from the policy.
3. Click **Remove**.
4. In the **Confirmation** window, click **OK**.

### Remove Identity Provider Policies

You can use Oracle Identity Cloud Service to remove multiple identity provider policies simultaneously.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **IDP Policies**.
2. In the **Identity Provider Policies** page, if the policy that you want to remove has apps assigned to it, then remove the apps from the policy. See **Remove Apps from the Policy**.
3. Select the check box for each identity provider policy that you want to remove.
4. Click **Remove**.
5. In the **Confirmation** window, click **OK**.
Manage Oracle Identity Cloud Service Sign-On Policies

This section describes how to manage Oracle Identity Cloud Service sign-on policies.

Topics:

- Typical Workflow for Managing Oracle Identity Cloud Service Sign-On Policies
- Understand Sign-On Policies
- Add a Sign-On Policy
- View Details About a Sign-On Policy
- Activate and Deactivate Sign-On Policies
- Modify a Sign-On Policy
- Remove Sign-On Policies

Typical Workflow for Managing Oracle Identity Cloud Service Sign-On Policies

With the sign-on policy feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing sign-on policies.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand sign-on policies.</td>
<td>You can learn about sign-on policies, including how they are used to allow or deny access to Oracle Identity Cloud Service for users.</td>
<td>Understand Sign-On Policies</td>
</tr>
<tr>
<td>Add a sign-on policy.</td>
<td>You can add a sign-on policy using the Sign-On Policies page.</td>
<td>Add a Sign-On Policy</td>
</tr>
<tr>
<td>View details about a sign-on policy.</td>
<td>You can view details about a sign-on policy using the Sign-On Policies page.</td>
<td>View Details About a Sign-On Policy</td>
</tr>
<tr>
<td>Modify a sign-on policy.</td>
<td>You can modify a sign-on policy using the Sign-On Policies page.</td>
<td>Modify a Sign-On Policy</td>
</tr>
</tbody>
</table>
You can create, manage, and remove sign-on policies by:

- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage sign-on policies by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Sign-On Policies

A sign-on policy allows identity domain administrators, security administrators, and application administrators to define criteria that Oracle Identity Cloud Service uses to determine whether to allow a user to sign in to Oracle Identity Cloud Service or prevent a user from accessing Oracle Identity Cloud Service.

Oracle Identity Cloud Service provides you with a default sign-on policy that contains a default sign-on rule. Oracle Identity Cloud Service evaluates the criteria of the rule for any user attempting to sign in to Oracle Identity Cloud Service. By default, this rule allows all users to sign in to Oracle Identity Cloud Service. This means whichever authentication the user uses, either local authentication, by supplying a user name and password, or authentication by using an external identity provider, will be sufficient. However, you can build upon this policy by adding other sign-on rules to it. By adding these rules, you can prevent some of your users from signing in to Oracle Identity Cloud Service. Or, you can allow them to sign in, but prompt them for an additional factor to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console.

For example, you can create two sign-on rules for the default sign-on policy. The first rule prevents any users from signing in to Oracle Identity Cloud Service if they’re using an IP address that falls within the range of a network perimeter that you defined. The second rule allows users who belong to a particular group (for example, the UA_Developers group) to sign in to Oracle Identity Cloud Service; however, they will be prompted for a second factor as part of the 2-Step Verification process. All other users will be able to sign in without being prompted for a second factor.

Because you can define multiple sign-on rules for a sign-on policy, Oracle Identity Cloud Service must know the order in which the rules are to be evaluated. To do this, you can set the priority of the rules. For the example above, you can have the network perimeter sign-on rule evaluated first, and the UA_Developers group rule evaluated next. If a user meets the criteria of the network perimeter sign-on rule (that is, the IP address used to attempt to sign in to Oracle Identity Cloud Service falls within the IP range that you defined in the network perimeter), the user is prevented from accessing Oracle Identity Cloud Service-protected resources. Users who attempt to sign in to Oracle Identity Cloud Service from IP addresses that don’t fall within this range don’t meet the criteria of this sign-on rule, and so, the rule with the next highest priority is evaluated. For this example, this is the UA_Developers group rule. Any users who attempt to sign in, and who also belong to the UA_Developers group, will be prompted for an additional factor to sign in to Oracle Identity Cloud Service. Users who aren’t members of the UA_Developers group don’t meet the criteria of this rule, and so, the rule with the next highest priority is evaluated. For this example, this is the default sign-on rule. Because, this rule, by default, allows all users to sign in to Oracle Identity Cloud Service, the user will be able to sign in without being prompted for a second factor.
Important:

For the default sign-on rule, never set access for all of your users to be denied because if users don’t meet the criteria of any other rules you define that allow them to sign in to Oracle Identity Cloud Service, they will be prevented from accessing Oracle Identity Cloud Service-protected resources. Also, configure Oracle Identity Cloud Service to evaluate this sign-on rule last because, by default, it allows all users to sign in to Oracle Identity Cloud Service.

In addition to the default sign-on policy, you can create sign-on policies and associate them with specific apps. When a user uses one of these apps to attempt to sign in to Oracle Identity Cloud Service, Oracle Identity Cloud Service checks to see if the app has any sign-on policies associated with it. If so, then Oracle Identity Cloud Service evaluates the criteria of the sign-on rules assigned to the policy. If there are no sign-on policies for the app, then the default sign-on policy is evaluated by Oracle Identity Cloud Service.

Add a Sign-On Policy

Oracle Identity Cloud Service provides you with a wizard to add a sign-on policy. As a result, you define criteria that Oracle Identity Cloud Service uses to determine whether to allow or deny access to users who are using apps to attempt to sign in to Oracle Identity Cloud Service.

Criteria that you can define for sign-on policies include:

• The identity providers that will be used to authenticate the user
• The groups of which the user is a member
• Whether the user is an Oracle Identity Cloud Service administrator
• The IP address that the user is using to sign in to Oracle Identity Cloud Service
• Whether the user will be forced to sign in to Oracle Identity Cloud Service again (for authentication purposes), or will be authenticated the next time they sign in to Oracle Identity Cloud Service
• Whether the user will be prompted for an additional factor to sign in to Oracle Identity Cloud Service

The sign-on policy wizard contains three panes:

• **Details**: Provide the name and description for the policy.
• **Sign-On Rules**: Assign or remove rules for this policy.
• **Apps**: Assign or remove apps for this policy.

**Tip:**

In the Sign-On Policies page, Oracle Identity Cloud Service provides you with a default sign-on policy. See Understand Sign-On Policies for more information about this policy.

2. Click **Add**. The **Add Sign-On Policy** wizard appears.

3. Use the following table to populate the **Details** pane of the wizard, and then click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Enter the name of the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter explanatory information about the policy.</td>
</tr>
</tbody>
</table>

After providing information in the **Details** pane and clicking **Next**, Oracle Identity Cloud Service adds the sign-on policy and saves it in a deactivated state. See Activate Sign-On Policies to activate the policy.

You may want to assign or remove rules or apps for this policy. To do this, the wizard has the **Sign-On Rules** and **Apps** panes.

4. In the **Sign-On Rules** pane of the wizard, click **Add** to add a sign-on rule to this policy.

5. Use the following table to populate the **Add Rule** window, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter the name of the sign-on rule.</td>
</tr>
<tr>
<td>If the user is authenticated by</td>
<td>Enter or select all identity providers that will be used to authenticate the user accounts evaluated by this rule.</td>
</tr>
<tr>
<td>And is a member of these groups</td>
<td>Enter or select the groups that the user must be a member of to meet the criteria of this rule.</td>
</tr>
<tr>
<td>And is an administrator</td>
<td>If the user must be assigned to administrator roles in Oracle Identity Cloud Service to meet the criteria of this rule, then select this check box. See Add or Remove a User Account from an Administrator Role. Otherwise, leave the check box deselected.</td>
</tr>
<tr>
<td>And is not one of these users</td>
<td>Enter or select the user accounts that will be excluded from the rule.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
And the user's client IP address is | There are two options associated with this field: **Anywhere** and **In one or more of these network perimeters**.
- If you select **Anywhere**, then users can log in to Oracle Identity Cloud Service using any IP address.
- If you select **In one or more of these network perimeters**, then a text area appears. In this text area, you can enter or select network perimeters that you defined in Oracle Identity Cloud Service. See Add a Network Perimeter. Users can log in to Oracle Identity Cloud Service using only IP addresses that are contained in the defined network perimeters.

Access is | There are two items in this menu: **Allowed** and **Denied**. Select whether a user will be allowed or prevented from accessing the apps that are assigned to them if the user account meets the criteria of this rule.

Prompt for reauthentication | Select this check box to force the user to log in to Oracle Identity Cloud Service again. By not selecting this check box, the user will be authenticated the next time they log in to Oracle Identity Cloud Service.

If you have activated Adaptive Security, then additional fields appear in the Add Rule window. You can use these fields to specify conditions that Oracle Identity Cloud Service will evaluate to determine whether a user who meets these conditions will be allowed to sign in to Oracle Identity Cloud Service or will be prevented from accessing Oracle Identity Cloud Service.

For example, you can specify that if a user's risk range is High and the risk score associated with the user from a risk provider is greater than a particular value, then the user is a security risk, and shouldn't be allowed to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console, the Identity Cloud Service console, or any apps assigned to the user.

Or, you can determine that if a user's risk range is Low, based on the risk score associated with a risk provider, then the user is not a risk, and therefore, should be able to sign in to Oracle Identity Cloud Service.

See **Activate Adaptive Security** for more information about activating Adaptive Security, and **Understand Risk Providers** to learn more about risk ranges, risk providers, and risk scores associated with users.

Field | Description
--- | ---
And if the user's risk level is | Select whether the user's risk range must be greater than, equal to, or less than a Low, Medium, or High risk range to meet the criteria of this rule.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>And the risk provider name</td>
<td>Select the risk provider and the risk score that will be used to determine whether a user who meets the criteria of this rule will be allowed to sign in to Oracle Identity Cloud Service or will be prevented from accessing Oracle Identity Cloud Service. Click the <strong>Plus</strong> button + to add another risk provider to the <strong>Add Rule</strong> window or the <strong>X</strong> button × to remove the risk provider from this window.</td>
</tr>
</tbody>
</table>

**Important:**

Be careful when setting Adaptive Security conditions. For example, suppose you specify that a user who meets the criteria of this rule because their risk score meets or exceeds the risk score that you set is prevented from accessing Oracle Identity Cloud Service. Unless the user changes their password or Oracle Identity Cloud Service runs the **Time-based risk-score re-evaluation** event to lower the user's risk score, the user can't sign in to Oracle Identity Cloud Service.

If you have selected at least one factor for Multi-Factor Authentication, then additional fields appear in the **Add Rule** window. See **Configure Multi-Factor Authentication Settings**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt for an additional factor</td>
<td>Select this check box to prompt the user for an additional factor to log in to Oracle Identity Cloud Service. If you select this check box, then you must specify whether the user is required to enroll in Multi-Factor Authentication and how often this additional factor is to be used to log in to Oracle Identity Cloud Service. By not selecting this check box, the user can log in to Oracle Identity Cloud Service using their user name and password only.</td>
</tr>
</tbody>
</table>

**Important:**

If you choose to secure an application with MFA by selecting this check box, then you must also select this check box for the default sign-on policy. You must complete this action to secure MFA self-service operations.
## Field	Description

**Enrollment**

This menu contains two options: Required and Optional.

- Select Required to force the user to enroll in Multi-Factor Authentication.
- Select Optional to give users the option of skipping enrolling in Multi-Factor Authentication. Users see the inline enrollment setup process after they enter their user name and password, but can click Skip. Users can then enable MFA later from the 2-Step Verification tab of the My Profile console. Users are not prompted to set up a factor the next time that they sign in to Oracle Identity Cloud Service.

**Frequency of an additional factor when using a trusted device**

There are three options associated with this field: Once per Session (Default), Every time, and Once every.

- If you select Once per Session (Default), then for each session that the user has opened for accessing Oracle Identity Cloud Service from an authoritative device, they must use both their user names and passwords, and a second factor.
- If you select Every time, then each time users log in to Oracle Identity Cloud Service from a trusted device, they must use their user names and passwords, and a second factor.
- If you select Once every, then you must specify how often users must provide a second factor to log in to Oracle Identity Cloud Service. For example, if you want users to use this additional factor twice a month, then enter 15 in the text field and select Days from the drop-down menu to the right of the field.

---

**Note:**

You may have added incorrect sign-on rules to this policy inadvertently. If so, then you can remove them. To do so, select the check boxes for each of the rules that you want to remove, click Remove, and then click OK from the confirmation window.

6. In the Sign-On Rules pane, click Add to add another sign-on rule to this policy. Otherwise, click Next.
Note:
If you have added multiple sign-on rules to this policy, then you can change the order that will Oracle Identity Cloud Service evaluate them. See Change the Priority of a Sign-On Rule for the Policy.

7. In the Apps pane of the wizard, click Assign to assign apps to this policy.
8. In the Assign Apps window, select the check box for each app that you want to assign to the policy. Then, click OK.

Note:
You can assign only one sign-on policy to an app. If the app isn't assigned to any sign-on policy explicitly, then the default sign-on policy applies to the app.
You can remove apps from the policy by selecting the check box for each app that you want to remove, clicking Remove, and then clicking OK from the confirmation window.

9. Click Finish.

View Details About a Sign-On Policy

By default, you can see the name, description, and activation status of each sign-on policy you added to Oracle Identity Cloud Service. You can also see other information about the policy, such as the rules added to the policy and any apps assigned to the policy.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Sign-On Policies.
2. In the Sign-On Policies page, click the sign-on policy about which you want to see more information.
   The policy opens and displays three tabs: Details, Sign-On Rules, and Apps.
3. To view high-level information about the sign-on policy, such as the policy name or description, click Details.
4. To view sign-on rules added to the policy or apps assigned to the policy, click Sign-On Rules or Apps, respectively.

Note:
For more information about changing high-level information about the sign-on policy, or the rules or apps associated with the policy, see Modify a Sign-On Policy.
Activate and Deactivate Sign-On Policies

You can use Oracle Identity Cloud Service to activate and deactivate sign-on policies.

- Deactivating a sign-on policy prevents Oracle Identity Cloud Service from using the criteria in the policy to allow or deny access to users who are attempting to sign in to Oracle Identity Cloud Service.
- Activating a sign-on policy allows Oracle Identity Cloud Service to evaluate the criteria in the policy to determine whether to allow or deny users from accessing Oracle Identity Cloud Service-protected resources.

**Note:**

A green check mark ✅ indicates an activated sign-on policy. A red circle ❌ with a white line through the circle ❌ indicates a deactivated sign-on policy.

Activate Sign-On Policies

You can use Oracle Identity Cloud Service to activate sign-on policies.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Sign-On Policies.
2. In the Sign-On Policies page, select the check box for each sign-on policy that you want to activate.
3. Click Activate.
4. In the Confirmation window, click OK. The status of each sign-on policy changes from deactivated ❌ to activated ✅.

Deactivate Sign-On Policies

You can use Oracle Identity Cloud Service to deactivate sign-on policies.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Sign-On Policies.
2. In the Sign-On Policies page, select the check box for each sign-on policy that you want to deactivate.
3. Click Deactivate.
4. In the Confirmation window, click OK. The status of each sign-on policy changes from activated ✅ to deactivated ❌.
Modify a Sign-On Policy

After viewing details about, activating, or deactivating a sign-on policy, you can modify it. Modifying a sign-on policy in Oracle Identity Cloud Service includes:

- Changing the name or description of the policy
- Adding, editing, changing the priority of, and removing sign-on rules for the policy
- Assigning apps to the policy
- Removing apps from the policy

To modify a sign-on policy:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Sign-On Policies.
2. In the Sign-On Policies page, click the sign-on policy that you want to modify.

The policy opens and displays three tabs: Details, Sign-On Rules, and Apps. See View Details About a Sign-On Policy for more information about these tabs.

Change the Policy Name and Description

You can change the name and description for a sign-on policy.

1. Click the Details tab.
2. In the Policy Name and Description fields, enter the new name and description for the sign-on policy.
3. Click Save.

Add Sign-On Rules to the Policy

You can add sign-on rules to a sign-on policy. By adding these rules, you can prevent some of your users from signing in to Oracle Identity Cloud Service. Or, you can allow them to sign in, but prompt them for an additional factor to access resources that are protected by Oracle Identity Cloud Service, such as the My Profile console or the Identity Cloud Service console.

1. Click the Sign-On Rules tab.
2. Click Add.
3. Add sign-on rules to the policy. See Add a Sign-On Policy.

Change the Priority of a Sign-On Rule for the Policy

You can change the priority of a sign-on rule for a sign-on policy to change the order that Oracle Identity Cloud Service will evaluate it.

1. Click the Sign-On Rules tab.
2. Click the ellipsis button to the left of the sign-on rule for which you want to change the priority.
3. Drag-and-drop this rule to change the order that Oracle Identity Cloud Service will evaluate it.

   For example, if your sign-on rule has a priority of 4, and you want Oracle Identity Cloud Service to evaluate it first, drag the rule and drop it so that it appears directly above the sign-on rule with a priority of 1. Your sign-on rule will appear first in the list, and the other rule will now have a priority of 2.

4. Click Save.

Edit a Sign-On Rule for the Policy

   You can modify configuration settings for a sign-on rule of a sign-on policy.

1. Click the Sign-On Rules tab.

2. Click the Action menu to the right of the sign-on rule that you want to edit.

3. Select Edit. A window that displays configuration settings for the sign-on rule opens.

4. Modify a configuration setting for the sign-on rule:

   a. Enter the value in the attribute field (for example, changing the name of the sign-on rule in the Rule Name field).

   b. Select the value from the drop-down menu (for example, selecting Allowed from the Access is menu).

   c. Select or clear a check box or option (for example, selecting the Prompt for reauthentication check box or the Anywhere option).

   d. Remove the value from the field (for example, removing a group that appears in the And is a member of these groups field by clicking the X button to the right of the group name).

5. After editing the sign-on rule, click Save.

Remove Sign-On Rules from the Policy

   You can remove sign-on rules from a sign-on policy. Oracle Identity Cloud Service will no longer evaluate the criteria in the rules to determine whether to allow a user to sign in to Oracle Identity Cloud Service or prevent a user from accessing Oracle Identity Cloud Service-protected resources.

1. Click the Sign-On Rules tab.

2. Select the check box for each sign-on rule that you want to remove from the policy.

3. Click Remove.

4. In the Confirmation window, click OK.

Assign Apps to the Policy

   You can assign apps to a sign-on policy. When a user uses one of these apps to attempt to sign in Oracle Identity Cloud Service, Oracle Identity Cloud Service evaluates the criteria of the sign-on rules that are also assigned to the policy to
determine whether to allow or deny the user from accessing resources that are
protected by Oracle Identity Cloud Service.

1. Click the Apps tab.
2. Click Assign.
3. In the Assign Apps window, select the check box for each app that you want to
   assign to the policy. Then, click OK.

Remove Apps from the Policy

You can remove apps from a sign-on policy. Oracle Identity Cloud Service will no
longer evaluate the criteria of the sign-on rules assigned to the policy to determine
whether to allow or deny the user from signing in to Oracle Identity Cloud Service from
one of these apps.

1. Click the Apps tab.
2. Select the check box for each app that you want to remove from the policy.
3. Click Remove.
4. In the Confirmation window, click OK.

Remove Sign-On Policies

You can use Oracle Identity Cloud Service to remove multiple sign-on policies
simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click
   Security, and then click Sign-On Policies.
2. In the Sign-On Policies page, if the policy that you want to remove has apps
   assigned to it, then remove the apps from the policy. See Remove Apps from the
   Policy.
3. Select the check box for each sign-on policy that you want to remove.
4. Click Remove.
5. In the Confirmation window, click OK.
Manage Oracle Identity Cloud Service Network Perimeters

This section describes how to manage Oracle Identity Cloud Service network perimeters.

Topics:
- Typical Workflow for Managing Oracle Identity Cloud Service Network Perimeters
- Understand Network Perimeters
- Add a Network Perimeter
- View Details About a Network Perimeter
- Modify a Network Perimeter
- Remove Network Perimeters

Typical Workflow for Managing Oracle Identity Cloud Service Network Perimeters

With the network perimeter management feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing network perimeters.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand network perimeters.</td>
<td>You can learn about network perimeters, including how they are used to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service.</td>
<td>Understand Network Perimeters</td>
</tr>
<tr>
<td>Add a network perimeter.</td>
<td>You can add a network perimeter using the Network Perimeters page.</td>
<td>Add a Network Perimeter</td>
</tr>
<tr>
<td>View details about a network perimeter.</td>
<td>You can view details about a network perimeter using the Network Perimeters page.</td>
<td>View Details About a Network Perimeter</td>
</tr>
<tr>
<td>Modify a network perimeter.</td>
<td>You can modify a network perimeter using the Network Perimeters page.</td>
<td>Modify a Network Perimeter</td>
</tr>
<tr>
<td>Remove network perimeters.</td>
<td>You can remove network perimeters using the Network Perimeters page.</td>
<td>Remove Network Perimeters</td>
</tr>
</tbody>
</table>

You can create, manage, and remove network perimeters by:
- The Identity Cloud Service console
• SCIM-based APIs

The following sections describe how to manage network perimeters by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Network Perimeters

For security purposes, identity domain administrators, security administrators, and application administrators can define network perimeters in Oracle Identity Cloud Service. A network perimeter contains a list of IP addresses.

After creating a network perimeter, you can prevent users from signing in to Oracle Identity Cloud Service if they use one of the IP addresses in the network perimeter. This is known as blacklisting. A blacklist contains IP addresses or domains that are suspicious. As an example, a user may be trying to sign in to Oracle Identity Cloud Service with an IP address that comes from a country where hacking is rampant.

An IP address is a string of numbers that identifies the network of any device connected to the internet. It's like a return address on an envelope, and is associated with a human-readable domain. Since the IP address tells other devices where data is coming from, it can be a good way to track bad content.

Blacklists can list a single IP address or a (set) range of IPs. Oracle Identity Cloud Service can use this information to block users who attempt to sign in from suspicious IP addresses.

You can also configure Oracle Identity Cloud Service so that users can log in, using only IP addresses contained in the network perimeter. This is known as whitelisting, where users who attempt to sign in to Oracle Identity Cloud Service with these IP addresses will be accepted. Whitelisting is the reverse of blacklisting, the practice of identifying IP addresses that are suspicious, and as a result, will be denied access to Oracle Identity Cloud Service.

You can configure Oracle Identity Cloud Service so that only users who use a particular IP address or IP address in a specific range will be allowed to sign in to Oracle Identity Cloud Service. Or, you can configure Oracle Identity Cloud Service to monitor for suspicious IP addresses or IP address ranges, and prevent users who use these IP addresses from signing in to Oracle Identity Cloud Service.

With a network perimeter, you can define, in a standard format, an exact IP address, a range of IP addresses, or a set of masked IP addresses. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) protocols are supported.

Detailed information about these three formats appears below.

• Exact IP address. You can enter a single IP address or multiple IP addresses. If you enter multiple exact IP addresses, then put a comma between each one.

• Two IP addresses, separated by a hyphen, which is an IP range. For example, if you specify the IP range of 10.10.10.1-10.10.10.10, any user who attempts to sign in to Oracle Identity Cloud Service with an IP address from 10.10.10.1 through 10.10.10.10 will be using an IP address that falls within the IP range.

• Masked IP address range. Each number of an IP address is 8 bits. For example, if you have a masked range of 10.11.12.18/24, then the first three numbers (24
bits) is the mask that must be applied to see if an IP address falls in this range. For this example, valid IP addresses will be those that begin with 10.11.12.

Note:
The examples listed above are using IP addresses with the IPv4 protocol. However, you can apply the same formats to IP addresses that use the IPv6 protocol (for example, B138:C14:52:8000:0:0:4D8).

After defining your network perimeters, you can assign them to a sign-on policy, and configure the policy so that if you're trying to sign in to Oracle Identity Cloud Service using an IP address that's defined in the network perimeter, you can log in to Oracle Identity Cloud Service or you'll be prevented from accessing Oracle Identity Cloud Service.

See Add a Sign-On Policy for more information about assigning network perimeters to a sign-on policy.

Add a Network Perimeter

You can add a network perimeter in Oracle Identity Cloud Service, and then configure Oracle Identity Cloud Service to restrict the IP addresses that users can use to log in to Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Network Perimeters.
2. In the Network Perimeters page, click Add. The Add Network Perimeter window appears.
3. Use the following table to populate the Add Network Perimeter window, and then click Save:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Perimeter Name</td>
<td>Enter the name of the network perimeter.</td>
</tr>
<tr>
<td>List of IP Addresses</td>
<td>Enter the exact IP address or IP addresses, IP range, or masked IP address range for the network perimeter. See Understand Network Perimeters for more information about these IP address formats.</td>
</tr>
</tbody>
</table>

You added a network perimeter. See Add a Sign-On Policy for more information about using this network perimeter in sign-on policy rules.

View Details About a Network Perimeter

By default, you can see the name of each network perimeter you defined in Oracle Identity Cloud Service. You can also see other information about the policy, such as the IP addresses for the network perimeter.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Network Perimeters.
2. In the **Network Perimeters** page, click the **Action** menu to the right of the network perimeter about which you want to see more information, and then click **Edit**.

A window opens and displays the name and IP addresses associated with the network perimeter. From this window, you can modify this information. See **Modify a Network Perimeter**.

### Modify a Network Perimeter

After viewing details about a network perimeter, you can modify it. Modifying a network perimeter in Oracle Identity Cloud Service includes changing the name of the network perimeter or the IP addresses associated with the network perimeter.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Network Perimeters**.

2. In the **Network Perimeters** page, click the **Action** menu to the right of the network perimeter about which you want to modify, and then click **Edit**.

A window opens and displays the name and IP addresses associated with the network perimeter.

3. In the **Network Perimeter Name** field, enter the new name of the network perimeter.

4. In the **List of IP Addresses** text area, modify the IP addresses associated with the network perimeter by adding, editing, or removing IP addresses for the network perimeter. If you enter multiple new IP addresses, then put a comma between each one.

5. Click **Save**.

### Remove Network Perimeters

You can use Oracle Identity Cloud Service to remove multiple network perimeters simultaneously.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Network Perimeters**.

2. In the **Network Perimeters** page, select the check box for each network perimeter that you want to remove.

3. Click **Remove**.

4. In the **Confirmation** window, click **OK**.
Manage Oracle Identity Cloud Service App Gateways

This section describes how to manage Oracle Identity Cloud Service App Gateways.

Topics:

• Typical Workflow for Managing Oracle Identity Cloud Service App Gateways
• What is App Gateway?
• Register an App Gateway
• View Details About an App Gateway
• Activate and Deactivate App Gateways
• Modify an App Gateway
• Remove App Gateways

Typical Workflow for Managing Oracle Identity Cloud Service App Gateways

With the App Gateways feature in Oracle Identity Cloud Service, you can perform tasks such as creating, managing, and removing App Gateways.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is App Gateway</td>
<td>You learn what an App Gateway is.</td>
<td>What is App Gateway?</td>
</tr>
<tr>
<td>Add an App Gateway</td>
<td>You learn how to register an App Gateway in Oracle Identity Cloud Service before you install and configure the App Gateway software.</td>
<td>Register an App Gateway</td>
</tr>
<tr>
<td>View Details About an App Gateway</td>
<td>You can view details about an App Gateway using the App Gateways page.</td>
<td>View Details About an App Gateway</td>
</tr>
<tr>
<td>Activate and Deactivate App Gateways</td>
<td>You can activate and deactivate App Gateways using the App Gateways page.</td>
<td>Activate and Deactivate App Gateways</td>
</tr>
<tr>
<td>Modify an App Gateway</td>
<td>You can modify an App Gateway using the App Gateways page.</td>
<td>Modify an App Gateway</td>
</tr>
<tr>
<td>Remove App Gateways</td>
<td>You can remove App Gateways using the App Gateways page.</td>
<td>Remove App Gateways</td>
</tr>
</tbody>
</table>
You can create, manage, and remove App Gateways by:

- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage App Gateways by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

What is App Gateway?

App Gateway is a software appliance that enables you to integrate applications hosted either on a compute instance, in a cloud infrastructure, or in an on-premises server with Oracle Identity Cloud Service for authentication purposes.

App Gateway acts as a reverse proxy protecting web applications by restricting unauthorized network access to them. App Gateway intercepts any HTTP request to these applications and ensures that the users are authenticated with Oracle Identity Cloud Service before forwarding the request to these application. App Gateway propagates the authenticated user's identity to the applications.

If the user isn't authenticated with Oracle Identity Cloud Service, then App Gateway redirects the user to Oracle Identity Cloud Service's Sign In page for credential validation.

Register an App Gateway

Before installing the binary file for App Gateway that appears on the Downloads page, you must register your App Gateway using Identity Cloud Service console.

To register an App Gateway you must add hosts and associate each host to an enterprise application your App Gateway will protect:

- In the Hosts pane, you define host identifiers. Each host identifier represents a domain name and port number App Gateway uses to proxy an enterprise application.
- In the Apps pane, you associate an enterprise application with a host identifier.

To register an App Gateway, you must be assigned to either the Identity Domain Administrator role or the Security Administrator role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, click App Gateways, and then click Add.
2. In the Details pane, specify the name of your App Gateway, and then click Next (>).
3. In the Hosts pane, click Add.
4. In the Add Host dialog, provide a name in the Host Identifier field.
5. Enter the Host and Port values that the App Gateway server will respond to HTTP requests.

The port number you provide in this step is used by the App Gateway server to respond to HTTP requests.
6. To have your App Gateway listen to HTTP requests in secure mode (HTTPS), select the **SSL Enabled** check box. Otherwise, clear this check box and your App Gateway will listen to non-secure HTTP requests only.

7. If you select the **SSL Enabled** check box, then populate the **Additional Properties** text area with the following values to specify the certificate key pair the App Gateway server will use, protocols and ciphers for SSL:

   ```
   ssl_certificate /usr/local/example.com.rsa.crt;
   ssl_certificate_key /usr/local/example.com.rsa.key;
   ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
   ssl_ciphers HIGH:!aNULL:!MD5;
   ```

   The `/usr/local/example.com.rsa.crt` is the full path of a certificate file in the App Gateway server. The `/usr/local/example.com.rsa.key` is the secret key of that certificate file. You must upload both files to the App Gateway server after you install the App Gateway binary file.

8. In the **Add Host** dialog, click **Save**.

9. In the **Hosts** pane, click **Next >**.

10. In the **Apps** pane, click **Add**.

11. In the **Assign an App to Gate** dialog, map App Gateway to an enterprise application using the values below, and then click **Save**.

   - **Application**: Select the enterprise application you want to protect using this App Gateway.
   - **Select a Host**: Select the host identifier associated with the application you selected.
   - **Resource Prefix**: Enter the URL prefix used by App Gateway to proxy the enterprise application.
   - **Origin Server**: This is the actual base URL where the application is hosted. If the application is not directly accessible, but accessible through a web proxy, then enter the URL of the web proxy. See example diagram below.
   - **Additional Properties**: If the application is accessible through a web proxy, then enter the values below:

   ```
   proxy_pass_header on;
   proxy_set_header host "myapp.internal.example.com";
   ```

   where "myapp.internal.example.com" is the domain name where the application is hosted.

   The following figure provides examples of the mappings that you’re configuring between App Gateway and your enterprise application:
12. Click Finish.

13. In the App Gateway Details page, note the value of the Client ID.

14. Click Show Secret and note the value of the Client Secret.

   The Client ID and Client Secret are equivalent to a credential (for example, an ID and password) that your App Gateway server uses to communicate with Oracle Identity Cloud Service. You'll need these values when you configure the App Gateway server.

15. In the Navigation Drawer, click App Gateways.

16. In the App Gateways page, select your App Gateway, click Activate, and then click OK in the Confirmation window to activate your App Gateway.

### View Details About an App Gateway

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click App Gateways.

2. In the App Gateways page, click the App Gateway row to view the app gateway details.

   You can modify the App Gateway configurations.

### Activate and Deactivate App Gateways

You can use Oracle Identity Cloud Service to activate and deactivate app gateways.

- Deactivating an App Gateway prevents Oracle Identity Cloud Service from working with the App Gateway software.
- Activating an App Gateway enable Oracle Identity Cloud Service working with the App Gateway software.

**Note:**

A green check mark ✓ indicates an activated App Gateway. A red circle with a white line through the circle ☞ indicates a deactivated App Gateway.
Activate App Gateways

You can use Oracle Identity Cloud Service to activate app gateways.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click App Gateways.
2. In the App Gateways page, select the check box for each App Gateway that you want to activate.
3. Click Activate.
4. In the Confirmation window, click OK. The status of each App Gateway changes from deactivated 🚫 to activated ✔️.

Deactivate App Gateways

You can use Oracle Identity Cloud Service to deactivate app gateways.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click App Gateways.
2. In the App Gateways page, select the check box for each App Gateway that you want to deactivate.
3. Click Deactivate.
4. In the Confirmation window, click OK. The status of each app gateway changes from activated ✔️ to deactivated 🚫.

Modify an App Gateway

After viewing details about, activating, or deactivating an App Gateway, you can modify it.

Modifying an App Gateway in Oracle Identity Cloud Service includes:

- Changing the name or description of the App Gateway
- Show or regenerate the client secret
- Add or remove hosts
- Add or remove enterprise applications

To modify an App Gateway:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click App Gateways.
2. In the App Gateways page, click the App Gateway that you want to modify.
   The App Gateway page opens and displays three tabs: Details, Hosts, and Apps.
3. After you modify any App Gateway configuration, click Save to save the modification.
Remove App Gateways

You can use Oracle Identity Cloud Service to remove multiple app gateways simultaneously.

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click App Gateways.

2. In the App Gateways page, select the check box for each App Gateway that you want to remove.

3. Click Remove.

4. In the Confirmation window, click OK.
Manage Account Recovery in Oracle Identity Cloud Service

This section describes how to manage account recovery in Oracle Identity Cloud Service.

Topics:
- Typical Workflow for Managing Account Recovery in Oracle Identity Cloud Service
- Configure Account Recovery

Typical Workflow for Managing Account Recovery in Oracle Identity Cloud Service

With the account recovery feature in Oracle Identity Cloud Service, you can perform tasks such as configuring account recovery. This way, if users have trouble signing in, they're locked out, or they forget their passwords, then they can regain access to their accounts.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure account recovery</td>
<td>Configure account recovery using the Account Recovery Settings page.</td>
<td>Configure Account Recovery</td>
</tr>
</tbody>
</table>

You can configure account recovery by:
- The Identity Cloud Service console
- SCIM-based APIs

The following sections describe how to manage account recovery by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Configure Account Recovery

Account recovery is an automated process designed to help users regain access to their accounts if they have trouble signing in, they're locked out, or they forget their passwords.

There are three account recovery factors that identity domain administrators and security administrators can configure for users:
- Security questions: You can allow a user to select and answer security questions, and provide hints for answers to these questions, to verify their identity. If they
have to recover their account, then they must answer these questions correctly to regain access.

- **Email**: By default, a user’s primary email address has been set as the email address that Oracle Identity Cloud Service will use to help the user recover their account. If the user has to regain access, then Oracle Identity Cloud Service will send a notification to this email address. The user follows the instructions in the notification to recover their account.

  Instead of their primary email address, you can allow the user to specify an alternate (recovery) email address to regain access to their account.

- **Text message (SMS)**: You can allow a user to provide a mobile number that Oracle Identity Cloud Service will use to help them recover access to their account. This way, if they have to regain access, then Oracle Identity Cloud Service will send a passcode in a text message (SMS) to this mobile number. The user enters this passcode to recover their account.

  **Tip:**
  
  This account recovery factor is useful for users without Internet connectivity.

**Important:**

Because you want users to be able to regain access to their accounts, you must set at least one account recovery factor for them.

In addition to setting account recovery factors, identity domain administrators and security administrators can specify:

- How many consecutive, unsuccessful account recovery attempts a user can make before the user’s account is locked.
- How long the user’s account will be locked before they can attempt to recover their account again.

You can access the Manage Account Recovery in Oracle Identity Cloud Service infographic to see how to configure account recovery factors for users.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Account Recovery**. The **Account Recovery Settings** page appears.

2. Use the following table to populate the **Account Recovery Settings** page:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Questions</td>
<td>If you want users to be able to configure security questions to recover their accounts, then select this check box. Otherwise, deselect this check box, and in the Deactivate Security Questions? dialog box, click Deactivate Security Questions. If you select this check box, then click Configure to set up security questions that users can manage for their accounts. See Set Up Security Questions as an Authentication Method.</td>
</tr>
<tr>
<td>Email</td>
<td>If you want users to be able to specify an email address other than their primary email address to recover their accounts, then select this check box. Otherwise, deselect this check box, and in the Deactivate Email? dialog box, click Deactivate Email. If you select this check box, then click Configure to define the settings for the notification that’s sent to the user. See Configure Email Settings.</td>
</tr>
<tr>
<td>Text Message (SMS)</td>
<td>If you want users to be able to provide a mobile number to recover their accounts, then select this check box. Otherwise, deselect this check box, and in the Deactivate SMS? dialog box, click Deactivate SMS. If you select this check box, then click Configure to define the settings in Oracle Identity Cloud Service for sending a passcode as a text message (SMS) to the user. See Configure Text Message (SMS) Settings.</td>
</tr>
<tr>
<td>Maximum consecutive unsuccessful recovery attempts</td>
<td>Specify the number of consecutive, unsuccessful account recovery attempts after which the user’s account is locked.</td>
</tr>
<tr>
<td>Lockout duration</td>
<td>Specify (in minutes) how long the user’s account will be locked (because they exceeded the setting in the Maximum consecutive unsuccessful recovery attempts field) before the user can attempt to recover their account again.</td>
</tr>
</tbody>
</table>

3. Click Save.
4. In the Confirmation window, click OK.

Users can set up account recovery for their accounts. See Set Your Account Recovery Options.
Manage Oracle Identity Cloud Service Multi-Factor Authentication Settings

Learn how to configure security settings such as Multi-Factor Authentication (MFA) for your environments.

Topics

• Typical Workflow for Managing Oracle Identity Cloud Service Security Settings
• Understand Multi-Factor Authentication
• Configure Multi-Factor Authentication Settings
• Configure Authentication Factors
• Multi-Factor Authentication Authorization Flows

Typical Workflow for Managing Oracle Identity Cloud Service Security Settings

Use the MFA and Factors pages within the Security tab in Oracle Identity Cloud Service to perform tasks such as configuring MFA settings and configuring the authentication factors that you want to use.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand MFA</td>
<td>Learn about MFA and the types of authentication factors that are supported in Oracle Identity Cloud Service.</td>
<td>Understand Multi-Factor Authentication</td>
</tr>
<tr>
<td>Enable MFA</td>
<td>Enable MFA by adding a sign-on rule for MFA.</td>
<td>Add a Sign-On Policy</td>
</tr>
<tr>
<td>Configure MFA</td>
<td>Configure overall MFA policy settings such as the type of factors that you want to allow and compliance policies using the Multi-Factor Authentication (MFA) Settings page.</td>
<td>Configure Authentication Factors</td>
</tr>
<tr>
<td>Disable MFA</td>
<td>Disable MFA by deactivating the MFA sign-on rule.</td>
<td>Deactivate Sign-On Policies</td>
</tr>
</tbody>
</table>

You can access the Configure Multi-Factor Authentication (MFA) infographic to see how to enable and configure MFA.

You can enable, manage, and disable MFA by using:

• The Oracle Identity Cloud Service administration console
• SCIM-based APIs

In the following sections, you learn how to manage MFA by using the Oracle Identity Cloud Service administration console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Understand Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user’s identity.

With MFA enabled in Oracle Identity Cloud Service, when a user signs in to an application, they are prompted for their user name and password, which is the first factor — something that they know. The user is then required to provide a second type of verification. This is called 2-Step Verification. The two factors work together to add an additional layer of security by using either additional information or a second device to verify the user’s identity and complete the login process.

MFA may include any two of the following:

• Something that you know, like a password.
• Something that you have, like a device.
• Something that you are, like your fingerprint.

Users are increasingly connected, accessing their accounts and applications from anywhere. As an administrator, when you add MFA on top of the traditional user name and password, that helps you to protect access to data and applications. This also reduces the likelihood of online identity theft and fraud, which secures your business applications even if an account password is compromised.

Configure Multi-Factor Authentication Settings

Configure tenant-specific Multi-Factor Authentication (MFA) settings and compliance policies that define which authentication factors that you want to allow.

To define MFA settings in Oracle Identity Cloud Service, you must be assigned to either the identity domain administrator role or the security administrator role.

1. In the Oracle Identity Cloud Service console, expand the Navigation Drawer, click Security, and then MFA.

2. To enable MFA, select the factors that you want to enable for your users. You must then either edit the default sign-on rule or add a new sign-on rule for MFA.

3. Use the Trusted Device(s) section to configure trusted device settings. Similar to “remember my computer,” trusted devices don’t require the user to provide secondary authentication each time that they sign in (for a defined time period).

4. Use the Factors and Login Rules sections to configure the number of factors your users can enroll in and the number of times you want to allow a user to incorrectly provide MFA verification before they are locked out.

5. Click Save, and then click OK in the Confirmation window to save the configuration.
Configure Authentication Factors

Oracle Identity Cloud Service offers a variety of Multi-Factor Authentication (MFA) factors that you can configure.

The following is a brief overview of the authentication factors available for use with 2-Step Verification.

- **Mobile App Passcode**: Use an authenticator app, such as the Oracle Mobile Authenticator (OMA) app to generate an OTP. An OTP can be generated even when the user's device is offline. After the user enters their user name and password, a prompt appears for the passcode. The user obtains a generated passcode from the app, and then enters the code as the second verification method.
  
  Oracle Identity Cloud Service also works with any third-party authentication app that adheres to the TOTP: Time-Based One-Time Password Algorithm specification, such as the Google Authenticator.

- **Mobile App Notification**: Send a push notification that contains an approval request to allow or deny a login attempt. Push notifications are an easy and quick way to authenticate. After the user enters their user name and password, a login request is sent to the app on their phone. The user taps Allow to authenticate.

- **Security Questions**: Prompt the user to answer security questions to verify their identity. After the user enters their user name and password, they must answer a defined number of security questions as the second verification method.

- **Text Message (SMS)**: Send a passcode as a text message (SMS) to the user. This method is useful for users without Internet connectivity. After the user enters their user name and password, Oracle Identity Cloud Service sends a passcode to their device for use as a second verification method.

- **Email**: Send a one-time passcode in an email to the user. After the user selects Email as the authentication method, Oracle Identity Cloud Service sends a one-time passcode to the user’s primary email address for use as a second verification method. The user’s primary email address is defined in the user’s Oracle Identity Cloud Service account.

- **Bypass Code**: Use the Oracle Identity Cloud Service self-service console to generate bypass codes. The ability to generate a bypass code is available to the user after the user enrolls in 2-Step Verification. Users can generate bypass codes and save for use later. User-generated bypass codes never expire, but can only be used once. Users also have the option to contact an administrator to obtain a bypass code for access.

Learn About Using Mobile Authenticator Apps with MFA

Using a mobile authenticator application for MFA provides a second factor of authentication in the form of a time-based one-time passcode (OTP) or push notification, and offers multiple options for implementing app protection and compliance policy.

A mobile authenticator app is a soft token that is installed on a mobile device. A mobile authenticator app uses either OTP or push notifications to prove that the user has
possession of the mobile device. Only the mobile authenticator app that is in possession of the user’s secret key can generate a valid OTP. During MFA enrollment, when a user scans the Quick Response (QR) code or uses the enrollment URL, the mobile authenticator app is automatically configured with the Oracle Identity Cloud Service server. The mobile authenticator app retrieves a secret key, which is required to generate the OTP and to receive push notifications on the mobile authenticator app. That secret key is then shared between the client and the Oracle Identity Cloud Service server.

A user can use the mobile authenticator app to generate an OTP both online or offline. However, registering for push notifications and performing device compliance checks (jailbreak detection/PIN protection) can only be done while online.

- **Mobile App Passcode**: Use a mobile authenticator app, such as the Oracle Mobile Authenticator app, to generate an OTP. A new OTP is generated every 30-60 seconds and is valid for 90-180 seconds. After the user enters their user name and password, a prompt appears for the passcode. After generating the passcode using the mobile authenticator app, the user enters that code as the second verification method.

- **Mobile App Notification**: Send a push notification to the OMA app that contains an approval request to allow or deny a login attempt. After the user enters their user name and password, a login request is sent to their phone. The user taps Allow to authenticate.

The OMA app is available for Android, iOS, and Windows operating systems.

---

**Note:**

During MFA enrollment, a user must enter the key manually or use the enrollment URL when using the OMA app on a Surface Pro or Windows Desktop device. The QR code scanner can't be used due to a camera limitation. When a user enters that key manually, the OMA app supports only BASE32 encoding.

When you enable both the **Mobile App Passcode** and **Mobile App Notification** factors and a user is enrolled in Mobile App as a second method of verification, the Mobile App Notification factor is the default that is presented to the user. Users can change which factor they want to use by either selecting a different backup verification method when logging in or by selecting a different method as their default option.

Oracle Identity Cloud Service users can use the OMA app or any supported third-party authenticator app that they want to generate OTPs. However, users must use the OMA app to receive push notifications.

Oracle Identity Cloud Service works with any third-party authenticator app (such as Google Authenticator) that adheres to the TOTP: Time-Based One-Time Password Algorithm specification. There are no special administrator configuration steps for third-party authenticator apps. When a user enrolls in MFA and selects **Mobile App** as the method, the user can either select the **Enter Key Manually** or **Scan offline QR code** options to set up third-party authenticators. We recommend the use of the OMA app as it supports notifications and security features such as app protection policy, compliance policy, and silent key refresh.
Configure Mobile OTP and Notifications

Configure policy for the time-based one-time passcode (OTP), and protection and compliance policies for the Oracle Mobile Authenticator (OMA) app.

1. In the Oracle Identity Cloud Service console, expand the Navigation Drawer, click Security, Factors, and the Mobile App tab appears.

2. In the Passcode Policy section, the default values are the industry-recommended settings. Make changes to these settings, if necessary.
   - The value in the New Passcode Generation box indicates the number of seconds before a new passcode must be generated. To avoid clock skew, which is the time difference between the server and the device, the user must make sure that their device clock is synchronized. The maximum allowed time difference between the server and the device is 90 seconds.
   - The value in the Secret Key Refreshed box indicates the number of days before you want to refresh the shared secret. Each time that a user enrolls a mobile device, a secret key is pushed and securely stored on the device via the scanned Quick Response (QR) code or when the user enters the key manually. This key is the input to the OTP algorithm that is used to generate the OTP. The key is refreshed silently, so no user action is required.

3. In the Notification Policy section, select Enable pull notifications to allow the OMA App to pull pending notification requests from the server. Pull notifications are updates that are delivered to a mobile device or computer in response to a user who is manually checking for login request notifications. You can only enable this option if you enabled the Mobile App Notification factor on the Multi-Factor Authentication (MFA) Settings page.

Pull notifications are useful in scenarios where the GCM service (Android), APNS Service (iPhone), or WMS service (Windows) doesn't work. For example, China blocks the GCM service, so users don't receive notifications that are pushed to their device. However, if pull notifications are available, the user can manually pull notifications from a server using the OMA app. Also, offering pull notifications is useful in situations where push notifications are not 100% reliable.

4. In the lower section of the page, configure app configuration and compliance policy for the OMA app. Compliance policy checks are performed each time that the OMA app launches.

Configure Security Questions

Configure security questions settings, select the security questions that a user may use as a second verification method during log in, and add custom security questions.

1. In the Oracle Identity Cloud Service console, expand the Navigation Drawer, click Security, Factors, and then select the Security Questions tab.

2. In the Security Questions Settings section, set options for answer length and the number of questions a user is asked. The default number of security questions that a user must set up is set to three and can't be changed using the UI. If you need to change this number, you must use the /SecurityQuestionSettings endpoint.
3. In the **Manage Security Questions** section, select the check boxes for the questions that you want to use. To disable a default security question, deselect the check box for that question.

- To add a custom security question, select the language in which you want to view the security questions, click **Add Question**, enter the custom security question in the default language row indicated with an asterisk (*), and click **Save**. Optionally, enter the translated question text into the appropriate language row. When you view the custom security questions in a different language, those questions appear in your default language if you don't provide translated question text.
- To edit a custom security question, click the menu to the right of the question, select **Edit**, make your changes, and click **Save**.
- To remove a custom question (you can't remove default questions), click the menu to the right of the question, select **Remove**, and click **Remove** at the confirmation dialog box.

### Configure Text Message (SMS) Settings

Configure settings for sending a passcode as a text message (SMS) to the user in Oracle Identity Cloud Service. This method is useful for users without Internet connectivity.

1. In the Oracle Identity Cloud Service console, expand the **Navigation Drawer**, click **Security, Factors**, and then the **SMS** tab.
2. Make any necessary changes to the settings for the one-time passcode that is sent in a text to the user's device.
3. Select the language in which you want to view the text message, and then click **View** to preview the text message.
4. Use the message template to create the wording that is sent in the SMS message to the user. Oracle Identity Cloud Service provides a fixed list of message variables for your use. Click **Message Variables** to view the available variables and variable definitions.

**Note:**

When you use the `${companyName}` variable, be sure to add your company name to the **Company Name** field on the **Branding** page in **Settings**. If you don’t, your company details don’t appear in email notifications, SMS notifications, or in the Oracle Mobile Authenticator (OMA) app when a user completes MFA enrollment.

5. Click **Save**.

### Configure Email Settings

Configure settings for the one-time passcode (OTP) that is sent by Oracle Identity Cloud Service in an email to the user.
1. In the Oracle Identity Cloud Service console, expand the Navigation Drawer, click Security, Factors, and then select the Email tab.

2. Configure valid time frames for the account recovery and email activation notifications and whether you want to allow the user to add an alternate email address for account recovery.

3. In the Configure the mail settings for MFA section, make changes to the settings for the one-time passcode that is sent in an email to the user.

4. Click Save.

   To access the email template that is sent to the user’s primary email account, access that template by expanding the Navigation Drawer, click Settings, Notifications, and then select the Email Templates tab. The template name is 2-Step Email One-Time Passcode Verification.

---

Multi-Factor Authentication Authorization Flow

The authorization flows that support Oracle Identity Cloud Service Multi-Factor Authentication are the Authorization Code Grant Type and SAML2 Assertion.

Authorization Flows that Don't Support Oracle Identity Cloud Service Multi-Factor Authentication:

- Resource Owner Password Credentials Grant Type
- Client Credentials Grant Type
- Assertion Grant Type
- Implicit Grant Type
Manage Oracle Identity Cloud Service
OAuth Settings

Learn how to configure OAuth settings for your environments.

Topics
• Configuring OAuth Settings

Configure OAuth Settings

You can configure OAuth settings to allow all resources.

To configure OAuth settings:
1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Security.
2. Navigate and click OAuth.
3. In the OAuth Settings page, select Always Allow All Resources to allow the client to access any resource within the tenant regardless of the Trust Scope settings at the application level.
4. Click Save. OAuth settings are saved.
Configure Delegated Authentication in Oracle Identity Cloud Service

This section describes how to configure delegated authentication in Oracle Identity Cloud Service.

Topics:
• Typical Workflow for Managing Delegated Authentication in Oracle Identity Cloud Service
• Understand Delegated Authentication
• View Details About Delegated Authentication
• Deactivate Delegated Authentication
• Test Delegated Authentication
• Activate Delegated Authentication
• Handle Network Failure in Delegated Authentication

Important:
The delegated authentication feature is in early access. Contact Oracle Support to activate it.

Typical Workflow for Managing Delegated Authentication in Oracle Identity Cloud Service

With the delegated authentication feature in Oracle Identity Cloud Service, you can perform tasks such as viewing, deactivating, testing, and activating delegated authentication for a Microsoft Active Directory (AD) Bridge associated with an AD domain.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand delegated authentication.</td>
<td>You can learn about delegated authentication, including how administrators can use it so that users can use their AD passwords to sign in to Oracle Identity Cloud Service to access Oracle Identity Cloud Service-protected resources and applications.</td>
<td>Understand Delegated Authentication</td>
</tr>
</tbody>
</table>
Understand Delegated Authentication

With delegated authentication, identity domain administrators and security administrators don’t have to synchronize user passwords between an on-premises Microsoft Active Directory (AD) enterprise directory structure and Oracle Identity Cloud Service. Users can use their AD passwords to sign in to Oracle Identity Cloud Service to access resources and applications protected by Oracle Identity Cloud Service.

Suppose you have an AD domain that contains user accounts that you want to import into Oracle Identity Cloud Service. To transfer these accounts, install and configure an AD Bridge for this domain. The AD Bridge provides a link between the domain and Oracle Identity Cloud Service. Oracle Identity Cloud Service can synchronize with this domain so that any new, updated, or deleted user records are transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between AD and Oracle Identity Cloud Service. See Manage Microsoft Active
Directory (AD) Bridges for Oracle Identity Cloud Service for more information about installing and configuring AD Bridges in Oracle Identity Cloud Service.

After using an AD Bridge to transfer user accounts from the AD domain into Oracle Identity Cloud Service, you want to configure Oracle Identity Cloud Service so that users from this domain must use their AD passwords to sign in to Oracle Identity Cloud Service. To do this, activate delegated authentication for the AD Bridge. However, first, you may want to verify that the AD credentials from a user in the domain can be used to sign in to Oracle Identity Cloud Service. This way, if there are any issues, then you can resolve them before activating delegated authentication.

After you activate delegated authentication in Oracle Identity Cloud Service, if you change or reset a password in Oracle Identity Cloud Service, then the password is stored directly in AD. The AD password policies are applicable for the new password. Password policies configured in Oracle Identity Cloud Service aren't applicable for this password. Oracle Identity Cloud Service doesn't maintain the password.

**Statues**

Find here the three statuses of the Microsoft Active Directory (AD) Bridge.

There are three statuses for an AD Bridge that Oracle Identity Cloud Service uses to communicate with an AD domain to delegate responsibilities for authenticating users of that domain into Oracle Identity Cloud Service:

- **Connected**: The AD Bridge is installed and configured, and can communicate with the domain.
- **No Clients Found**: You installed or configured an AD Bridge without installing the client for the bridge. Click the [Click here to download the client.](#) link to download the client for the bridge.
- **Incompatible Client Found**: You used an outdated version of the client to install or configure an AD Bridge. Click the [Click here to download the client.](#) link to download the updated client for the bridge.

**View Details About Delegated Authentication**

By default, in the **Delegated Authentication** page, you can see the name and status of each Microsoft Active Directory (AD) Bridge that Oracle Identity Cloud Service uses to communicate with an AD domain. You can also see other information about the bridge, such as whether it's activated or deactivated for delegated authentication.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Delegated Authentication**.
2. Expand the node to the left of the AD Bridge about which you want to view additional information. You'll see an **Activate Delegated Authentication** switch, which indicates whether the bridge is activated or deactivated for delegated authentication.

**Tip:**

Click the AD Bridge to see detailed configuration information about it, as well as how many users and groups were transferred by the bridge from AD into Oracle Identity Cloud Service.
Note:

The **Activate Delegated Authentication** switch may be "greyed out" (that is, you can't turn the switch on or off) for one of the following reasons:

1. The status of the AD Bridge is **No Clients Found**. You can't activate delegated authentication for the bridge because the bridge won't work until you install a client for the bridge. Click the **Click here to download the client.** link to download the client for the bridge.

2. The status of the AD Bridge is **Incompatible Client Found**. You can't activate delegated authentication for the bridge because the bridge won't work until you install the correct version of the client for the bridge. Click the **Click here to download the client.** link to download the updated client for the bridge.

3. The AD Bridge isn't configured for delegated authentication. To configure it:
   a. Click the bridge.
   b. Click **Configuration**.
   c. In the **Configure the Microsoft Active Directory Domain** page, scroll down until you see the **Authentication Settings** area.
   d. Select **Enable local authentication**.
   e. Click **Save**.
   f. In the **Save Configuration Changes?** dialog box, click **OK**.

Deactivate Delegated Authentication

You can deactivate delegated authentication for a Microsoft Active Directory (AD) Bridge associated with an AD domain. Users transferred into Oracle Identity Cloud Service through this bridge must use their Oracle Identity Cloud Service passwords to authenticate into Oracle Identity Cloud Service. Also, by deactivating delegated authentication, you can verify that the AD credentials from a user in that domain can be used to sign in to Oracle Identity Cloud Service before activating delegated authentication for the bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Delegated Authentication**.

2. Expand the node to the left of the AD Bridge for which you want to deactivate delegated authentication.

3. Turn Off the **Activate Delegated Authentication** switch.

4. In the **Deactivate Delegated Authentication** window:
   a. Select the **Send a Password Reset Notification (recommended)** option if you want users in the AD domain associated with the AD bridge to receive notifications to reset the passwords for their accounts. This is recommended for security purposes.
   b. Select the **Create a Password** option if you want to create a password for the users in the domain associated with the bridge, and send them a notification to use this password to sign in to Oracle Identity Cloud Service.
5. Click **OK**.

## Test Delegated Authentication

You can verify that a user’s Microsoft Active Directory (AD) credentials from a domain associated with an AD Bridge can be used to sign in to Oracle Identity Cloud Service. This way, if there are any issues, then you can resolve them before activating delegated authentication for the bridge.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Delegated Authentication**.
2. Expand the node to the left of the AD Bridge for which you want to test delegated authentication.
3. Click **Test Delegated Authentication**.
4. In the **Test Delegated Authentication** window, enter the AD user name and password that you want to use to sign in to Oracle Identity Cloud Service.
5. Click **Test**.

## Activate Delegated Authentication

After verifying that the Microsoft Active Directory (AD) credentials of a user in the domain associated with an AD Bridge can be used to sign in to Oracle Identity Cloud Service, activate delegated authentication for the bridge. Users transferred into Oracle Identity Cloud Service through this bridge will use their AD passwords to authenticate into Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Delegated Authentication**.
2. Expand the node to the left of the AD Bridge for which you want to activate delegated authentication.
3. Turn **On** the **Activate Delegated Authentication** switch.
4. In the **Confirmation** window, click **Yes**.

## Handle Network Failure in Delegated Authentication

Most organizations still rely on Microsoft Active Directory (AD) for managing their user accounts, and users rely on Active Directory for authentication and access to various systems. If for some reasons, users are not be able to authenticate themselves with Active Directory credentials. This will have a huge impact on the daily operations and business of the organizations.

To avoid these kind of situations, Oracle Identity Cloud Service provides you with a network failure handling functionality. This functionality helps users to login with Active Directory credentials even when Oracle Identity Cloud Service is not able to reach the Oracle Identity Cloud Service Active Directory (AD) Bridge.

You configure delegated authentication for a bridge in Oracle Identity Cloud Service so that a user can use their Active Directory password to authenticate into Oracle Identity Cloud Service.

If AD Bridge is not reachable, then users are unable to validate their credentials with Active Directory and therefore cannot login into Oracle Identity Cloud Service. Your
Active Directory is not reachable for a number of reasons. This could be due to network connectivity between AD Bridge and Oracle Identity Cloud Service is down.

To avoid this situation, Oracle Identity Cloud Service provides the local password caching functionality to perform local authentication in case AD Bridge is not reachable. This functionality helps delegated users to login into Oracle Identity Cloud Service even if AD Bridge is not reachable. For security reasons, this password is stored in hashed form in Oracle Identity Cloud Service.

It is important to make sure that the lifetime of this cache password in Oracle Identity Cloud Service is limited. You can configure the maximum duration (5 days) you set to cache the password on Oracle Identity Cloud Service. For example, if your network connectivity is down and you have set the cache password duration to 2 days, then it will enable users to login to Oracle Identity Cloud Service for only 2 days. However, if Active Directory is still not reachable for longer than the specified duration, then you will not be able to login to Oracle Identity Cloud Service.

In order to guard against the possibility that someone can use brute force attacks to access your account, you can limit the number of unsuccessful password attempts during password caching in Oracle Identity Cloud Service. After several failed attempts, Oracle Identity Cloud Service locks your user account. There is a limit of 5 which is configurable.

You cannot perform the following operations while the network connectivity is down:

- A user cannot change their own password
- A user cannot reset their own password by validating the token
- A user cannot change their own email address
- An administrator cannot change a user's password to a known value
- An administrator cannot reset a user's password whose password is authenticated by Active Directory

However, if you recently changed a password in Active Directory, then you can login to Oracle Identity Cloud Service with that password while connectivity is down, provided you have already login to Oracle Identity Cloud Service while Active Directory was available.

**Note:**

Sometimes, you might encounter a system error even if you provide a correct password. This is either because the password cache is empty or because the password has expired.

## Activate Local Password Caching

You must activate the local password caching functionality to enable delegated authentication users to login into Oracle Identity Cloud Service in case Microsoft Active Directory is not reachable.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Delegated Authentication**.
2. Expand the node to the left of the AD Bridge for which you want to activate password cache.

3. Turn On the **Do you want to activate password cache** switch.

4. Set the duration you want to cache this password in **Cache password duration (days)**.

5. Select how many unsuccessful password attempts that you want during password caching in **No of unsuccessful password attempts during Password Caching**.

6. Click **Save**.
Transferring Oracle Identity Cloud Service Configuration Data

Learn how to transfer Oracle Identity Cloud Service configurations.

Topics:
- Overview of Transferring Oracle Identity Cloud Service Configurations
- Typical Workflow for Transferring Oracle Identity Cloud Service Configurations
- Download Exported Files

Overview of Transferring Oracle Identity Cloud Service Configurations

If you have more than one Oracle Identity Cloud Service environment, you can transfer configurations from one environment to another.

Transferring configurations permits you to transfer configuration information from one Oracle Identity Cloud Service to another Oracle Identity Cloud Service. It helps reduce the downtime involved in setting up a service.

You can transfer data using the following methods:
- The Identity Cloud Service console
- SCIM-based APIs

In the following sections, you learn how to transfer data by using the Identity Cloud Service console.

For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

This table summarizes the transfer operations permitted in the UI.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Administrator Role Required</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export users.</td>
<td>Export user accounts to a CSV file.</td>
<td>Identity Domain Administrator User Administrator</td>
<td>Exporting User Accounts</td>
</tr>
<tr>
<td>Export groups.</td>
<td>Export groups to a CSV file.</td>
<td>Identity Domain Administrator User Administrator</td>
<td>Exporting Groups</td>
</tr>
<tr>
<td>Export application role memberships.</td>
<td>Export users and groups for Oracle application roles</td>
<td>Identity Domain Administrator Application Administrator</td>
<td>Export Users and Groups for Oracle Application Roles</td>
</tr>
</tbody>
</table>
Typical Workflow for Transferring Oracle Identity Cloud Service Configurations

Use this typical workflow to get started transferring configurations.

After each import step, analyze the data recorded during the bulk load operation. After you import the file, a dialog box appears with the Job ID link for your import job, click the link. Review the details that appear on the Jobs page. This page shows how many accounts you imported, how many accounts imported successfully, and how many accounts can't be imported because of a system error. Common issues that prevent the system from importing the account include:

- Invalid email address format
- Invalid field formats
- Missing required fields
- Invalid CSV file

If there are many invalid accounts, correct the errors in the import file and then import the file again. See Viewing Jobs and Job Details.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Export users.</td>
<td>Use this task to create users only.</td>
<td>Exporting User Accounts</td>
</tr>
<tr>
<td>Step 2: Export groups.</td>
<td>Use this task to create groups and user memberships.</td>
<td>Exporting Groups</td>
</tr>
<tr>
<td>Step 3: Export application role memberships.</td>
<td>Use this task to create application role memberships for users and groups.</td>
<td>Export Users and Groups for Oracle Application Roles</td>
</tr>
<tr>
<td>Step 4: (Optional) Gather diagnostic data.</td>
<td>If you encounter errors, you can set a diagnostics level to capture operational logs. You can then view those logs to help you to determine the cause of the problem. Use the REST API for Oracle Identity Cloud Service to capture diagnostic data.</td>
<td>See Diagnostic Records REST Endpoints</td>
</tr>
</tbody>
</table>
### Task Description

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| Step 5: (Optional) Resolving | If you encounter errors during an export operation, resolve the errors and then try the export operation again.  
If Oracle Identity Cloud Service can't export a user account, then it evaluates the next account in the CSV file.  
View the details of the export job. If the job contains errors, you can export those errors to see the cause.  
If you cannot resolve the errors, use the diagnostic data report to capture operational logs to see if you can determine the cause of the problem. | View Jobs and Job Details  
Export Job Errors |

### Download Exported Files

After you export configuration files from Oracle Identity Cloud Service, you must download the files, for example, if you want to import them to another Oracle Identity Cloud Service.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Jobs**.
2. Locate the specific job for which you want to export the file.
3. Click **View Details**.
4. Click **Download**.

A comma-separated value (CSV) file downloads to your local machine. The CSV file contains a record for each error that includes the error type and the error description.
Part VI

Support

Learn about frequently asked questions, troubleshooting, and supported languages.

Chapters

• Frequently Asked Questions for Oracle Identity Cloud Service
• Troubleshooting for Oracle Identity Cloud Service
• Supported Languages
Frequently Asked Questions for Oracle Identity Cloud Service

To see a list of frequently asked questions for Oracle Identity Cloud Service, see the FAQ page at cloud.oracle.com.
Troubleshooting Oracle Identity Cloud Service

Learn about common problems that you might encounter when using Oracle Identity Cloud Service and learn how to solve them.

Topics

• System Settings and Profile Information
• Users
• Groups
• Import Users and Groups
• Applications
• Identity Providers
• Password Policies
• The Microsoft Active Directory (AD) Bridge
• Reports
• Customizing the Interface
• Web Browser

System Settings and Profile Information

Learn about common problems that you might encounter when specifying system settings and profile information and learn how to solve them.

Topics

• I'm an administrator. On the Default Settings page, I changed the language of the identity domain from English to French, and clicked Save. However, everything still appears in English. Why is that?
• I am trying to change my password but the Submit button is not enabled. How can I change my password?
• I'm a user and I want to provide a separate email address for password recovery. However, when I go to the Email Options tab of the My Profile console, I don't see a way to do this. Why is that?
• I logged out of the Identity Cloud Service console, logged back in, and am redirected to the My Profile console. Why is that?
• How do I change the domain name of the email address that appears in notifications to my company's domain name?
I'm an administrator. On the Default Settings page, I changed the language of the identity domain from English to French, and clicked Save. However, everything still appears in English. Why is that?

Sign out of the Identity Cloud Service console and log back in to see language-related changes for the Identity Cloud Service console.

I am trying to change my password but the Submit button is not enabled. How can I change my password?

Two things could be wrong:

- Make sure the password that you are setting meets all the requirements. If your password conforms to the password policy, then each criterion displays a green check mark.
- Make sure the password that you are entering in the New Password field and the password you are entering in the Confirm New Password field are the same.

I'm a user and I want to provide a separate email address for password recovery. However, when I go to the Email Options tab of the My Profile console, I don't see a way to do this. Why is that?

If your administrator did not enable the Password Recovery Email option for your Oracle Identity Cloud Service identity domain, then you can't specify a password recovery email address that is different than your primary email address.

I logged out of the Identity Cloud Service console, logged back in, and am redirected to the My Profile console. Why is that?

On the Session Settings page, the Logout URL field contains the URL that Oracle Identity Cloud Service uses to redirect the user after a successful login attempt. To redirect the user to the Identity Cloud Service console, change the value in the Logout URL field from /ui/v1/myconsole to /ui/v1/adminconsole.

How do I change the domain name of the email address that appears in notifications to my company's domain name?

As an example, in the Forgot your password? page, if a user enters an incorrect user name (the user name doesn't exist in the Oracle Identity Cloud Service identity store) and clicks Submit, then a message appears, stating that an email will be sent to ****@oracle.com.

How do I change the domain name of this email address to my company's domain name?

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Settings, and then click Default Settings.
2. In the Email Addresses text area, replace oracle.com with your company's domain name.
3. Click Save.
4. In the Confirmation window, click Yes.
Users

Learn about common problems that you might encounter when managing users and learn how to solve them.

Topics

- I logged in successfully to Oracle Identity Cloud Service as an administrator. However, on the Home page, I see only a small subset of functionality. As an example, I don't see the Applications tab. Also, the dashboard doesn't display the Applications pane. Why is that?
- I am locked out of my account? I know I did not change my password. What happened? How do I access the service?
- When importing users from a CSV file, I get an error that says “Invalid UTF-8...”
- While importing users, I am getting the following error, “Unable to determine ID for : [MANAGER NAME]”. How do I fix this?
- When activating a new user or resetting a user password, the administrator profile displays instead of the profile page for the newly activated user. Why?

I logged in successfully to Oracle Identity Cloud Service as an administrator. However, on the Home page, I see only a small subset of functionality. As an example, I don't see the Applications tab. Also, the dashboard doesn't display the Applications pane. Why is that?

The content that you see on the Identity Cloud Service console reflects the administration roles assigned to you. So, if you are not assigned to either the identity domain administrator or application administrator administration roles, you won't see any application-based functionality because you don't have permissions to do so. See Understanding Administrator Roles for a listing of the types of Oracle Identity Cloud Service administrator roles and the privileges for each role.

I am locked out of my account? I know I did not change my password. What happened? How do I access the service?

For security reasons, your administrator might have had to reset passwords for all users.

Check your inbox for an email from your administrator. If you do not have an email from your administrator, contact your administrator directly.

When importing users from a CSV file, I get an error that says “Invalid UTF-8...”

The problem is that the CSV file was not saved in an UTF-8 format. If you do not save the file in a CSV format with UTF-8 encoding, the import fails. Ensure that you have saved the CSV file in UTF-8 format and try to import the file again.

See Import User Accounts and Import Groups.

See Import User Accounts, and Import Groups, and Import Users and Groups for Oracle Application Roles.
While importing users, I am getting the following error, “Unable to determine ID for : [MANAGER NAME]”. How do I fix this?

Validate that the user with the ID given in the “Manager Name” column already exists in the system or that the user is being created as a new user in the same CSV import.

When activating a new user or resetting a user password, the administrator profile displays instead of the profile page for the newly activated user. Why?

This behavior occurs if the administrator and the user are sharing the same browser session or window at the same time.

To work around this issue, ensure that the administrator and the user are not sharing the same browser session or window at the same time.

Groups

Learn about common problems that you might encounter when using groups and learn how to solve them.

Topics

• While importing groups, I am getting the following error, “Unable to determine ID for : <userId>” What does this mean?

This error usually occurs because the user does not exist in the system. Make sure the user with the ID listed in the error exists in the system. New users are not created while importing groups.

Import Users and Groups

Learn about common problems that you might encounter when importing users and groups and learn how to solve them.

Topics

While importing users or groups, I am getting one of the following errors.

• “Failure Reason: Unable to parse CSV file for upload.…”
• “Failure Reason: Mandatory CSV Header not found : <Header Name>.”
• “Failure Reason: Invalid CSV headers found.…”
• “Reading of CSV file unsuccessful : Import CSV records count exceeds records limit”
• “No data to process for import”.

“Failure Reason: Unable to parse CSV file for upload….”

This error occurs when the CSV import file is invalid. Check the format of CSV file by opening the file in a standard spreadsheet application, such as Microsoft Excel or Google Sheets to make sure that each row contains same number of columns.
Tip:
This error also occurs if the CSV file that you are uploading is empty.

"Failure Reason: Mandatory CSV Header not found : <Header Name>.

There are minimum set of headers that must be provided in the CSV file while importing users or groups.

- For users, the CSV import file must contain "User ID", "Last Name", "First Name", "Work Email" columns.
- For groups, the CSV import file must contain "Display Name", "Description", and "User Members".

"Failure Reason: Invalid CSV headers found...."

This error means that the CSV file contains an extra CSV header, which is not permitted as a part of the CSV file.

1. Open the file in a standard spreadsheet application, such as Microsoft Excel or Google Sheets, and then delete the column identified in the error message.
2. Reimport the CSV file.

"Reading of CSV file unsuccessful : Import CSV records count exceeds records limit"

This error means that the CSV import file contains more records than the permissible limit. The maximum number of user accounts that can be imported in a single job must not exceed 100,000 user accounts. For optimal performance, Oracle recommends that you import your users in batches of 25,000. The maximum number of groups that can be imported in a single job must not exceed 100,000 groups. The maximum number of user members per group row in your CSV file must not exceed seven. For optimal performance, Oracle recommends that you import your groups in batches of 10,000.

"No data to process for import"

This error means that the uploaded CSV import file contains no data in it. Check the file to make sure that it contains data.

Applications

Learn about common problems that you might encounter when using applications and learn how to solve them.

Topics

- I added a custom mobile application, but the Client Secret doesn't appear in the Application Added window. Why is that?
- I'm trying to add an Oracle application to Oracle Identity Cloud Service, but I can't do this. Why is that?
- Unable to Obtain Access Token with Special Characters in the Client ID or Client Secret.
• I deleted an App Link associated with my SAML App, but it is still appearing on the My Apps page.

• I'm an end user and I do not see an application that has been granted to me on the My Apps page. Why is that?

• Unable to synchronize a deleted user when that user is created again in the authoritative application.

• When you delete a synchronized user from Oracle Identity Cloud Service, then the user is also deleted from the authoritative application.

I added a custom mobile application, but the Client Secret doesn't appear in the Application Added window. Why is that?

Because a custom browser or mobile device application runs on an unauthenticated browser, machine, or mobile device, Oracle Identity Cloud Service doesn't generate a Client Secret for this type of application.

I'm trying to add an Oracle application to Oracle Identity Cloud Service, but I can't do this. Why is that?

When you use an Oracle application as part of a subscription-based service, your application is cloud-ready (and ready for you). Therefore, you don't have to add it to Oracle Identity Cloud Service.

Unable to Obtain Access Token with Special Characters in the Client ID or Client Secret.

When requesting an access token, the client id and client secret cannot contain special characters.

If your client ID and client secret contain special characters, before base64 encoding, individually URL encode the client ID and the client secret.

If your client ID and client secret do not contain special characters, you are not required to URL encode them first. However, as a best practice, we highly recommend it.

I deleted an App Link associated with my SAML App, but it is still appearing on the My Apps page.

You need to wait (typically a few seconds) for the asynchronous task to remove the App Link before the App no longer appears on the My Apps page.

I'm an end user and I do not see an application that has been granted to me on the My Apps page. Why is that?

Contact your administrator with the details such as the application name. A likely cause could be that the administrator did not select the Display in My Apps option for that application.

Unable to synchronize a deleted user when that user is created again in the authoritative application.

After deleting a user from the authoritative application, you need to perform full synchronization before you create the user again in the authoritative application.
When you delete a synchronized user from Oracle Identity Cloud Service, then the user is also deleted from the authoritative application.

There is no workaround for this at the moment.

Identity Providers

Learn about common problems that you might encounter when using identity providers and learn how to solve them.

Topics

- I am getting invalid signature errors for my Identity Provider. My certificates look correct in the metadata. What could be wrong?
- I am trying to import the Oracle Identity Cloud Service metadata. However, it fails because the certificates are not considered as valid. Why is that?

I am getting invalid signature errors for my Identity Provider. My certificates look correct in the metadata. What could be wrong?

If an Identity Provider partner is created using metadata and the metadata contains two certificates with use="signing" specified, the runtime verifies that the messages from the Identity Provider are signed with the first certificate. If you see invalid signature errors, your Identity Provider is probably signing with the second certificate.

To remove the second signing certificate that is not being used by the Identity Provider to sign the messages, update the metadata.

I am trying to import the Oracle Identity Cloud Service metadata. However, it fails because the certificates are not considered as valid. Why is that?

Unlike many SAML 2.0 Identity or Service Providers, Oracle Identity Cloud Service does not use self-signed certificates for signing and encrypting of SAML 2.0 requests and responses. However, the metadata file only includes the signing and encryption certificates. To get the missing root certificate from Oracle Identity Cloud Service, see Obtaining the Root CA Certificate from Oracle Identity Cloud Service.

Password Policies

Learn about common problems that you might encounter when using password policies and learn how to solve them.

Topics

- I'm trying to customize the Simple and Standard password policies, but I can't do this. Why is that?

I'm trying to customize the Simple and Standard password policies, but I can't do this. Why is that?

The Simple password policy is used for your developer services, trial Cloud services, and demos when you don't want to customize a policy for them. You can't modify this type of password policy.
The Standard password policy is used when you don’t want to use the Oracle-recommended password policy for your enterprise applications. You can’t modify this type of password policy.

Use the Custom password policy to tailor the strength of your password policy to meet the business and security requirements for your enterprise applications.

The Microsoft Active Directory (AD) Bridge

Learn about common problems that you might encounter when using the Microsoft Active Directory (AD) Bridge and learn how to solve them.

Topics

- I can’t use the client for the AD Bridge to connect to Oracle Identity Cloud Service. What’s wrong?
- I’m trying to use the client for the AD Bridge to connect to my AD server. All of my connection details appear to be correct. However, when I click Test, the client can’t recognize the URL. Why is that?
- My AD Bridge now has a status of Unreachable, even though previously, it had a status of Active. Why is that?
- I used the AD Bridge to import a group into Oracle Identity Cloud Service, and then deleted the group in Oracle Identity Cloud Service. How can I re-establish a link between the group in AD and the group in Oracle Identity Cloud Service?
- I regenerated the Client Secret for my AD Bridge, and now my bridge isn’t working. Why is that?
- I’m trying to use the AD Bridge to import AD users into Oracle Identity Cloud Service, but I’m not able to do this. Why is that?

I can’t use the client for the AD Bridge to connect to Oracle Identity Cloud Service. What’s wrong?

If you receive the following error message when you’re creating an AD Bridge:

```
The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.
```

then select the Use SSL check box because your AD server is using an SSL connection to communicate with the bridge.

I’m trying to use the client for the AD Bridge to connect to my AD server. All of my connection details appear to be correct. However, when I click Test, the client can’t recognize the URL. Why is that?

Make sure that the Identity Cloud Service URL matches the URL that’s shown on the Install a Bridge for the Microsoft Active Directory Domain page. To access this page, launch the Identity Cloud Service console, expand the Navigation Drawer, click Settings, click Directory Integrations, and then click Add. In addition to the Identity Cloud Service URL, the page also displays the Client ID and Client Secret.
My AD Bridge now has a status of Unreachable, even though previously, it had a status of Active. Why is that?

Your AD Bridge can have an Unreachable status because:

1. The Oracle Identity Cloud Service administrator uninstalled the client associated with your AD Bridge, but the bridge couldn't be removed from the Directory Integrations page of the Identity Cloud Service console because the client can't connect to the Oracle Identity Cloud Service server. Oracle Identity Cloud Service can't use the bridge to communicate with AD. See Remove a Microsoft Active Directory (AD) Bridge.

2. The administrator regenerated the Client Secret for your AD Bridge, and then uninstalled the client for the bridge.

3. Your AD Bridge is installed and configured. However, the back-end service (or agent) used to establish communication between Oracle Identity Cloud Service and AD is stopped.

   To restart this agent:
   a. Click Start.
   b. In the Search programs and files text box, enter Services, and then press Enter.
   c. In the Services window, click Services (Local), Identity Cloud Service Microsoft Active Directory Bridge Service, and then click Start.
   d. Verify that Started appears as the status for the service.

I used the AD Bridge to import a group into Oracle Identity Cloud Service, and then deleted the group in Oracle Identity Cloud Service. How can I re-establish a link between the group in AD and the group in Oracle Identity Cloud Service?

1. In the Identity Cloud Service console, click Settings.
2. In the side navigation bar, click Directory Integrations.
3. Click the AD Bridge that you want to configure.
4. Click the Configuration tab.
5. In the Select organizational units (OUs) for groups pane, clear the check box for the designated group, and then click Save.
6. Select the check box for the group, and then click Save again.
7. Run the AD Bridge to synchronize the group between Oracle Identity Cloud Service and AD immediately.

I regenerated the Client Secret for my AD Bridge, and now my bridge isn't working. Why is that?

If you're using the 17.2.6 version of the client for the AD Bridge, then you must upgrade your client to the latest version. See Create a Microsoft Active Directory (AD) Bridge to install the updated client for the bridge.
I'm trying to use the AD Bridge to import AD users into Oracle Identity Cloud Service, but I'm not able to do this. Why is that?

The AD Bridge must be able to access the AD organizational units (OUs) and the parent OUs that contain the users you want to import into Oracle Identity Cloud Service. To ensure that the bridge can access the OUs:

1. Launch Active Directory Users and Computers.
2. Right-click the OU that contains the users you want to import into Oracle Identity Cloud Service, and select Properties from the drop-down menu.
3. In the Properties window, click the Security tab.
4. In the Advanced Security Settings window, click the Security tab, and click Advanced.
5. Click Add.
6. In the Permission Entry window, click the Select a Principal link.
7. In the Select User, Computer, Service Account, or Group window, search for the user with which the AD Bridge is configured, and click OK.
8. In the Permission Entry window:
   a. From the Type drop-down menu, select Allow.
   b. From the Applies to drop-down menu, select This Object and all descendant objects.
   c. From the Permissions pane, select the List contents, Read all properties, and Read permissions check boxes.
   d. Click OK.
9. In the Advanced Security Settings window, click OK.
10. In the Properties window, click OK.

Reports

Learn about common problems that you might encounter when using reports and learn how to solve them.

Topics

• I'm an audit administrator and I'm running the Successful Login Attempts report. Is there a way for me to see which users logged into Oracle Identity Cloud Service successfully by using an identity provider, and which users logged in successfully directly through Oracle Identity Cloud Service?

I'm an audit administrator and I'm running the Successful Login Attempts report. Is there a way for me to see which users logged into Oracle Identity Cloud Service successfully by using an identity provider, and which users logged in successfully directly through Oracle Identity Cloud Service?

When you open this report, click the Provider column. Oracle Identity Cloud Service sorts users who logged in successfully by the provider. If an external identity provider is not used, localIDP appears in the Provider column, signifying users logged in
Customizing the Interface

Learn about common problems that you might encounter when customizing the interface and learn how to solve them.

Topics

• I am unable to upload logos to Oracle Identity Cloud Service. Are there standards I am supposed to follow?

I am unable to upload logos to Oracle Identity Cloud Service. Are there standards I am supposed to follow?

The most common problems when uploading files are the incorrect file type or the incorrect file size. Make sure that your logo has a GIF, JPEG, or PNG file extension, does not exceed 200 pixels for the height or width, and has a maximum file size of 300 KB.

Web Browser

Learn about common problems that you might encounter when using a web browser with Oracle Identity Cloud Service and learn how to solve them.

Topics

• When I try to launch Oracle Identity Cloud Service using Firefox on Linux, the web browser crashes. What now?

When I try to launch Oracle Identity Cloud Service using Firefox on Linux, the web browser crashes. What now?

The problem is that you need an updated version of the Linux Firefox browser.


• When I try to configure the Microsoft Active Directory (AD) Bridge after downloading it by using Safari, it doesn't work. Why?

When I try to configure the Microsoft Active Directory (AD) Bridge after downloading it by using Safari, it doesn't work. Why?

The AD Bridge runs only on a Windows environment. If you must download it to another environment, then you still have to install it on a Windows environment.

• The User Name and Password Fields are Pre-Populating in the UI. How do I prevent this?

The User Name and Password Fields are Pre-Populating in the UI. How do I prevent this?

This is a common issue across browsers.
To resolve this issue, when the browser prompts you to remember the user name or password, for example, when logging in to Oracle Identity Cloud Service, select the option **Never save password for this site.**

**Troubleshoot App Gateway**

Learn about common problems that you might encounter when setting up App Gateway and how to solve them:

- I Made Changes in Oracle Identity Cloud Service but the App Gateway Server Doesn't Reflect the Changes
- Error Log Files Contain Invalid_session Message
- Error Log Files Contain GET 127.0.0.1:53 Command Responding Error Number 500

**I Made Changes in Oracle Identity Cloud Service but the App Gateway Server Doesn't Reflect the Changes**

Changes you make to enterprise application and App Gateway definitions in Oracle Identity Cloud Service may not be get reflected immediately on App Gateway because App Gateway caches Oracle Identity Cloud Service information, such as resources and authentication policies of enterprise applications.

**Explanation:** App Gateway contacts Oracle Identity Cloud Service using an agent to collect host and port information. When you start App Gateway, its NGINX server is automatically configured with this information. Any changes to Oracle Identity Cloud Service is periodically polled by the agent.

If you want the changes to be reflected immediately, restart the App Gateway server. See [Start and Stop App Gateway](#).

**Error Log Files Contain Invalid_session Message**

When App Gateway can’t communicate correctly with Oracle Identity Cloud Service, you’ll find invalid_session messages in the App Gateway error log files.

The following is an example of an invalid_session messages in error.log file:

```plaintext
www-authenticate: Bearer error="invalid_session",
error_description="Authentication Failure
```

This can be because of the way App Gateway processes a client request to a protected resource. App Gateway uses NGINX sub requests to make requests to Oracle Identity Cloud Service, and then App Gateway requires Linux NGINX resolver to be configured appropriately to allow these sub requests to function correctly.

1. Verify that the resolver setting in the file `/usr/local/nginx/conf/nginx-cg-sub.conf` is set to the correct IP.
2. Verify that the tenant name in `/usr/local/nginx/conf/cloudgate.config` file is configured correctly.
Error Log Files Contain GET 127.0.0.1:53 Command Responding
Error Number 500

Because App Gateway makes sub requests to an internal servlet, App Gateway requires your virtual machine to listen to port 53.

The App Gateway server must communicate to itself through IP address 127.0.0.1 and port 53.

If you're running App Gateway in a virtual machine software, configure port forward for this port from the host to the guest. See Configure Port Forwarding Rules
Supported Languages

Oracle Identity Cloud Service offers a localized user experience for its web interface.

By default, the web interface language is set to match the web browser locale, but users can override this setting in their profile details. If users change their language setting, the change won’t take effect until the next time they sign in.

The following languages are available:

<table>
<thead>
<tr>
<th>Language</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese – Simplified</td>
<td>Italian</td>
</tr>
<tr>
<td>Chinese – Traditional</td>
<td>Japanese</td>
</tr>
<tr>
<td>English</td>
<td>Korean</td>
</tr>
<tr>
<td>French</td>
<td>Norwegian</td>
</tr>
<tr>
<td>French – Canadian</td>
<td>Portuguese – Brazilian</td>
</tr>
<tr>
<td>German</td>
<td>Spanish</td>
</tr>
</tbody>
</table>
Part VII

Complete Oracle Identity Cloud Service Scenarios

This section describes use case scenarios where Oracle Identity Cloud Service can be used.

Topics:

• Enable Multi-Factor Authentication Security for Oracle Cloud
• Migrate from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service
• Manage Linux Authentication using the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)
Enable Multi-Factor Authentication Security for Oracle Cloud

This scenario is applicable to customers who have recently signed up for the Oracle Cloud Service or those who have migrated to a new Oracle Cloud account. In this scenario, you add one more layer of security to the Oracle Cloud sign in process by configuring Multi-Factor Authentication (MFA).

Topics:
- Scenario Description
- Understand MFA Options in Oracle Identity Cloud Service
- Create the Partners Group
- Enable the Factors
- Configure MFA for Email
- Configure MFA for the Mobile Authenticator App
- Create Users
- Verify that Users Can Access Oracle Cloud
- Generate and Use the Bypass Code

Scenario Description

In this scenario, the Oracle Cloud customer has hired a third-party company to work in the customer's cloud environment. These partner employees work remotely and need to manage Platform (PaaS) and Infrastructure (IaaS) instances in the customer's cloud environment. The customer's security office requires that each partner employee provide a second verification factor on top of the traditional user name and password for authentication.

This scenario's requirements are as follows:
- A second verification factor is required each time that a user signs in. Users can't sign in using just their user name and password.
- Enable two factors for 2-Step Verification: The Oracle Mobile Authenticator (OMA) app on each user's own mobile device and the one-time passcode (OTP) sent to the user's registered email address.
- During the authentication process, users can enable their device as a trusted device for a maximum time frame of one day and can register only one trusted device.
- The email passcode must not be valid for more than 10 minutes.
Understand MFA Options in Oracle Identity Cloud Service

The MFA feature in Oracle Identity Cloud Service enables the customer to add an extra security step to the authentication process. There are four possible factors and a backup method that can be enabled.

- **Security Questions:**
  Users are prompted during the sign-in process to correctly answer a defined number of security questions to verify their identity.

- **Mobile Authenticator Application:**
  Users generate an OTP on the OMA App on their device that must be used during log in.

- **Text Message (SMS):**
  Users receive a temporary passcode as a text message (SMS) on their device that must be used during log in.

- **Email:**
  Users receive an email message that contains a temporary passcode that must be used during log in.

- **Bypass Code:**
  Oracle Identity Cloud Service also enables users to generate a bypass code, which can be used as a backup method when users have forgotten the answers for the security questions, don't have a mobile phone, or can't access their email.

This scenario requires you to enable **Mobile Authenticator Application** and **Email**.

Create the Partners Group

Before setting up the MFA factors, you need to create a Partners group in Oracle Identity Cloud Service console.

Each of the partner's user need to be assigned to the Partners group.

Enable the Factors

In this scenario, you select **Mobile App Passcode** and **Email** as the MFA factors available to the users, and configure a sign-on policy rule for the Partners group.

The following are high level steps to enable these authentication factors:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **MFA**.
2. Select **Mobile App Passcode** and **Email** from the available factors, and then click **Save**.
3. Click **Security** in the **Navigation Drawer**, and then click **Sign-On Policies**.
4. Select the **Default Sign-On Policy**, click **Sign-On Rules** tab, and then click **Add** to add a new rule.
5. Provide a name for the rule, in the **And is a member of these groups** field select **Partners** from the list that appears, and then select **Prompt for an additional factor**.

6. In the **Action** section, select **Enrollment** as **Required** to force the user to enroll in MFA.

7. Click **Save**.

8. After you save the rule, drag the new rule to the position above the **Default Sign-On Rule**.

9. Click **Save** to save the default sign-on policy.

**Configure MFA for Email**

Select Email, so that Oracle Identity Cloud Service sends a one-time passcode to the user's primary email address that was provided while setting up the user's account.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then click **Factors**.

2. Click the **Email** tab, and update the settings according to your requirements.

**Configure MFA for the Mobile Authenticator App**

Select OMA, so that Oracle Identity Cloud Service you can use Mobile Authentication App to allow or deny access to Oracle Identity Cloud Service.

- In Oracle Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, and then **Factors**.

  The **Factors** page opens, and the **Mobile App** tab is selected by default.

The default values for the **Passcode Policy** section are the industry-recommended settings. There is no need to change any of these values.

Although there are no specific requirements about using rooted devices or an older operating system version, the **Compliance Policy** section allows you to define such verification:

- You can deny access to rooted devices, and devices that don’t have a screen lock method configured.
- You can deny access to devices that are using a specific operating system version.

**Create Users**

Use the Oracle Identity Cloud Service console to create a user for each partner employee, and then assign all of them to the **Partners** group.

The users need to be registered in Oracle Identity Cloud Service with their third-party company's email address, to receive the Welcome email.
Verify that Users Can Access Oracle Cloud

After you enable and configure Email or Mobile App factors and create users in Oracle Identity Cloud Service, the first time that a user logs in to Oracle Cloud, the user is prompted to enroll for MFA.

1. The user must select Enable, and then select Email or Mobile App. The user generates an OTP using the OMA App or receives an OTP via email, and then enters the code as the second verification method.

2. The user must then select an additional method as a backup factor. The user selects either Mobile App or Email, and then follows the on-screen instructions.

3. After the user successfully enrolls for both factors and closes all browser windows, the user should be able to open a new browser window and log in to the customer's Oracle Cloud environment.

Generate and Use the Bypass Code

If you enabled the Bypass Code factor in Oracle Identity Cloud Service, users can choose to generate a bypass code after they enroll in 2-Step Verification.

1. After the user successfully signs in and provides a second authentication factor, they can access the My Profile page in Oracle Identity Cloud Service by clicking their user initials in the upper-right corner, and then selecting My Profile from the drop-down list.

2. The user needs to then select the 2-step Verification tab, and then click Manage.

3. On the 2-Step Verification page, the user clicks Generate Bypass Code. In the confirmation dialog box, the user should copy the bypass code and store it in a safe place for future usage as a backup verification method.

4. The user then clicks Done. The bypass code appears in a table that displays the number of uses allowed and when the code expires.

5. Instruct the user to sign out and then access Oracle Identity Cloud Service's My Profile page again. Have the user sign in, but instead of providing the 2-Step Verification factor, click Use backup verification method, select Use a bypass code, and then provide the previously generated bypass code. The user should be able to successfully access the Oracle Identity Cloud Service My Profile page.

The generated Bypass Code works can only be used once. The user should generate a new bypass code and store it for future use.
Migrate from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service

This section describes how to migrate users and role memberships for Oracle Cloud services from traditional cloud accounts to cloud accounts with Oracle Identity Cloud Service.

Topics:

- Typical Workflow for Migrating from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service
- About Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service
- About Migrating Services from a Traditional Cloud Account to a Cloud Account with Identity Cloud Service
- Before You Begin
- Migrate Users
- Migrate Role Memberships
- Migrate Identity Domain Administrator Roles
- Provision and Synchronize Users Between Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service
- Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service
- Migrate Service-Specific Data and Artifacts

Typical Workflow for Migrating from Traditional Cloud Accounts to Cloud Accounts with Identity Cloud Service

You can migrate traditional cloud accounts to cloud accounts with Identity Cloud Service by migrating users, role memberships, and identity domain administrator roles, provisioning and synchronizing users between traditional cloud accounts and cloud accounts with Identity Cloud Service, and migrating service-specific data and artifacts.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand traditional cloud accounts and cloud accounts with Identity Cloud Service.</td>
<td>You can learn about how traditional cloud accounts differ from cloud accounts with Identity Cloud Service.</td>
<td>About Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Understand migrating services from traditional cloud accounts to</td>
<td>You can learn why you should migrate your traditional cloud accounts to cloud accounts with Identity Cloud Service. You can also learn about services in traditional cloud accounts that contain users and role memberships you can migrate, along with the corresponding services for cloud accounts with Identity Cloud Service to which you can import the users and application role memberships.</td>
<td>About Migrating Services from a Traditional Cloud Account to a Cloud Account with Identity Cloud Service</td>
</tr>
<tr>
<td>cloud accounts with Identity Cloud Service.</td>
<td></td>
<td>Before You Begin</td>
</tr>
<tr>
<td>Understand your prerequisites before migrating services.</td>
<td>You can learn about what you should have before migrating services from traditional cloud accounts to cloud accounts with Identity Cloud Service.</td>
<td>Migrate Users</td>
</tr>
<tr>
<td>Migrate users.</td>
<td>You can migrate users from traditional cloud accounts to cloud accounts with Identity Cloud Service.</td>
<td>Provision and Synchronize Users Between Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service</td>
</tr>
<tr>
<td>Migrate role memberships.</td>
<td>You can migrate role memberships from traditional cloud accounts to cloud accounts with Identity Cloud Service.</td>
<td>Migrate Role Memberships</td>
</tr>
<tr>
<td>Migrate identity domain administrator roles.</td>
<td>You can assign the identity domain administrator role to the users whom you migrated from traditional cloud accounts to cloud accounts with Identity Cloud Service.</td>
<td>Migrate Identity Domain Administrator Roles</td>
</tr>
<tr>
<td>Provision and synchronize users between traditional cloud accounts and cloud accounts with Identity Cloud Service.</td>
<td>You can configure a traditional cloud account to be a service provider and Oracle Identity Cloud Service to be an identity provider. As a result, a user can use their federated SSO credentials to log in to the traditional cloud account through their cloud account with Identity Cloud Service. You can also create an Oracle Cloud application in Oracle Identity Cloud Service that’s used to provision and synchronize users between traditional cloud accounts and cloud accounts with Identity Cloud Service.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Understand the mapping between traditional cloud roles and application roles in Oracle Identity Cloud Service.</td>
<td>View a reference table that lists the services in traditional cloud accounts that contain roles you want to export. It also lists the services for cloud accounts with Identity Cloud Service and the application roles to which you want to assign users. Use this table when migrating role memberships.</td>
<td>Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>Migrate service-specific data and artifacts.</td>
<td>You can migrate service-specific data and artifacts for some cloud services.</td>
<td>Migrate Service-Specific Data and Artifacts</td>
</tr>
</tbody>
</table>

### About Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service

You use an Oracle Cloud account to access your cloud services and log into the Oracle Cloud Infrastructure Classic Console, which is where you manage your account and your services.

When you go to sign in to your Oracle Cloud account, you can choose to sign in to two different types of cloud accounts: a traditional cloud account (also known as a cloud service account) and a cloud account with Identity Cloud Service. Traditional cloud accounts use one identity management system which is different from the identity management system associated with cloud accounts with Identity Cloud Service.

### About Migrating Services from a Traditional Cloud Account to a Cloud Account with Identity Cloud Service

You can migrate users and role memberships for Oracle Cloud services from traditional cloud accounts to cloud accounts with Identity Cloud Service.

Each Oracle Cloud service has a corresponding cloud account with Identity Cloud Service to which you can import the users and application role memberships. By migrating services from a traditional cloud account to a cloud account with Identity Cloud Service, the services can use Oracle Identity Cloud Service to manage users and to control access to the services. For this reason, you want to migrate your traditional cloud accounts to cloud accounts with Identity Cloud Service.

See Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service to view a table that lists the services in traditional cloud accounts and the role memberships that you can export along with the services for cloud accounts with Identity Cloud Service and the application roles to which you can assign users. Also, refer to Migrate Role Memberships to learn how to migrate role memberships from traditional cloud accounts to cloud accounts with Identity Cloud Service.
Before You Begin

Before migrating services from traditional cloud accounts to cloud accounts with Identity Cloud Service, ensure that you have the following access and administrative privileges:

- Access to the traditional cloud account that contains the users and role memberships you want to export
- Administrative privileges to export users and role memberships from this traditional cloud account
- Access to a cloud account with Identity Cloud Service
- Administrative privileges in Oracle Identity Cloud Service to import users and application role memberships

In the cloud account with Identity Cloud Service, create instances for each service that you plan to migrate. For example, if you plan to migrate two instances of Oracle Integration Cloud Service, then use the cloud account with Identity Cloud Service to create two instances of this Oracle Cloud service. Also, if there are multiple instances of a cloud service, then migrate each instance, one by one. So, there should be a one-to-one mapping between an old instance and a new service instance.

Migrate Users

To migrate users, export them from the traditional cloud accounts to a CSV file, modify the heading row in the CSV file, and import the users from the CSV file into Oracle Identity Cloud Service.

When you're migrating users to cloud accounts with Identity Cloud Service, you may want users to use the passwords from their traditional cloud accounts. To do this, change the minimum length of the custom password policy in Oracle Identity Cloud Service to eight characters.

**Important:**

Before importing user accounts into Oracle Identity Cloud Service, the account administrator or service administrator should notify the users about the migration of their traditional cloud accounts to cloud accounts with Identity Cloud Service.

After all user accounts are imported, each user will receive a Welcome email notification. The user can use the link in this notification to access their account and set a password for it.

Export Users from Traditional Cloud Accounts

1. Sign in to the Oracle Cloud Infrastructure Classic Console of the traditional cloud account that contains the users that you want to export.

2. Expand the **Navigation Drawer** in the top left corner, and then click **Users**.

3. In the **User Management** page, select the users that you want to export.
4. Click **Export**. The users will be exported into a CSV file.

5. In the dialog box that appears, save the CSV file to your machine.

**Modify the CSV File**

1. Open the CSV file for editing.
   
   You can use a standard spreadsheet application, such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.

2. Change the **User Login** column heading to **User ID** and the **Email** column heading to **Work Email**.

3. Save your changes to the CSV file.

**Import Users into Oracle Identity Cloud Service**

1. Sign in to Oracle Cloud.

2. In the Oracle Cloud Infrastructure Classic Console, expand the **Navigation Drawer** in the top left corner, and then click **Users**.

3. In the **User Management** page, click **Identity Console**.
   
   The Identity Cloud Service console opens.

4. Expand the **Navigation Drawer**, and then click **Users**.

5. Click **Import**.

6. In the **Import Users** dialog box, click **Browse** to locate and select your CSV file.

7. Verify that the path and name of the CSV file you selected appear in the **Select a file to import** field.

8. Click **Import**.

9. After Oracle Identity Cloud Service evaluates all users, review the job results.
   
   - If the job can be processed immediately, then a dialog box appears with the **Job ID** link for your import job. Click the link and review the details that appear on the **Jobs** page.
   
   - If the job can't be processed immediately, then a message appears with a Schedule ID in it. Copy that Schedule ID, and use it to search for the job on the **Jobs** page. The job will appear when processing completes. Go to step 9.

10. In the **Jobs** page, locate the job that you want to view, and then click **View Details**.

    A table displays the first names, last names, email addresses, user names, and statuses of the users that you imported into Oracle Identity Cloud Service.

11. Review the details that appear on the **Jobs** page.

    This page shows how many users you imported, how many users you imported successfully, and how many users can't be imported because of a system error.

---

**Migrate Role Memberships**

To migrate role memberships, first, export them from the traditional cloud accounts. Then, modify the CSV file that contains the role memberships you exported so that
you can import them into Oracle Identity Cloud Service. Next, import the role memberships into Oracle Identity Cloud Service.

You migrate role memberships individually. So, if you want to migrate 10 roles from a traditional cloud account to a cloud account with Identity Cloud Service, then you need to migrate one role at a time.

To see the mappings between roles in traditional cloud accounts and application roles in cloud accounts with Identity Cloud Service, refer to the table in Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service.

Export Role Memberships from Traditional Cloud Accounts

1. Sign in to the Oracle Cloud Infrastructure Classic Console of the traditional cloud account that contains the role memberships that you want to export.
2. Expand the Navigation Drawer in the top left corner, and then click Users.
3. Navigate to the Roles tab.
4. Select the role that contains memberships you want to export.
5. Click Export. The role memberships will be exported into a CSV file.
6. In the dialog box that appears, save the CSV file to your machine.

Modify the CSV File

1. Locate the exact name of the application role to which you want the users to belong.
2. Open the CSV file that you exported (because you want to modify it).
3. Modify the CSV file as follows:
   a. Remove the First Name, Last Name, and Email column headings.
   b. Change the User Login column heading to Grantee Name.
   c. Add the Entitlement Value column heading. The value for all rows of this column should be the name of the application role you noted in step 1 of this procedure.
   d. Add the Grantee Type column heading. The value for all rows of this column should be User.
4. Save your changes to the CSV file.

Import Role Memberships into Oracle Identity Cloud Service

1. In the Applications page of the Identity Cloud Service console, click the application that has a role to which you want to assign users.
2. Click Application Roles.
3. Click Import.
4. In the Import Application Roles dialog box, click Browse to locate and select your CSV file.
5. Verify that the path and name of the CSV file you selected appear in the Select a file to import field.
6. Click Import.
7. After Oracle Identity Cloud Service evaluates all users that are to belong to the application role, review the job results.
   
   • If the job can be processed immediately, then a dialog box appears with the Job ID link for your import job. Click the link and review the details that appear on the Jobs page.
   
   • If the job can’t be processed immediately, then a message appears with a Schedule ID in it. Copy that Schedule ID, and use it to search for the job on the Jobs page. The job will appear when processing completes. Go to step 8.

8. In the Jobs page, locate the job that you want to view, and then click View Details.
   
   A table displays the user names, classification type (User), and statuses of the users that you imported and assigned to the application role in Oracle Identity Cloud Service.

Migrate Identity Domain Administrator Roles

If a user is an identity domain administrator for their traditional cloud account, then they should also be an identity domain administrator for their cloud account with Identity Cloud Service.

If the user set up their cloud account with Identity Cloud Service, then they will have the identity domain administrator role. However, if this role is not assigned to the user, you must assign it.

In this topic, you assign the identity domain administrator role to the users that you imported into Oracle Identity Cloud Service.

1. Sign in to the Oracle Cloud Infrastructure Classic Console of the cloud account with Identity Cloud Service.

2. Expand the Navigation Drawer in the top left corner, and then click Users.

3. In the User Management page, click Identity Console.
   
   The Identity Cloud Service console appears.

4. Expand the Navigation Drawer, click Security, and then click Administrators.

5. Expand the Identity Domain Administrator node.

6. Click Add, select the check boxes only for those users whom you imported into Oracle Identity Cloud Service and who are identity domain administrators for their traditional cloud accounts, and then click OK.

Provision and Synchronize Users Between Traditional Cloud Accounts and Cloud Accounts with Identity Cloud Service

User provisioning and synchronization are important aspects of application management. Provisioning allows you to manage the lifecycle of accounts in applications like creating and deleting accounts using Oracle Identity Cloud Service.

For example, when you grant the user access to an Oracle Cloud application that’s used to provision users with traditional cloud accounts, then this user is provisioned with the traditional cloud account automatically. This allows you to quickly add new
users to traditional cloud accounts and de-provision users from these accounts instantly when they change roles or leave your organization.

After enabling provisioning, synchronization allows you to control how operations like creating and deleting traditional cloud accounts are reflected in Oracle Identity Cloud Service.

For provisioning and synchronization to occur for users between traditional cloud accounts and cloud accounts with Identity Cloud Service, you configure a traditional cloud account to be a service provider and Oracle Identity Cloud Service to be an identity provider. As a result, a user can use their federated SSO credentials to log in to the traditional cloud account through their cloud account with Identity Cloud Service.

A user must be authenticated only once. For this example, the user obtains a security token. This security token is then validated by Oracle Identity Cloud Service so that the user can access the traditional cloud account. This method is known as federated single sign-on (SSO), where a single token for the user is trusted across multiple IT systems. The same token can be used to authenticate the user against both the identity provider and the service provider (for this example, the cloud account with Identity Cloud Service and the traditional cloud account).

Get Information from the Traditional Cloud Account

In this topic, you get the identity domain, domain name, metadata, and signing certificate from the traditional cloud account. You need this information to set up an Oracle Cloud application in Oracle Identity Cloud Service so that provisioning and synchronization can occur for users between traditional cloud accounts and cloud accounts with Identity Cloud Service.

1. Sign in to the Oracle Cloud Infrastructure Classic Console of the traditional cloud account that contains the identity domain, domain name, metadata, and signing certificate that you want to get.

2. Expand the Navigation Drawer in the top left corner, and then click Users.

3. Navigate to the SSO Configuration tab.

4. In the Configure your Identity Provider Information pane:
   a. Find the value associated with the Provider id field.
   b. Copy the identity domain and the domain name to a text editor, such as Notepad or TextPad.

   **Note:**

   If the value of the Provider Id field is `https://login.dc.migrationsample.<YOUR-DOMAIN-NAME>.com:443/oam/fed/cloud/migration_id_domain`, then the domain name is `dc.migrationsample.<YOUR-DOMAIN-NAME>.com` and the identity domain is `migration_id_domain`.

   c. Click Export Metadata, and then select Provider Metadata (SAML 2.0) from the menu that appears.

   d. Click Export Metadata again, and then select Signing Certificate from the menu that appears.
Get the entityID Attribute Value from the Metadata File

In this topic, you get the entityID attribute value from the metadata file that you exported. You need this information to set up the Oracle Cloud application in Oracle Identity Cloud Service.

1. Open the metadata file that you exported in Get Information from the Traditional Cloud Account.
2. Locate the entityID attribute in this file.
3. Copy the value associated with this attribute to a text editor, such as Notepad or TextPad.

Create an Oracle Cloud Application in Oracle Identity Cloud Service

In this topic, you create an Oracle Cloud application in Oracle Identity Cloud Service that’s used to provision and synchronize users between traditional cloud accounts and cloud accounts with Identity Cloud Service.

Rather than build this application from scratch, use the App Catalog to create this application. The App Catalog contains pre-configured application templates. Using the templates, you can define the application, configure SSO, and configure provisioning and synchronization for the application.

1. Sign in to the Oracle Cloud Infrastructure Classic Console of the cloud account with Identity Cloud Service.
2. Expand the Navigation Drawer in the top left corner, and then click Users.
3. In the User Management page, click Identity Console. The Identity Cloud Service console appears.
4. Expand the Navigation Drawer, and then click Applications.
5. Click Add.
6. In the Add Application window, click App Catalog.
7. In the Type of Integration area of the App Catalog page, click Provisioning.
8. In the search field, enter Oracle Cloud. The Oracle Cloud application appears.
9. Click Add.
10. Populate the Identity Domain, Domain Name, and SSO Domain Name fields of the Details tab with the values that you retrieved in Get Information from the Traditional Cloud Account, and then click Next.

Note:

Use the same value for both the Domain Name and SSO Domain Name fields.

11. Populate the Entity ID field of the SSO Configuration tab with the entityID attribute value that you retrieved in Get the entityID Attribute Value from the Metadata File.
12. Click **Upload** to the right of the **Signing Certificate** field, and then import the signing certificate that you exported in **Get Information from the Traditional Cloud Account**.

13. Click **Download Signing Certificate** to import the Oracle Identity Cloud Service signing certificate into the traditional cloud account.

14. Click **Download Identity Provider Metadata** to import the Oracle Identity Cloud Service identity provider metadata into the traditional cloud account. The traditional cloud account needs this information so that it can trust and process the assertion that is generated by Oracle Identity Cloud Service as part of the federation process. This information includes, for example, profile and binding support, connection endpoints, and certificate information.

15. Click **Next**.

16. In the **Provisioning** tab, click **Continue** in the **Grant Consent** window that appears.

17. Turn on the **Enable Provisioning** switch.

18. In the **Configure Connectivity** pane, configure connectivity for your application by providing values in the respective fields and by testing connectivity.

19. Turn on the **Enable Synchronization** switch.

20. In the **Configure Synchronization** section, modify the attributes for your application.

21. Click **Add**.

**Import the Identity Provider Metadata into the Traditional Cloud Account**

In this topic, you import metadata from Oracle Identity Cloud Service (the identity provider) into the traditional cloud account. The account needs this data so that provisioning and synchronization can occur for a user between the traditional cloud account and a cloud account with Identity Cloud Service.

1. In the traditional cloud account, click the **Users** menu, and then navigate to the **SSO Configuration** tab.

2. In the **Configure SSO** pane, click **Edit**.

3. In the **Edit Single Sign-On Configuration** window, select the **Import identity provider metadata** option, and then click **Choose File** to the right of the **Load Provider Metadata** field.

4. Import the Oracle Identity Cloud Service identity provider metadata that you downloaded in **Create an Oracle Cloud Application in Oracle Identity Cloud Service**.

5. Select the **Enter identity provider metadata manually** option, and then click **Choose File** to the right of the **Load Signing Certificate** field.

6. Import the Oracle Identity Cloud Service signing certificate that you downloaded in **Create an Oracle Cloud Application in Oracle Identity Cloud Service**.

7. Click **Save**.

**Configure Single Sign-On for the Traditional Cloud Account**

In this topic, you configure single sign-on for the traditional cloud account. As a result, a user can use their federated SSO credentials to log in to the traditional cloud account through their cloud account with Identity Cloud Service.
1. In the SSO Configuration tab, click Enable SSO in the Enable SSO pane.

2. In the Enable Sign In to Oracle Cloud Services with Identity Domain credentials pane, click Enable.

Provision a User with a Traditional Cloud Account

In this topic, you use Oracle Identity Cloud Service to create a cloud account with Identity Cloud Service for a user. Oracle Identity Cloud Service will provision the user with a traditional cloud account automatically.

1. In the Identity Cloud Service console, open the Oracle Cloud application.

2. Click the Groups tab, and then click Assign.

3. In the Assign Groups window, assign the All Tenant Users group to this application.

Note: The All Tenant Users group is a default group that’s created by Oracle Identity Cloud Service. All Oracle Identity Cloud Service users are assigned to this group, by default. By assigning this group to the Oracle Cloud application, all users are assigned to this application indirectly.

4. Click Users, and then click Add.

5. In the First Name and Last Name fields of the Add User window, enter the user’s first and last name.

6. In the User Name / Email field, enter the user’s email address.

7. Click Next (because you want to assign the user to the All Tenant Users group).

8. Select the check box for the All Tenant Users group, and then click Finish.

Note: Because the user is assigned to the All Tenant Users group, Oracle Identity Cloud Service will provision the user with a traditional cloud account automatically.

See Verifying the Integration to confirm the integration between the traditional cloud account as the service provider and Oracle Identity Cloud Service as the identity provider.

Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service

The following table lists the services in traditional cloud accounts that contain roles you want to export. It also lists the services for cloud accounts with Identity Cloud Service and the application roles to which you want to assign users.
## Map Between Traditional Cloud Roles and Application Roles in Oracle Identity Cloud Service

<table>
<thead>
<tr>
<th>Service in a Traditional Cloud Account</th>
<th>Role in a Traditional Cloud Account</th>
<th>Service in a Cloud Account with Identity Cloud Service</th>
<th>Application Role in a Cloud Account with Identity Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Developer Cloud Service (Traditional)</td>
<td>DEVELOPER_USER DEVELOPER_ADMINISTRATOR</td>
<td>Oracle Developer Cloud Service</td>
<td>DEVELOPER_USER DEVELOPER_ADMINISTRATOR</td>
</tr>
<tr>
<td>Oracle Integration Cloud Service</td>
<td>Oracle Integration Cloud Administrator Oracle Integration Cloud Service Runtime Oracle Integration Cloud Service Developer Oracle Integration Cloud Service Monitor Oracle Integration Cloud Service Agent Role</td>
<td>Oracle Autonomous Integration Cloud</td>
<td>ServiceAdministrator ServiceUser ServiceDeveloper ServiceMonitor ServiceDeployer</td>
</tr>
</tbody>
</table>
## Migrate Service-Specific Data and Artifacts

You can migrate data and artifacts for the following cloud services:

- **Oracle Developer Cloud Service**: Migrate content from Oracle Developer Cloud Service (Traditional) to Oracle Cloud Infrastructure.
- **Oracle Business Intelligence Cloud Service**: Migrate content from Oracle Business Intelligence Cloud Service to Oracle Analytics Cloud.
- **Oracle Integration Cloud Service**: Migrate content from Oracle Integration Cloud Service to Oracle Autonomous Integration Cloud.
- **Oracle Mobile Cloud Service**: Migrate content from Oracle Mobile Cloud Service to Oracle Mobile Hub.
- **Oracle Process Cloud Service**: Migrate content from Oracle Process Cloud Service to Oracle Autonomous Integration Cloud.
- **Oracle Visual Builder Cloud Service**: Migrate Oracle Visual Builder Traditional Cloud Account instances to Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Service in a Traditional Cloud Account</th>
<th>Role in a Traditional Cloud Account</th>
<th>Service in a Cloud Account with Identity Cloud Service</th>
<th>Application Role in a Cloud Account with Identity Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Process Cloud Service</td>
<td>ProcessServiceAdministrator</td>
<td>Oracle Autonomous Integration Cloud</td>
<td>ServiceAdministrator</td>
</tr>
<tr>
<td></td>
<td>ProcessServiceDeveloper</td>
<td></td>
<td>ServiceDeveloper</td>
</tr>
<tr>
<td></td>
<td>ProcessServiceUser</td>
<td></td>
<td>ServiceUser</td>
</tr>
<tr>
<td>Oracle Visual Builder Cloud Service</td>
<td>Application Builder Developer</td>
<td>Oracle Visual Builder Cloud Service</td>
<td>ServiceDeveloper</td>
</tr>
<tr>
<td></td>
<td>Application Builder Administrator</td>
<td></td>
<td>ServiceAdministrator</td>
</tr>
</tbody>
</table>

---

**Migrate Service-Specific Data and Artifacts**

You can migrate data and artifacts for the following cloud services:

- **Oracle Developer Cloud Service**: Migrate content from Oracle Developer Cloud Service (Traditional) to Oracle Cloud Infrastructure.
- **Oracle Business Intelligence Cloud Service**: Migrate content from Oracle Business Intelligence Cloud Service to Oracle Analytics Cloud.
- **Oracle Integration Cloud Service**: Migrate content from Oracle Integration Cloud Service to Oracle Autonomous Integration Cloud.
- **Oracle Mobile Cloud Service**: Migrate content from Oracle Mobile Cloud Service to Oracle Mobile Hub.
- **Oracle Process Cloud Service**: Migrate content from Oracle Process Cloud Service to Oracle Autonomous Integration Cloud.
- **Oracle Visual Builder Cloud Service**: Migrate Oracle Visual Builder Traditional Cloud Account instances to Oracle Cloud Infrastructure.
Manage Linux Authentication using the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)

This scenario describes how you can use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to integrate your Linux environment with Oracle Identity Cloud Service to perform end user authentication with first and second factor authentication.

Topics:

- Typical Workflow for Managing the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)
- About the PAM
- Install and Configure the PAM
- Configure PAM-enabled Groups and Users
- Test Authentication into Linux Using Oracle Identity Cloud Service

Typical Workflow for Managing the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)

With the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM), you can install and configure the module to allow end users to authenticate in Linux environments with Oracle Identity Cloud Service, using first and second factor authentication.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the PAM.</td>
<td>You can receive an overview of the Oracle Identity Cloud Service Linux PAM.</td>
<td>About the PAM</td>
</tr>
<tr>
<td>Install and Configure the PAM.</td>
<td>You can download, install and configure the PAM.</td>
<td>Install and Configure the PAM</td>
</tr>
<tr>
<td>Configure PAM-enabled Groups and Users.</td>
<td>You can configure a PAM-enabled group and add users to the group using REST API's.</td>
<td>Configure PAM-enabled Groups and Users</td>
</tr>
<tr>
<td>Test Authentication into Linux using Oracle Identity Cloud Service.</td>
<td>You can authenticate on Linux using Oracle Identity Cloud Service first and second factor authentication.</td>
<td>Test Authentication into Linux Using Oracle Identity Cloud Service</td>
</tr>
</tbody>
</table>
About the PAM

The Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) allows you to integrate your Linux environment with Oracle Identity Cloud Service to perform end user authentication with first and second factor authentication.

Topics:

• **What is the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)?**

• **Why use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)**

• **Certified Components**

What is the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)?

The Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) is an authentication module for Linux that performs end user authentication with Oracle Identity Cloud Service.

The PAM also allows Linux administrators, or end users, to query information about users and groups stored in Oracle Identity Cloud Service using standard Linux commands that utilize NSS such as `id`, `group`, and `getent`.

Why use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM)

Use the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) when you want to authenticate users in Linux using Oracle Identity Cloud Service.

An organization may have large numbers of Linux servers, making management of users, for example creating, modifying, or deleting users, a time intensive and costly activity. With the Linux PAM you can manage Linux users centrally in Oracle Identity Cloud Service, providing cost and time savings.

Linux administrators can utilize Oracle Identity Cloud Service to authenticate end users. End users can log in to a Linux server, for example with SSH, and authenticate with their Oracle Identity Cloud Service user credentials. In addition, the multi-factor authentication offerings of Oracle Identity Cloud Service can be utilized so end users are prompted to authenticate with a second factor such as a One Time Password code sent via Email, SMS, a Mobile Authenticator application, or authenticate via security questions. As well as authenticating with single or multiple factors, administrators and end users can use NSS and standard Linux commands to query user and group information.
Certified Components

The following table lists the certified versions for Oracle Identity Cloud Service and your operating system (which is required for the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to run).

<table>
<thead>
<tr>
<th>Oracle Identity Cloud Service</th>
<th>64-Bit</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.2.1</td>
<td>Yes</td>
<td>Oracle Enterprise Linux 6.8+</td>
</tr>
</tbody>
</table>

Install and Configure the PAM

Learn how to download, install and configure the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM).

Topics:
- Download the PAM
- Install the PAM
- Configure a Confidential Application
- Create a Wallet
- Configure the PAM

Download the PAM

To download the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) see:

Download Oracle Identity Cloud Service SDKs and Applications

Install the PAM

To install the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) on your Linux environment, you install the PAM rpm's along with some dependencies:
1. Extract the downloaded zip file to a directory of your choice. This will extract the `pam_cloud.rpm` and `authn_oracle_cloud.rpm`.

2. Check the curl and json-c Linux dependencies are installed:
   - As the root user, run the following commands:
     - `yum list installed | grep curl.x86_64`
     - `yum list installed | grep json-c.x86_64`
   - If they are not installed, run the following commands:
     - `yum install json-c`
     - `yum install curl`

3. Change to the directory where you extracted the zip file:
   - `cd <folder_where_pam_oracle-cloud.pam_resides>`

4. Install the PAM rpm's as the root user.
   - If using `yum`:
     - `yum install pam_oracle-cloud.rpm authn-oracle-cloud.rpm`
   - If using `rpm`:
     - `rpm -Uvh pam_oracle-cloud.rpm authn-oracle-cloud.rpm`

A successful installation will install the following files:
   - `pam_oracle_cloud.so` in `/lib64/security`
   - `libnss_oracle_cloud.so.2` in `/lib64`
   - `libauthn_api.so` in `/lib64`
   - `libclntsh.so.11.1` in `/lib64`
   - `libnnz11.so` in `/lib64`
   - `opc.conf` in `/etc`
   - `walletMgr` in `/usr/bin`

**Configure a Confidential Application**

To register the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) as a client application in Oracle Identity Cloud Service, you create a confidential application with the POSIX Viewer role.

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.

2. Click Add.

3. In the Add Application page, click Confidential Application.

4. In the App Details pane of the Add Confidential Application window, enter the name of the application.

5. Click Next to proceed.
   - A confirmation message indicates that the application has been added in a deactivated state.
6. Click **Configure this application as a client now** and then check the **Client Credentials** and **JWT Assertion** check boxes.

7. In the **Grant the client access to Identity Cloud Service Admin APIs**, click **Add**, and select the **Signin, Me**, and **POSIX Viewer** roles.

8. Click **Next** to proceed.

9. Continue to click **Next** through the remaining screens, then click **Finish**.

10. Take note of the **Client ID** and **Client Secret** that appear in the **Application Added** window.

11. Click **Close**.

12. Click **Activate** and in the **Confirmation** window click **OK**.

Create a Wallet

Configure a wallet on your Linux environment to store the client_id and client_secret of the confidential application with the POSIX Viewer role. This enables the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) to communicate securely with the confidential application.

- On the Linux environment, run the following commands as the root user:
  - `walletMgr add <wallet_location> client_id <client_id>`
  - `walletMgr add <wallet_location> client_secret <client_secret>`

For example:

```
$ walletMgr add /etc/opc-wallet/ client_id b6d001f65da542c38ceb284ea8a05926
wallet initialized successfully.
key client_id is added successfully in wallet.

$ walletMgr add /etc/opc-wallet/ client_secret fea39433-5115-4050-b486-138cce381fb2
wallet initialized successfully.
key client_secret is added successfully in wallet.
```

Configure the PAM

Configure the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) on your Linux environment.

The PAM is configured using **either** the SSSD or NSCD service on Linux.
Note:
The PAM can't be configured using both SSSD and NSCD simultaneously. Choose one configuration only. Choosing whether to use SSSD or NSCD is dependent on how your Linux environment is currently configured. Contact your Linux Administrator for details.

Topics:
• Configure the PAM using SSSD
• Configure the PAM using NSCD

Configure the PAM using SSSD

Configure the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) on Linux using the SSSD service.

Note:
The following prerequisites must be met before proceeding with the configuration.

• The SSSD service should be installed. If it is not installed, install via `sudo yum install sssd`.
• The service must be configured to start when the system reboots. You can perform this configuration via `sudo chkconfig sssd on`.
• The property `SELINUX` must be set as `permissive` or `disabled` in file `/etc/selinux/config`. If it is not set, then set `SELINUX=permissive` or `SELINUX=disabled`.
• Restart Linux to incorporate the above changes.

1. Verify the `/etc/sssd/sssd.conf` file exists, has 600 permission, and is owned by the root user. If the file does not exist create it as follows and run `chmod 600 /etc/sssd/sssd.conf`.

/etc/sssd/sssd.conf

```ini
[sssd]
cfgfile = /etc/sssd/sssd.conf
services = nss, pam
domains = proxy_proxy
[nss]
  fallback_homedir = /home/%u
default_shell = /bin/sh

[pam]
[domain/proxy_proxy]
  auth_provider = proxy
  id_provider = proxy
  proxy_lib_name = oracle_cloud
```
proxy_pam_target = sssd_proxy_oracle_cloud
enumerate = false
cache_credentials = true
debug_level = 5
min_id = 500

2. Verify the `/etc/pam.d/sssd_proxy_oracle_cloud` file exists and is owned by the root user. If the file does not exist then create it as the root user and add the following:

   `/etc/pam.d/sssd_proxy_oracle_cloud` file

   ```
   auth required pam_oracle_cloud.so
   account required pam_oracle_cloud.so
   password required pam_oracle_cloud.so
   session required pam_oracle_cloud.so
   ```

3. Edit the `/etc/pam.d/sshd` and add the `pam_oracle_cloud` module:

   `/etc/pam.d/sshd`

   ```
   auth sufficient pam_oracle_cloud.so
   #Note: the above has to be added before the following line:
   auth include password-auth
   ```

4. Edit the `/etc/ssh/sshd_config` to configure sshd to allow the use of Multi-Factor Authentication:

   `/etc/ssh/sshd_config`

   ```
   #Search for the ChallengeResponseAuthentication property and set it to yes
   ChallengeResponseAuthentication yes
   ```

5. Edit the `/etc/opc.conf` to allow the plugin to interact with Oracle Identity Cloud Service:

   `/etc/opc.conf`

   ```
   #This is sample format of opc.conf file, please use the correct information to configure this file.
   #Enter the Oracle Identity Cloud Service tenancy base url.
   base_url = https://identity-cloud-service-instance-url
   #There is no need to change value of scope.
   scope = urn:opc:idm:__myscopes__
   #Enter the location of the wallet.
   wallet_location = /etc/opc-wallet
   #Enter the log level, this is optional and the default is 0, which means no log. 0 - None, 1 - Error, 2 - Info, 3 - Debug.
   log_level = 0
   #Enter the log file path, this is optional and defaults to /var/log/opc/pam_nss.log
   log_file_path = /var/log/opc/pam_nss.log
   #Enter the value for proxy usage to connect to Oracle Identity Cloud Service. Set the value to 1 to use a proxy and 0 to not use a proxy.
   ```
use_proxy=1
#Enter the information below if use_proxy=1
#Enter the proxy url
proxy_url=http://proxy.example.com
#Enter the proxy port
proxy_port=80
#Enter the username to connect to the proxy url.
proxy_username=username_example
#Enter the password of username to connect proxy url.
proxy_pwd=pwd_example

6. Restart sssd and sshd:
   • authconfig --enablesssd --enablesssdauth --enablemkhomedir --enablepamaccess --update
   • service sshd restart
   • service sssd restart

Configure the PAM using NSCD

Configure the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) on Linux using the NSCD service.

Note:
The following prerequisites must be met before proceeding with the configuration.

• The NSCD service should be installed. If it is not installed, install via `sudo yum install nscd`.
• The service must be configured to start when the system reboots. You can perform this configuration via `sudo chkconfig nscd on`.
• The property `SELINUX` must be set as `permissive` or `disabled` in file `/etc/selinux/config`. If it is not set, then set `SELINUX=permissive` or `SELINUX=disabled`.
• Restart Linux to incorporate the above changes.
1. Edit the `/etc/nsswitch.conf` and add `oracle_cloud` as follows:

   `/etc/nsswitch.conf`
   
   passwd:    files oracle_cloud
   group:     files oracle_cloud

2. Edit the `/etc/nscd.conf` and enable caching in the nscd service:

   `/etc/nscd.conf`
   
   enable-cache    passwd    yes
   enable-cache    group     yes

3. Edit the `/etc/pam.d/sshd` and add the `pam_oracle_cloud` module:
/etc/pam.d/sshd

auth sufficient pam_oracle_cloud.so
#Note: the above has to be added before the following line:
auth include password-auth

4. Edit the /etc/ssh/sshd_config to configure sshd to allow the use of Multi-Factor Authentication:

/etc/ssh/sshd_config

#Search for the ChallengeResponseAuthentication property and set it to yes
ChallengeResponseAuthentication yes

5. Edit the /etc/opc.conf to allow the plugin to interact with Oracle Identity Cloud Service:

/etc/opc.conf

#This is sample format of opc.conf file, please use the correct information to configure this file.
#Enter the Oracle Identity Cloud Service tenancy base url.
base_url = https://identity-cloud-service-instance-url
#There is no need to change value of scope.
scope = urn:opc:idm:__myscopes__
#Enter the location of the wallet.
wallet_location = /etc/opc-wallet
#Enter the log level, this is optional and the default is 0, which means no log. 0 - None, 1 - Error, 2 - Info, 3 - Debug.
log_level = 0
#Enter the log file path, this is optional and defaults to /var/log/opc/pam_nss.log
log_file_path = /var/log/opc/pam_nss.log
#Enter the value for proxy usage to connect to Oracle Identity Cloud Service. Set the value to 1 to use a proxy and 0 to not use a proxy.
use_proxy=1
#Enter the information below if use_proxy=1
#Enter the proxy url
proxy_url=http://proxy.example.com
#Enter the proxy port
proxy_port=80
#Enter the username to connect to the proxy url.
proxy_username=username_example
#Enter the password of username to connect proxy url.
proxy_pwd=pwd_example

6. Restart sshd and nscd:
   • authconfig --enablemkhomedir --enablepamaccess --update
   • service sshd restart
   • service nscd restart
Configure PAM-enabled Groups and Users

Learn how to create new groups and users with POSIX Viewer role attributes, or add POSIX Viewer role attributes to existing groups and users, to allow end users on Linux to authenticate with Oracle Identity Cloud Service using the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM).

Topics:
- Obtain an Access Token
- Create a Group with POSIX Attributes
- Create a User with POSIX Attributes and Add to Group
- Add POSIX Attributes to Existing Groups
- Add POSIX Attributes to Existing Users
- Verify Endpoints

Obtain an Access Token

Obtain an admin access token to allow you to create groups and users with POSIX attributes, or add POSIX attributes to existing groups and users.

- In the Linux environment run the following command:

  ```
curl -k -X POST -u "client-id:client-secret" -d
  "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__" "https://
  identity-cloud-service-instance-url/oauth2/v1/token"
  
  where:
  - client-id is the client ID of a confidential application with administrative privileges
  - client-secret is the client secret of a confidential application with administrative privileges
  - identity-cloud-service-instance-url is your Oracle Identity Cloud Service Instance URL
  ```

Create a Group with POSIX Attributes

Create a group with POSIX attributes.

1. Create a `group.json` file with the following request body:

   ```json
   group.json
   
   {  
   "schemas":  
   [  "urn:ietf:params:scim:schemas:core:2.0:Group",  
   ],  
   "displayName": "posix group",  
   
   
   
   
   ```
where:

- **displayName** is set to the name of the group you wish to create
- **gidNumber** must be set to a unique group id (gid) number. Use the `getent group` command on Linux to see the existing group gid's.

2. Run the following curl command to create the group:

```
```

where:

- **token-string** is the OAuth access token that you obtained
- **identity-cloud-service-instance-url** is your Oracle Identity Cloud Service Instance URL

---

**Note:**

It is not possible to create a group with POSIX attributes using the Oracle Identity Cloud Service Administration Console.

---

Create a User with POSIX Attributes and Add to Group

Create a user with POSIX attributes and add the user to the group previously created.

1. Create a `user.json` file with the following request body:

```json
user.json
{
    "password": "Securepasswd@1",
    "userName": "userPosix",
    "Name.givenName": "user",
    "Name.familyName": "Posix",
    "userType": "Employee",
    "emails": [
        {
            "value": "user.posix@example.com",
            "type": "work",
            "primary": true
        },
        {
            "value": "posix@example.com",
            "type": "home"
        }
    ],
}
```
"addresses": [ 
{
"type": "work",
"primary": true,
"streetAddress": "401 Island Parkway",
"locality": "Redwood Shores",
"region": "California",
"postalCode": "94065",
"country": "US",
"formatted": "userPosix"
}
],
"homeDirectory": "/home/userPosix",
"loginShell": "/bin/bash",
"gecos": "userPosix 24855",
" uidNumber": 12001,
" gidNumber": 11010
},
"meta": {
"resourceType": "User"
},
"schemas": [ 
] 
}

where:

- **userName** is set to the username of the user you wish to create
- **homeDirectory** is set to the location of the user's home directory
- **loginShell** is set to the default shell
- **gecos** is set to general information about the user, for example the user's username and phone number
- **uidNumber** must be set to a unique user id (uid) number in Linux. Use the `getent passwd` command on Linux to see existing users and their uid's
- **gidNumber** must be set to the group id (gid) number created previously

2. Run the following curl command to create the user and add it to the group:

```
user.json
```


where:
- **token-string** is the OAuth access token that you obtained
- **identity-cloud-service-instance-url** is your Oracle Identity Cloud Service Instance URL
Note:

It is not possible to create a user with POSIX attributes using the Oracle Identity Cloud Service Administration Console.

Once the user is created, the user will be sent a notification email to activate their account and set a new password. The user must activate their account before testing authentication in Linux.

Add POSIX Attributes to Existing Groups

Add POSIX attributes to existing groups.

1. Create a group_update.json file with the following request body:

   ```json
   group_update.json
   {
     "schemas": [
       "urn:ietf:params:scim:api:messages:2.0:PatchOp"
     ],
     "Operations": [
       {
         "op": "add",
         "value": 11020
       }
     ]
   }
   ```

   where:
   
   - gidNumber must be set to a unique group id (gid) number. Use the `getent group` command on Linux to see the existing group gid's.

2. Run the following curl command to retrieve the group id's:

   ```bash
   ```

   where:
   
   - token-string is the OAuth access token that you obtained
   - identity-cloud-service-instance-url is your Oracle Identity Cloud Service Instance URL
In the response, note the id of the group you want to update with POSIX attributes. For example, in the response below, the Marketing group id is 8c1f45fee6354e20aa9e57079082d6a2:

```json
...
{  "displayName": "Marketing",  "idcsLastModifiedBy": {    "type": "User",    "value": "f142a5ce639643c2befe8de0ca5bcec",    "display": "admin example",    "$ref": "https://identity-cloud-service-instance-url/admin/v1/Users/f142a5chjky3c2befe8de0ca5bcec"  },  "idcsCreatedBy": {    "type": "User",    "display": "admin example",    "value": "f142a5ce639643c2befe8de0ca5bcec",    "$ref": "https://identity-cloud-service-instance-url/admin/v1/Users/f142a5chjky3c2befe8de0ca5bcec"  },  "id": "8c1f45fee6354e20aa9e57079082d6a2",  "meta": {    "created": "2019-06-10T13:23:59.451Z",    "lastModified": "2019-06-10T13:23:59.451Z",    "resourceType": "Group",    "location": "https://identity-cloud-service-instance-url/admin/v1/Groups/8c1f45fee6354e20aa9e57079082d6a2"  },  "schemas": [    "urn:ietf:params:scim:schemas:core:2.0:Group"  ]}, ...
```

3. Run the following curl command to update the group:

```bash
```

where:
- **token-string** is the OAuth access token that you obtained
- **identity-cloud-service-instance-url** is your Oracle Identity Cloud Service Instance URL
- **id** is the id for the group you want to update with POSIX attributes

---

**Note:**

It is not possible to update a group with POSIX attributes using the Oracle Identity Cloud Service Administration Console.
Add POSIX Attributes to Existing Users

Add POSIX attributes to existing users.

Important note:
In order to add POSIX attributes to an existing user, that user must first be part of a group, and that group must have POSIX attributes.

1. Create a `user_update.json` file with the following request body:

```
user_update.json
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ],
    "Operations": [
        {
            "op": "add",
            "value": "/home/msmith"
        },
        {
            "op": "add",
            "value": "msmith 25895"
        },
        {
            "op": "add",
            "value": 12002
        },
        {
            "op": "add",
            "value": 11020
        },
        {
            "op": "add",
            "value": "/bin/bash"
        }
    ]
}
```
where:

- **homeDirectory** is set to the location of the user's home directory
- **gecos** is set to general information about the user, for example the user's username and phone number
- **uidNumber** must be set to a unique user id (uid) number in Linux. Use the `getent passwd` command on Linux to see existing users and their uid's
- **gidNumber** must be set to the group id (gid) number updated previously
- **loginShell** is set to the default shell

2. Run the following curl command to retrieve the user id's:

```bash
```

where:
- **token-string** is the OAuth access token that you obtained
- **identity-cloud-service-instance-url** is your Oracle Identity Cloud Service Instance URL

In the response, note the id of the user you want to update with POSIX attributes. For example, in the response below, the msmith user id is e5438fce80374d539b8638c289036ecd:

```json
...
{   "idcsCreatedBy": {     "type": "User",     "display": "admin example",     "value": "f142a5ce639643c2befe8deb0ca5bcec",     "$ref": "https://identity-cloud-service-instance-url/admin/v1/Users/f142a5chjky3c2befe8deb0ca5bcec"   },   "id": "e5438fce80374d539b8638c289036ecd",   "meta": {     "created": "2019-06-10T13:24:38.184Z",     "lastModified": "2019-06-10T13:28:50.096Z",     "resourceType": "User",     "location": "https://identity-cloud-service-instance-url/admin/v1/Users/e5438fce80374d539b8638c289036ecd"   },   "active": true,   "displayName": "Mark Smith",
```
3. Run the following curl command to update the user:

```bash
```

where:
- `token-string` is the OAuth access token that you obtained
- `identity-cloud-service-instance-url` is your Oracle Identity Cloud Service Instance URL
- `id` is the id for the user you want to update with POSIX attributes

**Note:** It is not possible to update a user with POSIX attributes using the Oracle Identity Cloud Service Administration Console.

### Verify Endpoints

Verify that you can view users and groups and their POSIX attributes.

1. Obtain a POSIX access token by running the following curl command:

```bash
```

where:
- `client-id` is the client ID for the POSIX confidential application
- `client-secret` is the client secret for the POSIX confidential application
- `identity-cloud-service-instance-url` is your Oracle Identity Cloud Service Instance URL

2. Run the following curl command to view users with POSIX attributes:

```bash
```

where:
- `token-string` is the OAuth POSIX access token that you obtained
- `identity-cloud-service-instance-url` is your Oracle Identity Cloud Service Instance URL

An example response is as follows:
GET HOST/admin/v1/Users

{
   "schemas": ["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
   "totalResults": 3,
   "Resources": [
   {
      "id": "af79f523f0f8416f8407ed80a3bd6cb",
      "userName": "userPosix",
         "homeDirectory": "/home/userPosix",
         "loginShell": "/bin/bash",
         "gidNumber": 12001,
         "gecos": "userPosix 24855",
         "uidNumber": 11010
      }
   },
   {
      "id": "e5438fce80374d539b8638c289036ecd",
      "userName": "msmith",
         "homeDirectory": "/home/msmith",
         "loginShell": "/bin/bash",
         "gidNumber": 11020,
         "gecos": "msmith 25895",
         "uidNumber": 12002
      }
   },
   {
      "id": "f142a5ce639643c2befe8deb0ca5bce",
      "userName": "admin@example.com"
   }
   ],
   "startIndex": 1,
   "itemsPerPage": 50
}

3. Run the following curl command to view groups with POSIX attributes:

   ```bash
   ```

   where:
   - token-string is the OAuth POSIX access token that you obtained
   - identity-cloud-service-instance-url is your Oracle Identity Cloud Service URL

   An example response is as follows:
GET HOST/admin/v1/Groups

{
 "schemas": [
  "urn:ietf:params:scim:api:messages:2.0:ListResponse"
],
 "totalResults": 3,
 "Resources": [
  {
   "displayName": "posix group",
   "id": "afb20ea78e84421aaba7009adf212ecf",
    {
     "gidNumber": 11010
    },
   "members": [
    {
     "value": "af79f523f0f8416fb4407ed80a3bdbc",
     "type": "User",
     "display": "user Posix",
     "name": "userPosix",
     "$ref": "https://identity-cloud-service-instance-url/admin/v1/Users/af79f523f0f8416fb4407ed80a3bdbc"
    }
   ]
  },
  {
   "displayName": "Marketing",
   "id": "8c1f45fee6354e20aa9e57079082d6a2",
    {
     "gidNumber": 11020
    },
   "members": [
    {
     "value": "e5438fce80374d539b8638c28903edc",
     "type": "User",
     "display": "Mark Smith",
     "name": "msmith",
     "$ref": "https://identity-cloud-service-instance-url/admin/v1/Users/e5438fce80374d539b8638c28903edc"
    }
   ]
  },
  {
   "displayName": "All Tenant Users",
   "id": "AllUsersId"
  }
],
 "startIndex": 1,
 "itemsPerPage": 50
}
Test Authentication into Linux Using Oracle Identity Cloud Service

Test authentication on Linux using a user in Oracle Identity Cloud Service.

1. SSH into your Linux environment where the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) is installed.

2. When prompted enter the password for the Oracle Identity Cloud Service user:
   For example:

   ```
   # ssh userPosix@host.example.com
   password:
   Last login: Thur Mar 28th 12:14:04 2019 from host.example.com
   [userPosix@host ~]$
   ```

   You should be logged in successfully.

Enable Multi-Factor Authentication to Authenticate into Linux

Learn how to set up Multi-Factor Authentication (MFA) so Linux users can authenticate via multiple factors.

1. Enable the MFA factors for your requirements. See Configure Multi-Factor Authentication Settings and Configure Authentication Factors

2. Create a group for MFA, and add the POSIX Users to this group.
   a. Navigate to Groups > Add.
   b. Enter the Name of the group and click Next.
   c. Search for the POSIX users you want to enable for MFA.
   d. Select the users and click Finish.

3. Create a Sign-On rule.
   b. Click Sign-On Rules and then Add.
   c. Enter a Rule Name, and under Conditions in the field And is a member of these groups type and select the group that you created above. Under Actions make sure Access is set to Allowed and check the Prompt for an additional factor checkbox. Change the Enrollment to Optional and click Save.

   ✍ Note:
   At present the only sign on policy that the Oracle Identity Cloud Service Linux Pluggable Authentication Module (PAM) supports, is the Default Sign-On Policy.
4. Move the newly created sign-on rule to the top by clicking on the sign-on rule and dragging it to the top of the list. Click **Save**. This will ensure that this rule gets evaluated first so that users belonging to the chosen group are prompted for MFA when they sign in.

5. Login to Oracle Identity Cloud Service as a user in the MFA Group, for example via [https://identity-cloud-service-instance-url/ui/v1/myconsole](https://identity-cloud-service-instance-url/ui/v1/myconsole)

6. Enroll the user in MFA and select the factors to enroll in. See *Enroll in 2-Step Verification for Your Account*

   **Note:**

   Backup factors are not currently supported with the Oracle Identity Cloud Service Linux PAM.

7. Once the user is enrolled in MFA, test authentication on Linux:
   a. SSH into your Linux environment where the Oracle Identity Cloud Service Linux PAM is installed.
   b. When prompted enter the password for the Oracle Identity Cloud Service user.
   c. Enter the second factor with which to authenticate.

   For example, for a user who has configured SMS as their second factor:

   ```bash
   # ssh userPosix@host.example.com
   password:
   Complete 2-Step Verification
   
   An SMS that contains a passcode was sent to +1XXXXXXX455. Enter the passcode or use the following option, and then press Enter:
   r - Resend passcode
   Enter the passcode or an option (r):
   Last login: Thu Mar 28 16:18:52 2019 from localhost
   [userPosix@host ~]$```