Oracle® Cloud

Using Oracle Identity Cloud Service

Release 21.2.1
E57683-09
April 2021

Oracle Cloud Using Oracle Identity Cloud Service, Release 21.2.1

E57683-09

Contents

3 Manage 2-Step Verification

Preface

Welcome to *Using Oracle Identity Cloud Service*.

This guide is intended for all users of Oracle Identity Cloud Service. Users are responsible for configuring settings and managing 2-Step Verification for their accounts, and for using the Oracle Mobile Authenticator (OMA) app.

Audience

Welcome to *Using Oracle Identity Cloud Service*. This guide is intended for non-administrator users of 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 that's available to users. 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

- Administering Oracle Identity Cloud Service
- Integrating Oracle Identity Cloud Service
- Known Issues for Oracle Identity Cloud Service
- REST API for Oracle Identity Cloud Service
- What's New for Oracle Identity Cloud Service
- Oracle Identity Cloud Service Infographics
- Oracle Identity Cloud Service Sample Applications
- Oracle Identity Cloud Service Solutions
- Oracle Identity Cloud Service Tutorials
- Oracle Identity Cloud Service Videos

Conventions

The following text conventions are used in this guide:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I
Get Started

Learn how to get started with Oracle Identity Cloud Service.

Chapters:

1

Get Started with Oracle Identity Cloud Service

The following sections describe how to get started with Oracle Identity Cloud Service for Oracle Cloud users. Familiarity with Oracle Cloud services is assumed.

Topics:

About Oracle Identity Cloud Service

Oracle Identity Cloud Service provides identity management, single sign-on (SSO), and identity governance for applications on-premise, 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.

You can use Oracle Identity Cloud Service to help effectively and securely configure settings and manage 2-Step Verification for your account, and to use the Oracle Mobile Authenticator (OMA) app.

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.

Supported Web Browsers

Oracle Identity Cloud Service supports the following web browsers:

OS	Chrome	Firefox	Internet Explorer **	Microsoft Edge	Safari
Android	Not Supported	Not Supported	N/A	Not Supported	N/A
iOS	Not Supported	Not Supported	N/A	Not Supported	Not Supported
Mac OSX	Supported	Supported	N/A	N/A	Supported
Windows	Supported	Supported	Supported (IE11 Only)	Supported	N/A

> **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.

About the Oracle Identity Cloud Service Consoles

This overview describes the ways that 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

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 Recover Your Account.

There are various ways that you can sign in and authenticate including email, passwordless authentication, and social accounts, If your administrator has configured Passwordless Authentication, you can choose to use it to bypass the standard web-

form-based authentication using email or a mobile device to sign in. For more details, see Understand Passwordless Authentication.

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.

To access the My Profile console, click the avatar icon in the top-right corner, and then select **My Profile**.

Element	Description
My Profile Details	Set up your profile information for the first time or modify your current profile information. See Set Up or Modify Your Profile.
Change My Password	Change your password to Oracle Identity Cloud Service. See Change Your Password.
Email Options	Change your primary email address. See Set Your Email Options.
Security	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.
Social Accounts	Link your social account to your Oracle Identity Cloud Service user account so that you can use your social account's login credentials to access Oracle Identity Cloud Service.
My Access	View the groups and applications to which you have been granted access. See View Group and Application Access.
My Requests	View your requests for access to groups and applications. See View Group and Application Access Requests.

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.

Typical Workflow for Using Oracle Identity Cloud Service

You can modify your profile information, change your password, set your email and account recovery options, link your social accounts, request access to groups and applications, view your requests, view the access that you have to groups and applications, view your applications, and set up 2-Step Verification.

Task	Description	Additional Information
Modify your profile information.	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.	Set Up or Modify Your Profile
Change your password.	Edit your password, recover your forgotten password, or reset your expired password.	Change Your Password
Set your email options.	Modify your primary email address.	Set Your Email Options
Set your account recovery options.	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.	Set Your Account Recovery Options
Link your social accounts.	Link your social accounts to Oracle Identity Cloud Service to access Oracle Identity Cloud Service using your social credentials.	Link and Unlink Social Accounts
Request access to groups and applications.	Request access to groups of which you want to be a member and applications that you want to use.	Request Group and Application Access

Task	Description	Additional Information
View your requests.	View your requests for access to groups and applications.	View Group and Application Access Requests
View your group and application access.	View the groups and applications to which you have been granted access.	View Group and Application Access
View your applications.	View all applications that are assigned to you.	Access My Apps
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 My Profile console	Enroll in 2–Step Verification for Your Account Manage 2–Step Verification from the My Profile Console

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

2

Configure User Settings

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

Topics:

Typical Workflow for Configuring User Settings

Here are the tasks that users can perform to change their passwords, manage their Oracle Identity Cloud Service profile information, manage applications to which they have been granted access, unlink their social accounts from their Oracle Identity Cloud Service accounts, and access their consents.

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.

Task	Description	Additional Information
Change your password.	You can change your password whenever you need to or when it expires.	Change Your Password
Manage your profile information.	You can set up your profile, set your primary email address, configure your account recovery factors, set up and manage your 2–Step Verification methods, and edit your profile information.	Set Up or Modify Your Profile Set Your Email Options Set Your Security Options Manage 2–Step Verification from the My Profile Console
Access and organize your applications.	You can access and organize the applications to which you have been granted access.	Access My Apps

Task	Description	Additional Information
Unlink your social account from your Oracle Identity Cloud Service user account.	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.	Link and Unlink Social Accounts
Access your consents.	Users can list and revoke their consents.	Access Your Consents

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're logging in to Oracle Identity Cloud Service for the first time, then set up your profile information. If you've already set up your profile, then you can modify this information.

Your profile includes the following types of information:

- Account information: Your user name, email address, full name, instant messaging address, and home and mobile phone numbers.
- Work information: Your job title, your work address, phone number, and country, and your time zone and language (locale). The time zone and locale determine the time zone and language that displays for your account in the Identity Cloud Service console.
- Other information: Your user type, employee number, organization name, division, department, and cost center.

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. If you have a multi-valued attribute for your profile, then a **Values** link appears to the right of the attribute. To populate this attribute with values:
   a. Click the **Values** link.
   b. In the popup window that appears, click **Add**.
   c. In the text box that appears, enter a value for the attribute.
   d. Repeat steps b and c to add other values for the attribute.

   > **Tip:**
   >
   > To remove an existing value from the attribute, click the **X** button to the right of the value.

   e. Click **OK**. The counter to the right of the **Values** link changes to reflect the updated number of values for the attribute.
3. 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 **Edit Primary Email** dialog box, enter a new email address in the **Primary Email** field.
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 .

> **Note:**
>
> If you don't see in this pane, then you have not set your mobile number as an account recovery factor.

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 .

> **Note:**
>
> If you don't see in this pane, then you have not set security questions as an account recovery factor.

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**.

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

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.

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.

For applications where your administrator enables the Oracle Secure Form Fill Plug-In, collects your credentials the first time you access the app from the **My Apps** page, and then seamlessly logs you in on future accesses.

Prerequisite: You must be using a Google Chrome or Mozilla Firefox browser.

> **Note:**
>
> Internet Explorer and Edge are not supported.

Install the Oracle Form Fill Plug-in

Learn when and how to install the plug-in that's required to use form fill apps.

When your administrator grants you access to an application that requires the Oracle Form Fill Plug-in, you see a prompt to install the plug-in the next time you open the **My Apps** page.

Follow the steps below to install the plug-in after you see the prompt in **My Apps**.

1. Click your avatar icon at the top right and select **My Apps**.
2. If you see a message at the top of the page that says, "One or more applications granted to you requires the Secure Form Fill Plug-in...", proceed with the steps below to install the form fill plug-in.

   If you don't see the message:
3. Click **Install Plugin** at top right.

   You may need to disable pop-up blocking in order to proceed.
4. Follow browser-specific instructions to complete the plug-in installation.
   - In Google Chrome, just click the **Add to Chrome** button.
   - In Firefox:
     a. Save the plug-in file (`stf.xpi`) locally.
     b. In the file system, right-click the file and open it with FireFox.
5. On the **My Apps** page, refresh the browser window after completing the plug-in installation.
6. Click the icon for an app that requires the form fill plug-in.

   In the **Enter Credentials** dialog box that opens in front of the **My Apps** page, enter your credentials and click **OK** to proceed to the application's home page.

> **Note:**
>
> If instead of the **Enter Credentials** dialog box you see the application's login page – the app doesn't support the form fill plug-in.:

You can now access form fill applications from the **My Apps** page:

1. The first time you access a form fill application:
   a. Instead of going to the application's login page, an **Enter Credentials** dialog box opens in front of the **My Apps** page.
   b. Enter the login credentials for the application in the **Enter Credentials** dialog box and click **Login**.
   The Oracle Form Fill Plug-in captures your credentials and logs you in to the application.
2. When you access the same form fill application from **My Apps** in the future, you are automatically logged in to the application.

> **Note:**
>
> If you later change your login credentials in the application, you must update your credentials from the application tile on the **My Apps** page. See Update Credentials for a Form Fill Application.

Update Credentials for a Form Fill Application

If you change your login credentials with an application that uses the Oracle Form Fill Plugin, you must update your credentials from the **My Apps** page.

After the first time you access a form fill application from the **My Apps** page, the Oracle Form Fill Plugin automatically logs you in to that application in the future. But when you change your login credentials within the application, the automatic login using your old credentials fails, and you must manually enter your credentials in the application's login page.

To restore your automatic login through the form fill plug-in:

1. Click your avatar icon at the top right and select **My Apps**.
2. Locate the form fill application for which your credentials have changed.
3. Click the gear icon in the bottom right corner of the application's tile and select **Update Credentials**.
4. Enter your current login credentials and click **OK**.

3

Manage 2-Step Verification

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

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.

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

Task	Description	Additional Information
Adding a 2–Step Verification Method	Learn how to add 2–Step Verification methods on the **2–Step Verification** page and the authentication methods that are available to you.	Adding a 2-Step Verification Method from the Self-Service Console

Task	Description	Additional Information
Removing a 2–Step Verification Method	Learn how to remove 2–Step Verification methods on the **2–Step Verification** page.	Removing a 2-Step Verification Method
Renaming a 2–Step Verification Method	Learn how to rename a 2–Step Verification method on the **2–Step Verification** page.	Renaming a 2-Step Verification Method
Managing Security Questions	Learn how to set up and manage security questions on the **2–Step Verification** page.	Managing Security Questions
Generating a Bypass Code	Learn how to generate bypass codes on the **2–Step Verification** page.	Generating a Bypass Code
Using a Bypass Code	Learn how to use a bypass code.	Using a Bypass Code
Removing a Trusted Device	Learn how to remove a trusted device on the **2–Step Verification** page.	Removing a Trusted Device

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 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 **Select Your Default 2-Step Verification Method** flow appears after you enter your user name and password.

1. Enter your name and password to log in to an Oracle Identity Cloud Service console where 2-step verification has been enabled.
2. On the **Enable 2-Step Verification** introduction page, click **Enable 2-Step Verification**.

   The authentication methods available to you appear on the **Select Your Default 2-Step Verification Method** page.
3. Click **Mobile SMS**.
4. Enter the mobile number where you want to receive the passcode, and then click **Send Passcode**.

   Oracle Identity Cloud Service sends a passcode by SMS to your mobile device.
5. Enter the passcode into the **Passcode** box, and then click **Verify Mobile Device**.

   The **Successfully Enrolled** page appears.

   If you do not receive a text, click **Resend.**
6. (Optional) 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.
7. Click **Done**.

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 **Mobile Number Verification** page appears, with a message saying that a passcode was sent to your mobile number.
2. Get the passcode from your mobile device and enter it into the **Passcode** box.

   If you didn’t receive the passcode, click **Resend Passcode**.
3. (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.
4. Click **Verify.**

5. (Optional) If you can't receive a text, for example, you don't have your phone with you, click **Show alternative login methods** 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.

6. (Optional) You can also select **Show alternative login methods** to change your default verification method.
   a. Click **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.

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 **Select Your Default 2-Step Verification Method** flow appears after you enter your user name and password.

1. Enter your name and password to log in to an Oracle Identity Cloud Service console where 2-step verification has been enabled.
2. On the **Enable 2-Step Verification** introduction page, click **Enable 2-Step Verification**.

   The authentication methods available to you appear on the **Select Your Default 2-Step Verification Method** page.
3. Click **Mobile App**.

   You are prompted to download the Oracle Mobile Authenticator app from the app store.
4. 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. The 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) 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.

4. (Optional) If you are unable to use the OMA app, for example, you don't have your phone with you, click **Show alternative login methods** 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.

5. (Optional) You can also select **Show alternative login methods** to change your default verification method.
    a. Click **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.

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 **Select Your Default 2-Step Verification Method** flow appears after you enter your user name and password.

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. On the **Enable 2-Step Verification** introduction page, click **Enable 2-Step Verification**.

   The authentication methods available to you appear on the **Select Your Default 2-Step Verification Method** page.
3. Click **Mobile App,** and then select the **Scan offline QR** code check box.
4. 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.
5. 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.
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 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.
3. (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.
4. Click **Verify**.
5. (Optional) If you are unable to use the App, for example, you don't have your phone with you,click **Show alternative login methods** 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.

6. Optional. You can also select **Use backup verification method** to change your default verification method.
   a. Click **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.

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 **Select Your Default 2-Step Verification Method** flow appears after you enter your user name and password.

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. On the **Enable 2-Step Verification** introduction page, click **Enable 2-Step Verification**.

   The authentication methods available to you appear on the **Select Your Default 2-Step Verification Method** page.

3. Click **Security Questions.**

The number of security questions that you are required to answer appear.

4. Select the questions, and then provide your answers.
5. (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.
6. Click **Save**.

   The **Successfully Enrolled** page appears.
7. 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.
3. (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.
4. click **Verify**.
5. (Optional) If you forgot your answers, click **Show alternative login methods** 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.

6. (Optional) You can also select **Show alternative login methods** to change your default verification method.
   a. Click **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.

Set Up Recovery Email or Email as an Authentication Method

Enroll your email as your 2–Step Verification method.

> **Note:**
>
> Depending on how your administrator has configured your email settings, you may see either **Recovery Email**, or **Email**, or both as 2–Step Verification options.

When multi-factor authentication (MFA) is enabled, the first time that you log in, the **Select Your Default 2-Step Verification Method** flow appears after you enter your user name and password.

1. Enter your name and password to log in to an Oracle Identity Cloud Service console where 2-step verification has been enabled.
2. On the **Enable 2-Step Verification** introduction page, click **Enable 2-Step Verification**.

   The authentication methods available to you appear on the **Select Your Default 2-Step Verification Method** page.
3. Click **Recovery Email** or **Email**.

   Oracle Identity Cloud Service sends a one-time passcode to your primary email address.
4. Enter the passcode into the **Code** box, and then click **Verify Email Address**.
5. (Optional) 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.
6. Click **Done**.

Use Recovery Email or Email as an Authentication Method

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

> **Note:**
>
> Depending on how your administrator has configured your email settings, you may see either **Recovery Email**, or **Email**, or both as 2–Step Verification options.

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 email address.

If email isn't your default 2–Step Verification method, you can click **Show alternative login methods** and select **Recovery Email** or **Email** from the list of alternative methods.

After you enroll in email as a 2–Step Verification method, if you change your 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 **Email Verification** page.

   If you didn't receive the email, click **Resend email**.

3. (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.
4. Click **Verify.**
5. (Optional) If you can't receive an email, click **Show alternative login methods** 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.

6. (Optional) You can also select **Show alternative login methods** to change your default verification method.
   a. Click **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.

Enroll in 2-Step Verification After First Login

If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab.

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**.

3. In the **2-Step Verification** section, click **Enable**.
4. In the **2-Step Verification** dialog box, click the button for the method you wish to enable as your default method.
5. Follow the prompts to complete your enrollment.

   See the topic for the method you've selected, under Enroll in 2–Step Verification for Your Account, for more detailed instructions.

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 your Oracle Identity Cloud Service **My Profile** console, **Security** tab.

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 from the My Profile 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.

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 **Show alternative login methods**. All 2–Step Verification methods that you are enrolled in appear in the **Alternative login methods** 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.
- **Recovery Email** or **Email**: Send an OTP to your email address.

> **Note:**
>
> Your administrator determines whether you see options for **Recovery Email**, **Email**, or both.

- **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.
- **Duo Security**: If Duo Security is enabled, use Duo Security as an MFA factor.

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

- Configure an Additional 2–Step Verification Method from the My Profile Console
- Remove a 2–Step Verification Method
- Rename 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

Configure an Additional 2–Step Verification Method from the My Profile Console

Use the 2–Step Verification section of the **Security** tab in the Oracle Identity Cloud Service **My Profile** console to configure an additional verification method for your account.

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

> **Note:**
>
> Only Mobile Number and Mobile App methods can be added from the **My Profile** console **Security** tab.

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**.
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. See the topic for the method you want to add under Enroll in 2–Step Verification for Your Account.

Remove a 2–Step Verification Method

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

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

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**.
3. In the method pane for the method that you want to remove, click the **Action** menu  and select **Remove**.
4. Click **OK** when prompted to confirm the removal.

> **Note:**
>
> You can't remove all of the methods. If you have only one method configured, an error message appears at the top of the page when you confirm the removal.

Rename a 2–Step Verification Method

Use the **2–Step Verification** section of the **Security** tab in Oracle Identity Cloud Service **My Profile** console to rename a verification method associated with your account.

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

> **Note:**
>
> Only Mobile App methods can be renamed.

As an example, you might want to do this 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**.
3. In the method pane for the method that you want to remove, click the **Action** menu and select **Rename**.
4. Enter a new name for the method, and then click **Save**.

Manage Security Questions

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

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

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**.
3. In the **Security Questions** pane:

- If the **Security Questions** pane is **Configured**, click the **Configure** link.
- If the **Security Questions** pane is **Not Configured**, click the **Action** menu and select **Edit**.

4. In the **Security Questions** dialog box:
   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**.

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.

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

Use the **Security** tab in Oracle Identity Cloud Service **My Profile** console 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**.
3. In the **Bypass Codes** section, click **Generate**.
4. In the **Bypass Code** dialog box, copy your bypass code, and then store it in a safe place for use the next time that you need a backup verification method.

> **Note:**
>
> The **Bypass Code** dialog box displays the number of uses allowed. Your bypass code doesn't expire, but you can only used it once.

5. Click **Done**.
6. (Optional) To view and copy your bypass code, in the **Bypass Code** pane, click the **Reveal** icon.
7. (Optional) To send the bypass code to yourself in an email:
   a. In the **Bypass Code** pane, click the **Action** menu and select **Email**.
   b. In the **Confirmation** dialog box, click **OK**.

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 **Show alternative login methods** to use an alternative method to verify your identity.
3. In the **Alternative login 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. Enter your code in the **Bypass code** box.

   If you can't locate your bypass code, contact the help desk to have an administrator generate a bypass code for you.

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.
6. Click **Verify**.

Remove a Trusted Device

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

Prerequisites:

- You must have enrolled in 2–Step Verification. See Enroll in 2–Step Verification for Your Account or Enroll in 2-Step Verification After First Login.
- You must have specified that a device be trusted. See Trust a Device.

Removing a trusted device is a good idea if you no longer plan to connect to Oracle Identity Cloud Service using that device within the time period during which it's trusted.

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**.
3. Scroll down to the **Trusted Devices** section.

4. In the pane for the trusted device that you want to remove, click the **Action** menu  and select **Remove**.
5. In 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 2-Step Verification**. Or, from the **Security** page in the **My Profile** console, click **Enable**.
2. Click the Action menu icon at right end of the **2-Step Verification** line and select **Change Default**.
3. In the **Select Default** dialog box, select a new verification method and click **Done**.

You can also change your default verification method login. See Change Your Default Verification Method During Login.

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.

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

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**.

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

3. In the **2-Step Verification** section, click the **Action** menu  and select **Change Default**.
4. In the **Change Default** dialog box, select the method that you want to use as your default verification method.

> **Note:**
>
> Only those 2–Step Verification methods that you are enrolled in are displayed.

5. Click **Done.**

The check mark appears on the method pane that you just set as your default.

Disable or Re-Enable 2-Step Verification

If your administrator has made 2-Step Verification optional, you can disable and re-enable your enrollment from the Oracle Identity Cloud Service **My Profile** console.

Prerequisite: You must first enable 2-Step Verification. Most users do this when they first log in to Oracle Identity Cloud Service. If your administrator made 2-Step Authentication optional, and you have clicked **Skip** each time you log in, you can enable 2-Step Authentication in the **My Profile** console **Security** tab. See Enroll in 2-Step Verification After First Login.

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**.
3. To disable 2-Step Verification:
   a. Open the **Action** menu icon at the right end of the **2-Step Verification** line and select **Disable**.
   b. In the **Confirmation** dialog box, click **OK**.

   > **Note:**
   >
   > If your administrator has made 2-Step Verification required, disabling it from the **My Profile** console has no effect.

4. To re-enable 2-Step Verification:
   a. In the **2-Step Verification** section, click **Enable**.
   b. In the **2-Step Verification** dialog box, click the button for the method you wish to enable as your default method.
   c. Follow the prompts to complete your enrollment.

      See the topic for the method you've selected, under Enroll in 2–Step Verification for Your Account, for more detailed instructions.

4

Use and Manage the Oracle Mobile Authenticator App

Topics

Typical Workflow for Using and 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.

Task	Description	Additional Information
Use the OMA App	Learn how to add an account to the OMA App by scanning the QR code, entering the key manually, or using the enrollment URL	Use the Oracle Mobile Authenticator App
Manage the Oracle Mobile Authenticator App	Learn how to switch between grid and list views, edit and delete accounts, manage your PIN, and view notification history.	Manage the OMA App

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.

OMA App Version	Mobile Platform Version
Version 4.0+	iOS 7.1+
Version 8.0+	Android 4.1+

OMA App Version	Mobile Platform Version
Version 1.0+	Windows 8.1+

- Add an Account to the OMA App by Scanning the QR Code
- Add an Account to the OMA App by Entering the Key Manually
- Add an Account to the OMA App by Using the Enrollment URL
- Use the Oracle Mobile Authenticator App as an Authentication Method
- Enable OMA App Protection
- Manage the Oracle Mobile Authenticator App

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.

Prerequisite: Complete the steps in Use the Oracle Mobile Authenticator App as an Authentication Method.

1. Open the OMA app on your phone, and then tap **Add Account.**
2. Scan the QR code that displays on the **Download and Configure the Mobile App** 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.

Prerequisite: Complete the steps in Use the Oracle Mobile Authenticator App as an Authentication Method.

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.

Prerequisites:

- Complete the steps in Use the Oracle Mobile Authenticator App as an Authentication Method.
- 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

- 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
Support

Learn about enabling multi-factor authentication for Oracle Cloud.

Chapters

5

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:

Chinese – Simplified	Italian
Chinese – Traditional	Japanese
English	Korean
Finnish	Norwegian
French	Portuguese – Brazilian
French – Canadian	Spanish
German	