

Oracle® FMW

Administering Oracle Universal Authenticator



F88895-02
October 2024



Oracle FMW Administering Oracle Universal Authenticator,
F88895-02

Copyright © 2024, Oracle and/or its affiliates.

Primary Authors: Oracle Corporation, (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Part I Introduction to Oracle Universal Authenticator

Part II Installing Oracle Universal Authenticator

Part III Performing Device Authentication with Oracle Universal Authenticator

Part IV Administering Oracle Universal Authenticator

Part V Self-Service Portal

Part VI Use Cases

Part VII Troubleshooting

Preface

Administering Oracle Universal Authenticator (OUA) describes how to install and configure Oracle Universal Authenticator for device authentication. Oracle Universal Authenticator is a unified authentication solution that provides device authentication with multi-factor authentication (MFA) and cross-platform single sign-on (SSO) to web-based applications.

Audience

This guide is intended for:

- Administrators responsible for installing and configuring Oracle Universal Authenticator (OUA)
- End users who manage their factors and devices using the Self-Service Portal

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <https://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 <https://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <https://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

What's New in This Guide?

This preface shows current and past versions of Oracle Universal Authenticator. When new versions of Oracle Universal Authenticator are released, details of new functionality is outlined.

- [Oracle Universal Authenticator October 2024 Release \(24.10.0001\)](#)
- [Oracle Universal Authenticator April 2024 Release \(24.4.1.0.0\)](#)

Oracle Universal Authenticator October 2024 Release (24.10.0001)

The following are the new features in this release:

- **Password Management** - Administrators can configure Oracle Universal Authenticator (OUA) with Forgot Password URL and Reset Password URL's, so end users can change or reset their Oracle Access Management (OAM) password during login. For example, if they have forgot their password, the password is due to expire or has expired. See, [Configuring Password Management](#).
- **Passwordless Login using Configurable Challenges** - Allows users to use passwordless login where users authenticate with only a second factor during a configurable time window. Administrators can customize the duration and the allowed methods of authentication. See, [Configuring Passwordless Login using Configurable Challenges](#).

Oracle Universal Authenticator April 2024 Release (24.4.1.0.0)

This is the first production release of Oracle Universal Authenticator.

Part I

Introduction to Oracle Universal Authenticator

- [About Oracle Universal Authenticator](#)
- [Key Oracle Universal Authenticator Features and Use Cases](#)
- [System Architecture and Components](#)
- [How Oracle Universal Authenticator Works?](#)

Introducing Oracle Universal Authenticator

Learn more about Oracle Universal Authenticator.

Topics:

- [About Oracle Universal Authenticator](#)
- [Key Oracle Universal Authenticator Features and Use Cases](#)
- [System Architecture and Components](#)
- [How Oracle Universal Authenticator Works?](#)

About Oracle Universal Authenticator

Oracle Universal Authenticator is a unified authentication solution that provides device authentication and cross-platform single sign-on (SSO) to web-based applications.

Users login to their devices using their Oracle Access Management (OAM) credentials with step-up Multi-Factor Authentication (MFA), or alternatively using passwordless login. Users can then access protected applications without the need to enter their single sign-on credentials again.

Oracle Universal Authenticator leverages Oracle Advanced Authentication (OAA) to extend device authentication with MFA, strengthening your organizations security framework, and preventing phishing attacks.

Key Oracle Universal Authenticator Features and Use Cases

The Oracle Universal Authenticator (OUA) key features and use cases are as follows.

Universal Access for Devices With MFA or Passwordless

Use one credential for device login. In this release Microsoft Windows machines are supported.

Seamless Integration With Oracle Access Management

Out of the box integration with Oracle Access Management (OAM) as a single authenticator for device logins, bypassing the need for users to use their Microsoft Entra ID for Windows device login.

Consistent Experience Across Operating Systems and Devices

Oracle Universal Authenticator utilizes open standards for authentication, ensuring seamless operation across different operating systems and devices. Provides a consistent user experience with platform-agnostic design.

Unified Single-Sign On (SSO) Experience

One set of credentials grants access to all OAM protected web-based applications, improving productivity and user satisfaction with less time spent on login procedures and password recovery.

Robust MFA at Device Level

Multi-Factor Authentication (MFA) options to step up authentication at device level. Factors supported include:

- TOTP (Time-based One Time Passcode) with a Mobile Authenticator application
- Push Notifications with Oracle Mobile Authenticator
- One Time Passcode (OTP) with SMS, Email, and Yubico YubiKey

Convenient Passwordless Options

Sign in to devices using passwordless login within configurable time windows.

Centralized Administration Console

Administrators can manage and monitor user and device registrations from a single web-based administration console, ensuring consistency across the enterprise. Easily enforce and update security policies and access rights, improving compliance and control.

Self-Service Portal

A user-friendly self-service portal, accessible anytime, leading to higher user adoption rates. Allows users to independently set up and manage their device MFA options, reducing administrative overhead.

For more information on these use cases, and step by step tutorials, see [Use Cases](#).

System Architecture and Components

Oracle Universal Authenticator (OUA) contains the following components.

Oracle Universal Authenticator Client Application

The Oracle Universal Authenticator client application allows end-users to login to their device using their Oracle Access Management (OAM) credentials with step-up Multi-Factor Authentication (MFA), or alternatively using passwordless login.

Oracle Access Management

Oracle Access Management is used by Oracle Universal Authenticator as the identity provider (IDP) for device logins.

Oracle Advanced Authentication

Oracle Advanced Authentication provides multi-factor authentication and passwordless login for devices.

Device Runtime Support Service

The Device Runtime Support Service (DRSS) is installed as a microservice during the deployment of Oracle Advanced Authentication (OAA). It runs as a pod in the Kubernetes cluster alongside other OAA pods.

DRSS is responsible for accepting connections from the Oracle Universal Authenticator client application, validating the user's Oracle Access Management credentials, logging the user into Oracle Access Management, and performing multi-factor authentication with OAA.

Oracle Adaptive Risk Management

Oracle Adaptive Risk Management (OARM) is installed as part of the Oracle Advanced Authentication (OAA) deployment. It aggregates risk data associated with users and user activities, analyzes and evaluates business risks posed by users and their activities and provides advice to be acted on to mitigate them.

Microsoft Entra ID Domain

For Microsoft Windows devices, Oracle Universal Authenticator (OUA) requires the device to be joined to a Microsoft Entra Domain Services managed domain. When a user logs into Microsoft Windows using the OUA client application and their Oracle Access Management credentials, the user is automatically logged into the domain.

Single-Sign On Browser Extension

The Single Sign-On (SSO) Browser Extension allows Microsoft Windows users authenticated with Oracle Universal Authenticator, to login to protected web applications automatically using SSO.

Administration Console

The Administration Console allows administrators to administer Oracle Universal Authenticator (OUA). Administrators can enable or disable OUA, view and manage registered devices, allow or disable users on a registered device, or block devices. It also allows administrators to set allowed authentication factors for OUA, restrict access based on required LDAP user groups, and perform device software management tasks.

Self-Service Portal

The Self-Service Portal allows users to manage their devices and factors used with Oracle Universal Authenticator. A user can view and manage their registered devices, can enable or disable a device, or rename a device to a friendly name. Users can also manage their factors for multi-factor authentication (MFA) that are configured in Oracle Advanced Authentication.

How Oracle Universal Authenticator Works?

The following shows a typical scenario on how Oracle Universal Authenticator works for device authentication.

1. After starting or unlocking the Microsoft Windows device, the user is prompted to sign in to Windows using Oracle Universal Authenticator (OUA). The user enters their Oracle Access

Management (OAM) username and password. If this is the first time the user has logged into this device with OUA they will also be prompted to enter their Windows credentials.

 Note:

Entering Windows credentials is not required for subsequent logins. It is for first time device registration only.

2. The user credentials are passed to the Oracle Universal Authenticator microservice (DRSS). DRSS validates the user's Oracle Access Management (OAM) credentials, and logs the user into OAM. If this is the first time this user has logged on from this device, the device is registered.
3. The user will be asked to authenticate with a second factor. If the user has multiple authentication methods configured, they can select any option available. Multi-Factor Authentication (MFA) options include:
 - TOTP (Time-based One Time Passcode) with a Mobile Authenticator application
 - Push Notifications with Oracle Mobile Authenticator
 - One Time Passcode (OTP) with SMS, Email, and Yubico YubiKey
4. If the credentials and second factor are successfully verified by Oracle Universal Authenticator, the end user is successfully logged into Windows.
5. The end user accesses an on-premises or cloud based application that is protected using OAM. As the user is already authenticated using Oracle Universal Authenticator, the end user gains access seamlessly without the need to enter any further credentials.

 Note:

If the application is protected further using Oracle Advanced Authentication with MFA, users must provide an additional factor for access.

6. For any subsequent Windows logins, as the device is registered, the end user will only need to enter their Oracle Access Management credentials and any additional second factor credentials. Windows credentials are no longer required. After successful verification of OAM credentials and second factor, the user is automatically logged into Windows using the end user's Windows credentials.

 Note:

An end user can login without entering their OAM password, using only a second factor, if the end user attempts to login again during a specified time window. This is called passwordless login. See [Configuring Passwordless Login using Configurable Challenges](#).

For more information on the above use cases, see [Use Cases](#).

Part II

Installing Oracle Universal Authenticator

Oracle Universal Authenticator requires the following installations:

- Oracle Advanced Authentication with Oracle Universal Authenticator enabled.
- Oracle Universal Authenticator client application installed on the devices.

This section contains the following chapters:

- [Installing Oracle Advanced Authentication](#)
- [Installing the Oracle Universal Authenticator Client Application](#)

Installing Oracle Advanced Authentication

Oracle Advanced Authentication must be installed on a Kubernetes cluster with Oracle Universal Authenticator enabled.

Installing Oracle Advanced Authentication

If you are performing a new installation of Oracle Advanced Authentication (OAA), you must install with the `common.deployment.mode=OUA` parameter set in the `installOAA.properties` file.

For detailed instructions on installing Oracle Advanced Authentication with Oracle Universal Authenticator, see [Installing OAA, OARM and OUA](#).

Upgrading an Existing Oracle Advanced Authentication Deployment

If you have an existing Oracle Advanced Authentication (OAA) deployment, you must upgrade it to include Oracle Universal Authenticator.

For details on upgrading, see [Upgrading OAA, OARM, and OUA](#).

Installing the Oracle Universal Authenticator Client Application

The sections below describe how to install the Oracle Universal Authenticator client application on Microsoft Windows devices.

- [Performing Prerequisite Tasks](#)
- [Installing the Client Application](#)
- [Activating the Single Sign-On Browser Extension](#)

Performing Prerequisite Tasks

Before following this section, you must have deployed Oracle Advanced Authentication with Oracle Universal Authenticator enabled. See, [Installing Oracle Advanced Authentication](#) .

The sections below show the prerequisite configurations that must be performed by the Administrator before installing the Oracle Universal Authenticator client application on Microsoft Windows devices.

Prerequisite Configurations for Microsoft Entra Domain

A Microsoft Entra Domain is required for use with Oracle Universal Authenticator. The following prerequisites are required:

- Users using Oracle Universal Authenticator must exist in the Microsoft Entra Domain.
- In order to seamlessly access local resources protected by Active Directory on your local network, a hybrid join with Microsoft Entra Domain may be necessary.



Note:

This documentation does not contain instructions on how to setup a Microsoft Entra Domain, LDAP directories, or user accounts. Administrators must have a working knowledge of Microsoft Entra before using Oracle Universal Authenticator.

Prerequisite Configurations for Microsoft Windows Clients

The following prerequisites are required for Microsoft Windows clients to login with Oracle Universal Authenticator. These are required for any Microsoft Windows computer where the Oracle Universal Authenticator client application will be installed:

- A computer running Microsoft Windows 10 or 11.
- The Microsoft Windows computer must have joined the Windows domain in Microsoft Entra.
- The Microsoft Windows user who wants to login via Oracle Universal Authenticator must be able to login to the Windows domain with a valid username and password.
- You must be logged in as a local Administrator user to install the Oracle Universal Authenticator client application software on the computer.
- The following must be installed on the Windows computer:
 - [Visual Studio C++ runtime libraries](#)
 - [.NET 4.7.2 framework](#)
- If Windows [automatic login](#) has been enabled, then it must be disabled before installing Oracle Universal Authenticator.

Prerequisite Configurations for the SSO Browser Extension

The following browsers are certified with the Oracle Universal Authenticator SSO Browser Extension:

- Chrome v88+
- Firefox v113+

- Microsoft Edge v92+

 Note:

If you intend to use Firefox you should install Firefox prior to installing the Oracle Universal Authenticator client application. If you choose to install Firefox afterward, you will need to reinstall the Oracle Universal Authenticator client application for the Firefox SSO browser extension to be installed. This is not applicable to Chrome and Edge browsers.

If your organization has group policy controls which specify the extensions that can be installed in the browser, the Microsoft Windows Enterprise Administrator must add the extension ID of the OUA SSO Browser Extension to the policy. The extension ID for Chrome and Microsoft Edge is as follows:

- `dpmpkcofhbmhlhagnklehljiagfhegni`

 Note:

For Firefox no extension ID is required because the signed Firefox extension file is provided with the Oracle Universal Authenticator software.

Prerequisite Configurations for Oracle Access Management

The Microsoft Windows user must have a user account in the User Identity Store used by Oracle Access Management (OAM). The user must be able to login with Single Sign-On (SSO) to an application protected with OAM.

Installing the Client Application

The Oracle Universal Authenticator client application must be installed on any Windows device that will use Oracle Universal Authenticator to log in. How the installer or application is deployed on the client will depend on how your organization normally rolls out applications.

The installer can run in GUI mode, or in silent mode. Regardless of how the Oracle Universal Authenticator application or installer is deployed, you must login as a local Administrator user to run the installer.

Before running the Oracle Universal Authenticator client application installer, you must know the following information about the DRSS endpoint, for example `https://oaa.example.com:443/oa-drss:`

- **Host:** <DRSS_HOSTNAME>, for example `oaa.example.com`.
- **Port:** <DRSS_PORT>, for example `443`.
- **User name:** <DRSS_APIUSER>, for example `OAA_INSTALL_OAA_DRSS`.
- **Password:** <DRSS_APIKEY>.

**Note:**

For details on how to find the required DRSS information, see [Print Deployment Details](#).

Downloading the Oracle Universal Authenticator Client Application Software

Follow the instructions below to download the Oracle Universal Authenticator client application software:

1. Download the `Oracle_Universal_Authenticator_<version>.zip` from [Oracle Software Delivery Cloud](#). Alternatively, it can be downloaded from the location referenced in document ID 2723908.1 on [My Oracle Support](#).
2. Extract the zip file to a working directory `%WORKDIR%` on the installation host. The `Oracle Universal Authenticator.msi` will be extracted.

Running the Installer in GUI Mode

Follow the instructions below to install the Oracle Universal Authenticator client application in GUI mode:

1. Double click on the `Oracle Universal Authenticator.msi`.
2. In the **Welcome** screen, select **Next**.
3. In the **DRSS Server Endpoint Setup** screen, enter the following information and click **Next**:
 - **Server:** `<DRSS_HOSTNAME>`
 - **Endpoint:** `/oaa-drss`
 - **Port:** `<DRSS_PORT>`
 - **API User:** `<DRSS_APIUSER>`
 - **API Key:** `<DRSS_APIKEY>`
4. In the **Setup Type** screen, select **Complete** and click **Next**.
5. In the **Ready to Install the Program** screen, click **Install**.
6. In the **InstallShield Wizard Complete** screen, click **Finish**.
7. In the **Oracle Universal Authenticator Installer Information** screen, select **Yes** to restart the system.

Running the Installer in Silent Mode

Follow the instructions below to install the Oracle Universal Authenticator client application in silent mode:

1. Start a **Command Prompt** selecting **Run As Administrator**.
2. Inside the command prompt run the following to set the permissions:

```
powershell.exe Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

3. Inside the command prompt, run the installer as follows:

```
Msiexec.exe /i "%WORKDIR%\Oracle Universal Authenticator.msi"  
HOST=<DRSS_HOSTNAME> ENDPOINT="/oaa-drss" PORT=<DRSS_PORT>  
APIUSER=<DRSS_APIUSER> APIKEY=<DRSS_APIKEY> /qn
```

 Note:

The /qn flag runs the installer in silent mode. If /qn is not used the GUI will launch and the Administrator will need to navigate through the screens as per **Running the Installer in GUI Mode**.

4. Restart Windows.

Activating the Single Sign-On Browser Extension

The Single Sign-On (SSO) browser extension is installed in the browser during the installation of the Oracle Universal Authenticator client application. When the user starts the browser for the first time after the installation, they will be notified that the Oracle Universal Authenticator extension has been installed and should click the **Okay** button.

Firefox users need to set the permissions of the extension to access data from all websites:

1. Click the **Extensions** icon in the top right of Firefox.
2. Click the ellipsis button next to the Oracle Universal Authenticator extension and select **Manage**.
3. Click the **Permissions** tab.
4. Under **Optional permissions for added functionality**, select the toggle button to enable **Access your data for all websites**.

Part III

Performing Device Authentication with Oracle Universal Authenticator

Once the Oracle Universal Authenticator client application is installed, the end user can log into Microsoft Windows using the Oracle Universal Authenticator option.

When the Oracle Universal Authenticator login is selected for the first time, the user is required to enter both their Oracle Access Management (OAM) credentials and their Windows credentials, and any second factor credentials previously configured. This is required so Oracle Universal Authenticator can configure the tokens it needs for successful operation.



Note:

Before using Oracle Universal Authenticator, users must have at least one factor configured in the Self-Service Portal:

- Administrators should refer to the following documentation for onboarding users and their factors: [Onboarding Users](#)
- Users can manage their factors using the Self-Service Portal: [Managing Factors in the Self-Service Portal](#)

Once the initial logins are successful and the user and device is registered, the user can login to OAM protected applications and Windows applications without the need to enter any further credentials.

For any subsequent Windows login, if the same user selects to login with Oracle Universal Authenticator, the user will only be asked to enter their OAM credentials, and a second factor credential. Once logged in, the user can login to OAM protected applications and Windows applications without the need to enter any further credentials.

This chapter contains the following topics:

- [First time login to Microsoft Windows with OUA](#)
- [Subsequent login to Microsoft Windows with OUA](#)
- [Accessing Applications Protected with SSO](#)
- [Offline Login](#)



Note:

For more detailed information and step by step tutorials, see [Usecases](#).

First Time Login to Microsoft Windows with OUA

The steps for a user to login to Windows with Oracle Universal Authenticator for the first time are as follows:

1. At the Windows login screen select Oracle Universal Authenticator.
2. The user will be asked to enter their username. In the Username field, enter the OAM username and click the arrow.
3. As the user has not previously registered with Oracle Universal Authenticator, the user is prompted to enter their OAM Password, and their Windows Username and Windows Password. Enter the required credentials and click the arrow.

Note:

The Windows username can take the format of `azuread\<username>` for Azure users, or `.\<username>` for local Windows users.

4. The user is prompted to enter a One-Time Passcode (OTP) for a second factor. If the user has a default factor set, they will be prompted to enter the OTP for that factor. If no default factor is set, and the user has multiple factors configured, the user is prompted to choose which factor to use. Enter the OTP and click the arrow.

Note:

If using Push Notifications, the user will be asked to approve the login on their mobile device.

5. If the login is successful, the Windows desktop appears.

Subsequent Login to Microsoft Windows with OUA

The instructions for a user to login to Windows with Oracle Universal Authenticator for subsequent logins are as follows:

1. At the Windows login screen select Oracle Universal Authenticator.
2. The user will be asked to enter their username. In the Username field, enter the OAM username and click the arrow.
3. The user is prompted to enter their OAM Password. Enter the required password and click the arrow.
4. The user is prompted to enter the One-Time Passcode (OTP) for a second factor. If the user has a default factor set, they will be prompted to enter the OTP for that factor. If no default factor is set, and the user has multiple factors configured, the user is prompted to choose which factor to use. Enter the OTP and click the arrow.

5. If the login is successful, the Windows desktop appears.

**Note:**

An end user can login without entering their OAM password, using only a second factor, if the end user attempts to login again during a specified time window. This is called passwordless login. See [Configuring Passwordless Login using Configurable Challenges](#).

Accessing Applications Protected with SSO

Once a user is logged into Windows with Oracle Universal Authenticator, users can access the following applications using Single Sign-On (SSO) without being prompted for user credentials:

- Browser-based OAM protected web applications
- Microsoft applications, such as Office 365 and Outlook 365.
- Microsoft applications integrated with Azure SSO.

**Note:**

These application uses standard Azure SSO, not Oracle Universal Authenticator SSO.

Offline Login

Offline login allows users to continue to login to their device with Oracle Universal Authenticator if any of the following scenarios occur:

- Any part of the Oracle Universal Authenticator infrastructure is unavailable. For example, Oracle Access Management (OAM) or Oracle Advanced Authentication is unavailable due to a system outage or network issue.
- Login is denied due to the OAM user account being locked, the user's OAM password expired, or if a mandatory password change is required for the OAM user.

If any such scenario occurs, Oracle Universal Authenticator allows the user to login to Windows using their OAM credentials until the situation is resolved. In offline mode, the user will not be automatically logged into applications using single-sign on.

For example:

1. The users selects Oracle Universal Authenticator at the Windows login screen.
2. The user enters their OAM credentials.
3. The user receives an error message related to the reason that login is denied.
4. The user enters the password for their OAM user and clicks the arrow.
5. If login is successful, the Windows desktop appears.

6. Once the situation is resolved, the user can logout of Windows, then login again using their OAM credentials.

The sections below outline the error messages received in each scenario when login is denied:

Part of the Oracle Universal Authenticator Infrastructure Is Down

System is offline. Please provide your password to proceed. Some features of your Login with Oracle will not be available. To restore all features, please logout and login again when system is online.

The OAM User Account Is Locked

Your account is locked. Please provide your password to proceed. Some features of your Login with Oracle will not be available. To restore all features, you need to logout and login again after resolving your account status.

The OAM User Password is Expired

The following message is shown when password management is enabled. See, [Configuring Password Management](#):

Your password has expired. Click OK to go to the password management service, or click Cancel to continue logging in, which may result in some features being unavailable.

The following message is shown when password management isn't enabled:

Your password has expired. Please provide your password to proceed. Some features of your Login with Oracle will not be available. To restore all features, you need to logout and login again after resolving your account status.

Mandatory OAM User Password Change is Required

You must change your password. Please provide your password to proceed. Some features of your Login with Oracle will not be available. To restore all features, you need to logout and login again after resolving your account status.

Part IV

Administering Oracle Universal Authenticator

Oracle Universal Authenticator (OUA) administrators can perform administration tasks via the Oracle Advanced Authentication (OAA) Administration Console (<https://<AdminUrl>>).



Note:

For details on the <AdminURL>, see Print Deployment Details.



Note:

If the Administrator is accessing the Administration Console from a device with Oracle Universal Authenticator installed, the Administrator will need to disable the SSO Browser Extension first. When accessing the console, you will then be redirected to Oracle Access Management and asked to enter your administrator credentials and login.

The Administration console allows you to perform the following tasks:

- Enable/Disable Universal Authenticator.
- Restrict Oracle Universal Authenticator availability for specific LDAP user groups.
- Configure allowed authentication factors for Oracle Universal Authenticator.
- Manage Devices:
 - List and search all devices
 - View details of a device
 - View registered users for a device
 - Enable/Disable a specific user using a device
 - Enable/Disable a device for all users
- Perform Device Software Management tasks.

The following administration tasks can be performed by REST API's only:

- Configure passwordless login using configurable challenges.
- Configure password management.

This chapter contains the following topics:

- [Enabling and Disabling Oracle Universal Authenticator](#)
- [Restricting Oracle Universal Authenticator to Specific User Groups](#)
- [Configuring Allowed Authentication Factors](#)
- [Managing Devices](#)
- [Device Software Management](#)

- [Configuring Passwordless Login using Configurable Challenges](#)
- [Configuring Password Management](#)

More information on common Administration tasks can be found in [Performing Administration Tasks in Oracle Universal Authenticator](#).

Enabling and Disabling Oracle Universal Authenticator

Oracle Universal Authenticator is enabled by default.

The following steps show how to disable Oracle Universal Authenticator in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Select **Universal Authenticator** in the left-hand navigation menu.
3. In the **Universal Authenticator** home page, select **Disable Universal Authenticators**.
4. To enable Universal Authenticator again, select **Enable Universal Authenticators**.

Restricting Oracle Universal Authenticator to Specific User Groups

Administrators can choose to restrict the users who can login with Oracle Universal Authenticator, to specific user LDAP groups. For example, you may only want to enable Oracle Universal Authenticator for users in the HR and Finance LDAP groups.

The following sections describe common LDAP group administration tasks:

- [Adding LDAP Groups](#)
- [Editing LDAP Groups](#)
- [Deleting LDAP Groups](#)

Adding LDAP Groups

By default, when Oracle Universal Authenticator is enabled, users in all LDAP groups can login using Oracle Universal Authenticator with their registered device(s).

The following steps show how to restrict Oracle Universal Authenticator to specific LDAP user groups in the OAA Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Under **Universal Authenticator** in the left-hand navigation menu, select **User Groups**.
3. In the **User Groups** page, select **Enable for LDAP Group**.
4. In the **Enable for LDAP Group** field, enter the name of the LDAP group, for example **HR**.
5. Click **Add**.

6. The LDAP group added appears in the **User Groups** page.

Editing LDAP Groups

The following steps show how to edit LDAP user groups for Oracle Universal Authenticator in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Under **Universal Authenticator** in the left-hand navigation menu, select **User Groups**.
3. In the **User Groups** page, select the **Edit** button for the required LDAP group.
4. Make any required changes and click **Save**.

Deleting LDAP Groups

The following steps show how to delete an LDAP user group for Oracle Universal Authenticator in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Under **Universal Authenticator** in the left-hand navigation menu, select **User Groups**.
3. In the **User Groups** page, select the **Delete** button for the required LDAP group.
4. Confirm the group removal by selecting **Remove**.

Configuring Allowed Authentication Factors

You can choose the authentication factors that can be used for Oracle Universal Authenticator. By default, all factors are enabled.

Note:

Administrators should be aware of the following:

- Security Questions and FIDO2 are not enabled by default as they are currently not supported for Oracle Universal Authenticator.
- For OMA Push Notifications to be used with Oracle Universal Authenticator, the property `bharosa.uio.default.challenge.type.enum.ChallengeOMAPUSH.retrycount` must be set to the value 50. For details how to set this parameter, see, [Configuration Properties for OAA](#).

The following steps show how to configure the authentication factors for Oracle Universal Authenticator in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Select **Manage Integration Agents** in the left-hand navigation menu.

3. Select the name of your Oracle Universal Authenticator agent.

 Note:

The agent name is the value passed to `oua.tapAgentName` in the `installOAA.properties`. See, [OAM Requirements for Oracle Universal Authenticator](#).

4. Click the **Assurance Level** displayed.
5. In the Assurance Level page, under **Uses**, all the factors that are enabled are displayed.
6. To disable a factor, click the checkbox for the factor you want to disable and click **Save**.
7. To enable a disabled factor, click the checkbox for the factor you want to enable and click **Save**.

Managing Devices

The Administration Console allows you to manage devices registered with Oracle Universal Authenticator in the following ways:

- List and search all devices
- View details of a device
- View registered users for a device
- Enable/Block a specific user using a device
- Enable/Disable a device for all users

The following sections describe common device administration tasks:

- [List and Search Devices](#)
- [View Details of a Device](#)
- [Enabling or Disabling a User for a Device](#)
- [Enabling or Disabling a Device for all Users](#)

Listing and Searching Devices

You can list or search for devices registered for use with Oracle Universal Authenticator.

The following steps show how to view all registered devices:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Under **Universal Authenticator** > **Device Management** in the left-hand navigation menu, select **Devices**. All registered devices will be displayed by default, sorted by most recently used.
3. If you need to search for a specific device, in the **Manage Devices** screen, enter the name of the device to search for. You can also filter the search by selecting any of the following buttons:
 - **Status Enabled** : List only enabled devices

- **Status Disabled** : List only disabled devices
- **Status Unreachable**: List only unreachable devices. Indicates that a device has not sent a heartbeat within the default two hours, or the time period configured for `echo.elapsed.time`. See, Configuration Properties for OAA.

 Note:

A device can be considered unreachable in the following circumstances:

- The device is turned off
- The monitoring agent on the device is not working properly or is not turned on
- There is a network issue and the device cannot connect with DRSS

- **Status Needs attention**: List only devices that need attention. Indicates that the software version on the device does not match the published version in [Device Software Management](#).

Viewing Details of a Device

The following steps show how to view the details of a device:

1. In the **Manage Devices** screen, select the ellipsis next to the required device. In the drop-down menu, select **View details**.
2. The Device details screen shows the following information:
 - The Operating System (OS) of the device
 - If the device is enabled or disabled
 - The user who registered the device
 - The date the device was registered
 - The user who last logged in on the device
 - The date of the last login
 - The Oracle Universal Authenticator (OUA) software version installed on the device
 - The date the OUA software version was installed on the device
 - The user(s) who the device is registered to, the status of the user(s) assigned to the device (enabled or disabled), and the date of last login
 - The device history
 - The OUA software upgrade history

Enabling or Disabling a User for a Device

In the Device details screen you can enable or block a user registered to a device.

Enabling a user for a device allows that user to login using Oracle Universal Authenticator from that device. Blocking a user prevents that user from logging in with Oracle Universal Authenticator from that device.

The following steps show how to enable or block a user registered to a device:

1. In the Device details screen, under the **Registered to** section, select **Enable User** or **Block User**.
2. In the confirmation screen, select to confirm to **Enable** or **Block** the user from that device.

**Note:**

If an Administrator blocks a user from a device, the user will not see the device in the Self-Service Portal.

Enabling or Disabling a Device for all Users

In the Device details screen you can enable or block a device for all users.

Enabling a device allows all users registered to that device, to login using Oracle Universal Authenticator from that device. Blocking a device prevents all users registered to that device, from logging in with Oracle Universal Authenticator from that device.

The following steps show how to disable or enable a device for all users:

1. In the Device details screen, from the **Actions** menu, select **Enable device** to enable a device, or **Disable device** to disable the device.
2. In the confirmation screen, select to confirm to enable or disable the device.

**Note:**

If an Administrator disables a device, the user will not see the device in the Self-Service Portal.

Device Software Management

The Administration console allows you to control the roll out and upgrade of new versions of the Oracle Universal Authenticator client application.

When a new version of the Oracle Universal Authenticator client application is available, the Administrator can upload it using the Administration console. When the new version is published, devices will automatically pull down the new version and install it.

**Note:**

The SSO Browser extension will get updated automatically by the browser when new versions are available and happens separately to the Device Software Management process.

The Administration console allows you to perform the following tasks for the Oracle Universal Authenticator client application software:

- View the software versions uploaded

- Upload new versions of the software
- Publish the version of the software to be downloaded by devices
- View devices where specific software versions are applied
- Rollback the published version of the software to the previous version
- Freeze a software version to prevent it being downloaded
- Delete versions of software no longer required

The following sections describe common device software management tasks:

- [Viewing Device Software](#)
- [Adding New Device Software](#)
- [Managing Device Software](#)

Viewing Device Software

The following steps show how to view details of device software uploaded in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted..
2. Under Universal Authenticator in the left-hand navigation menu, select **Device Software Management**. All versions of the Oracle Universal Authenticator client application software uploaded are displayed by default, sorted by the most recent. The version of the software that is currently published is marked as **PUBLISHED**.
3. If you need to search for a specific version, in the **Device Software Management** screen, enter the version to search for. You can also filter the search by selecting any of the following buttons:
 - **Added Today**: List only software added today
 - **Added This Week**: List only software added this week
 - **Status Published**: List only published software
4. To see the devices that are currently using a specific version of the software, click the number next to **devices**.

Adding New Device Software

The following steps show how to upload new Oracle Universal Authenticator client software in the Administration console:

1. Login to the Administration console (<https://<AdminURL>>). Enter the user credentials when prompted.
2. Under Universal Authenticator in the left-hand navigation menu, select **Device Software Management**.
3. Click **Add new software**.
4. In the **Add new software** window, select the `Oracle_Universal_Authenticator_<version>.zip` file to upload, or drag the file to the **Upload or drag and drop** field.

 Note:

Administrators should be aware of the following:

- When you download a new version of the software you must not rename the zip file otherwise the software will fail to load. New software versions can be found by referring to the document ID 2723908.1 on [My Oracle Support](#).
- You can only upload software that is newer than the last version uploaded. Any attempt to upload an earlier version will fail.

5. Click **Upload** to upload the file without publishing, or **Upload and publish** to upload the file and immediately publish it.

 Note:

Publishing means the new software version is available for devices to automatically pull down and install the new Oracle Universal Authenticator client application software.

6. The new software version will appear at the top of the list. If **Upload and publish** was selected, the software shows as **Published**.

Administrators should be aware of the following:

- Devices check for new software every 12 hours by default. This can be customized using the `oua.drss.lcm.pollingFrequency` property. See, Configuration Properties for OAA.
- Upgrades are quick and there will be minimal impact on the SSO experience.
- If the device upgrade or rollback process is interrupted due to system restart, the OUA login screen might not show up immediately in the subsequent login. If this occurs it is recommended to login using a local administrator user and then wait for the OUA software to be upgraded to the published version. This can be checked in the **Add or Remove Programs** under Microsoft Windows **System Settings**. Once the version gets upgraded or rolled back, logout or restart. The OUA login screen should then appear.

Managing Device Software

The following sections show how to manage Oracle Universal Authenticator client software in the Administration console.

Rollback a software version

To rollback the current published software version to the previous version:

1. In the **Device Software Management** screen, click the ellipsis next to the version of the published software you wish to rollback.
2. From the drop-down menu select **Rollback**.
3. In the **Rollback software** window, select **Confirm** to rollback the software.
4. The previous version of the software listed in the **Device Software Management** screen will become the **Published** version.
5. Devices will automatically download and install the new published version of the Oracle Universal Authenticator client application software.

Freezing a software version

Freezing a software version prevents devices who are not currently running that published version from downloading it and installing it. Devices that are currently running that version will continue to use that version. Freezing a software version is useful if, for example, Administrators want to test new software on a few devices and then freeze it while testing takes place.

Freezing a software version prevents you from publishing a new version of the software and prevents devices downloading any other version of the software. Once software is unfrozen, a device will download the latest published software if it is not currently on that version.

1. In the **Device Software Management** screen, click the ellipsis next to the version of the published software you wish to freeze.
2. From the drop-down menu select **Freeze**.
3. In the **Freeze software** window, select **Freeze** to freeze the software.
4. The software version will be marked as **Frozen**.
5. To unfreeze a version of the software, repeat the steps above but select **Unfreeze**.

Deleting a software version

Deleting a software versions removes it from the list. A software version can only be deleted if no devices are using that version.

To delete a software version:

1. In the **Device Software Management** screen, click the ellipsis next to the version of the software you wish to delete.
2. From the drop-down menu select **Delete**.
3. In the **Delete software** window, select **Confirm** to delete the software.

Configuring Passwordless Login using Configurable Challenges

Configurable Challenges is a feature of Oracle Universal Authenticator (OUA) that allows passwordless login within a configurable time window. Administrators can customize the methods of second factor authentication that are allowed to use passwordless login, and the duration of the time window.

For example, when a user logs into their device, they login with their OAM credentials, followed by authentication using a second factor. With configurable challenges a user can skip entering their OAM password if they last logged in, or performed a second factor only login, within a specified time window.

In order to configure configurable challenges, administrators can set the following parameters within Oracle Advanced Authentication:

Parameter	Default Value	Description
<code>oua.drss.skipPrimaryAuthDurationWithLastFullAuth</code>	1800 seconds (30 minutes)	Specifies the time duration from the last full OAM login. If the last full OAM login is within this time duration, the user will not be prompted for their OAM password, and will be allowed to authenticate using only the second factor. Once the duration elapses, the user will be prompted to enter their full OAM credentials, followed by a second factor.
<code>oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth</code>	600 seconds (10 minutes)	Specifies the time duration from the last successful second factor only login time. If the user performed a second factor only login within this time duration, the user will not be prompted for their OAM password, and will be allowed to authenticate using only the second factor. When their duration elapses, the user will be prompted for their OAM credentials, followed by a second factor.

Parameter	Default Value	Description
<code>oua.drss.skipPrimaryAuthFactorTrustLevel</code>	3	Specifies the trust level value for skip password rule evaluation. The trust level determines which factors are allowed to perform a passwordless login within the <code>oua.drss.skipPrimaryAuthDurationWithLastFullAuth</code> and <code>oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth</code> time periods. The default trust levels are as follows: - Trust Level 1 = SMS Challenge - Trust Level 2 = Yubico Yubikey TOTP, OMA TOTP - Trust Level 3 = Email Challenge - Trust Level 4 = Push Notification Challenge For example, if <code>TrustLevel=3</code>, then all those factor assigned level 3 or higher are allowed to perform passwordless login. Administrators can change the trust level for individual factors using the <code>bharosa.uio.default.challenge.type.enum.{FACTOR_KEY}.oua.trustLevel</code> parameters outlined in the rows below.

Note

:

FIDO 2 and Security Question challenge is not currently supported with Oracle Universal Auth

Parameter	Default Value	Description
bharosa.uio.default.challenge.type. enum.ChallengeSMS.oua.trustLevel	1	Sets the trust level for the SMS Challenge.
bharosa.uio.default.challenge.type. enum.ChallengeOMATOTP.oua.trustLevel	2	Sets the trust level for the OMA TOTP Challenge.
bharosa.uio.default.challenge.type. enum.ChallengeYubicoOTP.oua.trustLevel	2	Sets the trust level for the Yubikey Yubico OTP Challenge.
bharosa.uio.default.challenge.type. enum.ChallengeEmail.oua.trustLevel	3	Sets the trust level for the Email Challenge.
bharosa.uio.default.challenge.type. enum.ChallengeOMAPUSH.oua.trustLevel	4	Sets the trust level for the OMA Push Challenge.
oua.drss.allowPrimaryAuthDuringMFAOnly	true	Determines whether the user is given the option to login with their OAM password during a second factor only login.

For details on how to set these parameters using REST API's, see **Configuration Properties for OUA** in Configuration Properties for OAA.

The following examples show the authentication flow based on the default values for the above parameters:

Example 1:

- A user logs in at 9 AM with their OAM credentials, and uses the Email challenge as a second factor to authenticate.
- The user locks their machine at 9.15 AM.
- The user unlocks their machine at 9.20 AM and enters their OAM username.
- The user did not authenticate with only a second factor in the last 10 minutes, (oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth=10).
- The user did however perform a full login with their OAM credentials 20 minutes ago, which is inside the 30 minute window (oua.drss.skipPrimaryAuthDurationWithLastFullAuth=30).
- The user is therefore allowed to use passwordless login using any registered second factor at trust level 3 or above (oua.drss.skipPrimaryAuthFactorTrustLevel=3), for example Email Challenge (bharosa.uio.default.challenge.type.enum.ChallengeEmail.oua.trustLevel=3) or Push Notification Challenge (bharosa.uio.default.challenge.type.enum.ChallengeOMAPUSH.oua.trustLevel=4).

Example 2

- A user logs in at 9 AM with their OAM credentials, and uses the SMS challenge as a second factor to authenticate.

- The user reboots their machine at 9.15 AM.
- The user attempts to login to their machine at 9.20 AM.
- The user enters their OAM username.
- The user did not authenticate with only a second factor in the last 10 minutes, (`oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth=10`).
- The user did however perform a full login with their OAM credentials 20 minutes ago, which is inside the 30 minute window (`oua.drss.skipPrimaryAuthDurationWithLastFullAuth=30`).
- The user is therefore allowed to use passwordless login using any registered second factor at trust level 3 or above (`oua.drss.skipPrimaryAuthFactorTrustLevel=3`), for example Email Challenge (`bharosa.uio.default.challenge.type.enum.ChallengeEmail.oua.trustLevel=3`) or Push Notification Challenge (`bharosa.uio.default.challenge.type.enum.ChallengeOMAPUSH.oua.trustLevel=4`). The user cannot use the SMS challenge again because that is at trust level 2 (`bharosa.uio.default.challenge.type.enum.ChallengeSMS.oua.trustLevel=2`).
- If the user does not have a registered factor at trust level 3 or above, they cannot perform a passwordless login and are asked to login with their full OAM credentials, and then authenticate with any registered second factor.

Example 3

- A user logs in at 9 AM with their OAM credentials, and uses the Push Notification challenge as a second factor to authenticate.
- The user locks their machine at 9.05 AM.
- The user unlocks their machine at 9.25 AM and enters their OAM username.
- The user did not authenticate with only a second factor in the last 10 minutes, (`oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth=10`).
- The user did however perform a full login with their OAM credentials 25 minutes ago, which is inside the 30 minute window (`oua.drss.skipPrimaryAuthDurationWithLastFullAuth=30`).
- The user is therefore allowed to use passwordless login and is only asked to authenticate with the Push Notification Challenge.
- The user locks their machine again at 9.30 AM.
- The user unlocks their machine at 9.32 AM and enters their OAM username.
- The user did authenticate with only a second factor in the last 10 minutes, (`oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth=10`).
- The user is therefore allowed to use passwordless login using any registered second factor at trust level 3 or above (`oua.drss.skipPrimaryAuthFactorTrustLevel=3`), for example Email Challenge (`bharosa.uio.default.challenge.type.enum.ChallengeEmail.oua.trustLevel=3`) or Push Notification Challenge (`bharosa.uio.default.challenge.type.enum.ChallengeOMAPUSH.oua.trustLevel=4`).
- The user authenticates with the Push Notification Challenge and locks their screen again at 9.40 AM.
- The user unlocks their screen again at 10 AM and enters their OAM username.

- The user did not authenticate using only a second factor in the last 10 minutes, (oua.drss.skipPrimaryAuthDurationWithLastMFAOnlyAuth=10, nor did they perform a full login with their OAM credentials in the last 30 minutes (oua.drss.skipPrimaryAuthDurationWithLastFullAuth=30).
- The user is therefore asked to login with their full OAM credentials, and then authenticate with any registered second factor.

Configuring Password Management

Administrators can configure password functionality so end users can change their Oracle Access Management password during Oracle Universal Authenticator (OUA) login. For example, if a user has forgotten a password, or if the password has expired or is about to expire, administrators can configure Oracle Universal Authenticator with the relevant links, so end users can perform a password reset.

Administrators can set the following parameters within the Oracle Advanced Authentication installation:

Parameter	Default Value	Description
oua.drss.password.reset.forgoturl		Specifies the URL where users can initiate the forgot password process. This is the URL accessed when users click the Forgot Password link during login with OUA. Through this URL, users will be guided to reset their password by utilizing the password reset mechanism configured for their account.
oua.drss.password.reset.url		Defines the URL where users can change their password. This is the URL accessed when users click the Change Password during login with OUA. Accessing this URL allows users to verify their identity, through mechanisms configured to create a new password for their account.

Parameter	Default Value	Description
oua.drss.password.reset.supportedBrowsers	chrome, firefox	Outlines the browsers supported by the system. When a forgot URL or reset URL is called from within OUA, a browser is opened.


Note:

In this release, only Google Chrome and Mozilla Firefox are supported.

If both browsers are installed, the system will prioritize using Chrome for optimal functionality. These browsers are required for the proper execution of this feature.

For details on how to set these parameters using REST API's, see **Configuration Properties for OUA** in Configuration Properties for OAA.



Note:

If these parameters are not set, the **Forgot Password** and **Change Password** links will not be visible to the end user during OUA login.

For details on the password functionality flow for end users, see [Using Password Management in Oracle Universal Authenticator](#).

Part V

Self-Service Portal

Oracle Universal Authenticator users can manage their devices and factors from the Self-Service Portal (<https://<SpuiURL>>).



Note:

For details on the <SpuiURL>, see Print Deployment Details.



Note:

If you have logged in to your device with Oracle Universal Authenticator, you will automatically be logged into the Self-Service Portal without the need to enter your Oracle Access Management credentials.

This chapter contains the following topics:

- [Managing Devices in the Self-Service Portal](#)
- [Managing Factors in the Self-Service Portal](#)

Managing Devices in the Self-Service Portal

The Self-Service Portal allows you to manage your factors used for multi-factor authentication (MFA) and device authentication in the following ways:

- Viewing your devices
- Enabling or disabling a device
- Renaming a device
- Viewing device details

The following sections describe the common factor management tasks:

- [Viewing All My Devices](#)
- [Enabling or Disabling a Device](#)
- [Renaming a Device](#)
- [Viewing Device Details](#)

Viewing All My Devices

The following steps show how you can view all your registered devices:

- In the left navigation menu, select **My Devices**. A list of all devices registered to the user will appear.

- Users can filter the search by selecting any of the following buttons:
 - **Status Enabled**: List only enabled devices
 - **Status Disabled** : List only disabled devices
 - **Registered Today**: List only devices registered today
 - **Registered This Week**: List only devices registered this week
 - **Registered Over a week ago**: List only devices registered over a week ago
 - **Last logged in Today**: List only devices that last logged in today
 - **Last logged in This week**: List only devices that last logged in this week
 - **Last logged in Over a week ago**: List only devices that last logged in over a week ago

Enabling or Disabling a Device

In the **My Devices** screen you can enable or disable a device registered to you.

Enabling a device allows you to login using Oracle Universal Authenticator from that device. Disabling a device prevents you from logging in with Oracle Universal Authenticator from that device.

The following steps show how to enable or a disable a device registered to you:

1. In the **My Devices** screen, select the ellipsis next to the required device. In the drop-down menu, select **Enable device** or **Disable device**.
2. In the confirmation screen, select to confirm to enable the device, or disable the device.



Note:

You can also enable or disable the device from the **View Details > Actions** menu.

Renaming a Device

When a device is registered, the device name assigned takes a basic format, for example Device1. In the Device details screen, you can rename a device to a user-friendly name.

The following steps show how to rename a device registered to you:

1. In the **My Devices** screen, select the ellipsis next to the required device. In the drop-down menu, select **Rename device**.
2. In the **Rename device** screen, enter the name you wish to rename the device to.
3. Click **Rename**.



Note:

You can also rename the device from the **View Details > Actions** menu.

Viewing Device Details

The following steps show how to view details of a device:

1. In the **My Devices** screen, select the ellipsis next to the required device. In the drop-down menu, select **View details**.
2. The Device details screen shows the following information:
 - The date the device was registered
 - The date of the last login
 - The device history
 - Whether the device is enabled or disabled

Note:

You can also enable or disable the device, or rename the device, from the **Actions** menu.

Managing Factors in the Self-Service Portal

The Self-Service Portal allows you to manage your factors used for multi-factor authentication (MFA) and device authentication in the following ways:

- Viewing configured factors
- Adding and configuring factors
- Enabling, disabling, and deleting factors
- Setting the default factor

The following sections describe the common factor management tasks:

- [Viewing Configured Factors](#)
- [Adding Factors](#)
- [Enabling, Disabling, or Deleting Factors](#)
- [Setting the Default Factor](#)

Viewing Configured Factors

The following steps show how to view the factors configured in the Self-Service Portal:

1. In the left navigation menu, select **My Authenticators**.
2. On the **My Authenticators** page, for each of the factors registered, a corresponding challenge factor tile is displayed. For example, if the user is registered with Oracle Mobile Authenticator (OMA) and Email challenge factors, the corresponding tiles named **Oracle Mobile Authenticator** and **Email Challenge** are displayed.

Adding Factors

The following steps show how to add factors in the Self-Service Portal:

1. In the left navigation menu, select **My Authenticators**.
2. From the **Add Authentication Factor** drop-down menu, choose the factor you wish to add. The following factors can be added:
 - **Oracle Mobile Authenticator**
 - **Email Challenge**
 - **FIDO2 Challenge**
 - **Security Question Challenge**
 - **SMS Challenge**
 - **Yubico OTP Challenge**
 - **OMA Push Notification Challenge**

Note:

FIDO2 Challenge and Security Question Challenge are not currently supported with Oracle Universal Authenticator.

3. After selecting the factor you wish to add, you will be asked to enter the values outlined in the table below:

Factors	Values
Oracle Mobile Authenticator	Friendly Name: Specify a name. Key: A key is generated by Oracle Advanced Authentication. QR Code: Scan the QR code using the Oracle Mobile Authenticator, Google Authenticator, or Microsoft Authenticator application.
Email Challenge	Friendly Name: Specify a name. Email: Specify the required email.
FIDO2 Challenge	Friendly Name: Specify a name. Click Register and press the button on your FIDO2 device. The key is copied into Oracle Advanced Authentication.
Security Question Challenge	Question 1: Select a question to answer. Answer 1: Provide an answer the question. Repeat for the remaining Question and Answers.
SMS Challenge	Friendly Name: Specify a name. Phone: Specify the phone number.

Factors	Values
Yubico OTP Challenge	Friendly Name: Specify a name. Public ID: Type the Public ID. It must be the same as the Public ID (or serial) specified while configuring the Yubico OTP for your YubiKey device. Secret Key: Type the Secret Key. It must be the same as the Secret Key generated while configuring the Yubico OTP for your YubiKey device. Private ID: Type the Private ID. It must be the same as the Private ID generated while configuring the Yubico OTP for your YubiKey device.
OMA Push Notification Challenge	Scan the QR code, or manually register your device. In the Oracle Mobile Authenticator application enter the username and PIN displayed here.

For detailed step by step tutorials on configuring these factors, see:

- [Configuring Email Challenge in the Oracle Advanced Authentication Self-Service Portal](#)
- [Configuring Mobile Authenticator TOTP with Oracle Advanced Authentication](#)
- [Configuring Knowledge Based Authentication.](#)
- [Configuring FIDO2 with Oracle Advanced Authentication.](#)
- [Configuring YubiKey with Oracle Advanced Authentication.](#)
- [Configuring Mobile Authenticator TOTP with Oracle Advanced Authentication Self-Service Portal](#)
- [Configuring OMA Push Notification in the Oracle Advanced Authentication Self-Service Portal](#)

Enabling, Disabling, or Deleting Factors

The Self-Service Portal allows you to enable, disable, or delete a factor.

By default, when a factor is added it is enabled. Enabling a factor means it can be used with device authentication. Disabling a factor means it cannot be used with device authentication, but it can be enabled at a later point. Deleting a factor removes the factor entirely.

The following steps show how to enable, disable, or delete a factor in the Self-Service Portal:

1. In the left navigation menu, select **My Authenticators**.
2. For the factor you wish to enable, disable, or delete, select the ellipsis in the factor tile.
3. In the drop-down menu, select the operation you wish to perform, **Enable**, **Disable**, or **Delete**.
4. If you enabled or disabled a factor, the factor tile for your chosen factor will now display **Enabled** or **Disabled**. If you deleted a factor, the factor tile will disappear from the **My Authenticators** page.

Setting the Default Factor

The default factor is the factor used when performing device authentication. If no default factor is set, then the user is presented with a challenge choice based on the factors configured.

The following steps show how to set the default factor in the Self-Service Portal:

1. In the left navigation menu, select **My Authenticators**.
2. For the factor you wish to enable as the default factor, select the ellipsis in the factor tile.
3. In the drop-down menu, select **Set as Default**.
4. The factor tile for your chosen factor will now display **Default**.

Part VI

Use Cases

This section outlines some of the common usecases for Oracle Universal Authenticator.

This chapter contains the following topics:

- [Performing Administration Tasks in Oracle Universal Authenticator](#)
- [Configuring Factors for Device Authentication in the Self-Service Portal](#)
- [Configuring Device Authentication on Windows using Oracle Access Management and Multi-Factor Authentication](#)
- [Seamless Single Sign-On with Oracle Universal Authenticator](#)
- [Using Password Management in Oracle Universal Authenticator](#)

Performing Administration Tasks in Oracle Universal Authenticator

The following tutorial shows you some common tasks that can be performed by Administrators in the Administration Console for Oracle Universal Authenticator:

- [Performing Common Administration Tasks in Oracle Universal Authenticator](#)

Configuring Factors for Device Authentication in the Self-Service Portal

The following tutorials show how users can configure their factors for device authentication in the Self-Service Portal:



Note:

FIDO2 Challenge and Security Question Challenge are not currently supported with Oracle Universal Authenticator.

- [Configuring SMS Challenge in the Oracle Advanced Authentication Self-Service Portal](#)
- [Configuring Email Challenge in the Oracle Advanced Authentication Self-Service Portal](#)
- [Configuring Mobile Authenticator Challenge in the Oracle Advanced Authentication Self-Service Portal](#)
- [Configuring Security Questions Challenge in the Oracle Advanced Authentication Self-Service Portal.](#)
- [Configuring FIDO2 Challenge in the Oracle Advanced Authentication Self-Service Portal.](#)

- [Configuring YubiKey Challenge in the Oracle Advanced Authentication Self-Service Portal.](#)
- [Configuring Push Notification Challenge with Oracle Mobile Authenticator in the Oracle Advanced Authentication Self-Service Portal](#)

Configuring Device Authentication on Windows using Oracle Access Management and Multi-Factor Authentication

The following tutorial shows you how to set up your Microsoft Windows device to authenticate with Oracle Access Management (OAM) and multi-factor authentication (MFA), using Oracle Universal Authenticator:

- [Configuring Device Authentication on Windows using Oracle Access Management and Multi-Factor Authentication](#)

Seamless Single Sign-On with Oracle Universal Authenticator

The following tutorial shows you how seamless Single Sign-On (SSO) works for devices authenticated with Oracle Universal Authenticator:

- [Seamless Single Sign-On with Oracle Universal Authenticator](#)

Using Password Management in Oracle Universal Authenticator

The following tutorial shows you how to use password management features in Oracle Universal Authenticator:

- [Using Password Management in Oracle Universal Authenticator](#)

Part VII

Troubleshooting

This section describes common troubleshooting tips and known issues for the Oracle Universal Authenticator client application, SSO Browser Extension, and Device Runtime Support Service (DRSS).

- [Viewing Oracle Universal Authenticator Logs](#)
- [Known Issues](#)

Viewing Oracle Universal Authenticator Logs

The following sections show how to view logs for debugging issues with Oracle Universal Authenticator (OUA).

Viewing DRSS Logs

Administrators can check the `oua-drss` pod logs to find and troubleshoot any underlying errors for issues such as user login problems. To check the pod logs, run the following on the Kubernetes cluster:

```
kubectl logs <RELEASE-NAME>-oua-drss-<pod> -n <namespace>
```

Viewing OUA Client Application and SSO Browser Extension Logs

To view the logs for the OUA Agents and SSO Browser extension on the Microsoft Windows computer:

1. Open the Event Viewer using Windows Search.
2. In the left navigation pane, select **Event Viewer > Application and Services Logs**.
3. The following Agent logs are then available:
 - **OUIDesktopHelper**: Desktop agent logs.
 - **OUAUpgradeAgent**: Device software management and upgrade logs.
 - **OUIBrowserExtensionNativeApp**: SSO Browser extension logs.

For more detailed logs, you can also view the following log files:

- **OUIDesktopHelper**- C:\Program Files\Oracle\Oracle Universal Authenticator\LogsDesktopHelper
- **OUAUpgradeAgent** - C:\Program Files\Oracle\Oracle Universal Authenticator\LogsUpgradeAgent
- **OUIBrowserExtensionNativeApp**: - C:\Program Files\Oracle\Oracle Universal Authenticator\LogsBrowserExtensionNativeApp

Viewing OUA Client Application Runtime Logs

OUA client application runtime logs are available at C:\CredProv\CredProv_<seqNo>.log.

Known Issues

Browser Stuck on OAM Login Page Unable To Access the Web Application

When accessing an OAM protected application using a browser, the browser may get stuck on the OAM login page (<https://oam.example.com/oam/server/obrareq.cgi?encquery..>).

This may happen for the following reasons:

- The OUA Agent is not running. Start Task Manager and check if `OUADesktopHelper.exe` is running. If the agent is not running, start it by executing `OUADesktopHelper.exe` start from the path "C:\Program Files\Oracle Universal Authenticator".
- You are accessing an OAM protected resource that is using a different OAM server to the one configured with DRSS. To access URL's that use a different OAM server, you will need to disable the SSO Browser extension.
- You are accessing a URL for a protected OAM resource that runs on the same server as OAM. As per General OAM Requirements, the Oracle HTTP Server/WebGate cannot be on the same server as OAM.

Browser Redirects to OAM Login Page and Asks for Credentials

You have logged into Microsoft Windows using OUA successfully. You access an OAM protected application, are redirected to the OAM login page, and are asked for your SSO credentials.

This problem can happen for the following reasons:

- The **OUADesktopHelper.exe** has not started before you access the protected resource. This can happen if you have a slow machine. If this happens wait a few minutes and try again.
- You are using Firefox and Firefox was installed after the Oracle Universal Authenticator client application. To solve this problem deinstall and reinstall Oracle Universal Authenticator. The SSO Browser Extension for Firefox will then be installed.

Alternatively, check the OUA Agent logs as per [Viewing Oracle Universal Authenticator Logs](#).

If you see the error:

```
An error occurred while making token call to drss. Check previous logs for exact error.  
Error from drss= { "status" : "FAILURE", "info" : { "responseCode" :  
"DRSS-13003", "responseMessage" : "DRSS-13003 OAM Session Validation  
failed" } } ,
```

Logout and restart Microsoft Windows. After logging into Windows with OUA again, try and access the OAM protected application.

OUA Client Application Loops After Entering OAM Credentials When System Is Offline

A user attempts to login with OUA and receives a message saying the System is offline. The user attempts to perform offline login by entering their OAM credentials and the System is offline error message keeps looping.

If you see this error then the OUA client application was not installed when logged in as an Administrator. See, [Installing the Client Application](#).

OUA Agent Executables Do Not Start Up

If OUADesktopHelper.exe and OUAUpgradeAgent.exe don't start, and starting them manually doesn't work (for example running OUADesktopHelper.exe start from the path C:\Program Files\Oracle Universal Authenticator\, then reboot the system and the processes should start.

Incorrect Text Shown When Email or SMS Set As Default Factor

If Email or SMS is set as the default factor in the Self-Service Portal, incorrect text is shown when challenged in OUA to enter the OTP. For example send OTP to ***@**.com is shown instead of Enter OTP sent to ***@**.com

To solve this set the parameter

bharosa.uio.default.challenge.type.enum.ChallengeEmail.promptmessage to Enter OTP sent to {0}, and

bharosa.uio.default.challenge.type.enum.ChallengeSMS.promptmessage to Enter OTP sent to phone {0}.

For details on how to set the parameters using REST API see, Configuration Properties for OAA.

OUADesktopHelper and OUAUpgradeAgent Service Status After Deinstallation

When OUA client software is deinstalled, the OUADesktopHelper and OUAUpgradeAgent services can still be seen in Services in a "Disabled" state. This does not have any impact and the OUA client software has deinstalled successfully.

Enabling OUA SSO for Desktop Applications (Thick Clients)

Enabling OUA SSO for Desktop Application (thick clients) is not currently supported.

Azure AD Applications and OUA

OUA will not interfere with existing Azure AD SSO applications and will continue to work the way they did prior to installing OUA.

Known Issues in Accessibility

- In the Self-Service Portal the following issues are observed in the **My Device** section at 400% zoom:
 - In the **My Devices** screen, the circular image representing number of devices gets cut out towards the right side, and the text **Last logged in Over a week ago** inside the button is not completely visible.
 - When the ellipsis for a device is clicked and **View Details** is selected, entries under **Device history** are not visible.
 - When the ellipsis for a device is clicked and **Disable Device** or **Rename Device** is selected, the complete dialog box for **Disable Device** or **Rename Device** is not visible.
- In the Administration Console in the **Device** detail screen, clicking on **Block User** button brings up a dialog box with **Cancel** and **Confirm** buttons without any text.
- The **Cancel** and **OK** button in the OUA credential collector screen and incorrect password error message screen, are not in High Contrast.