Oracle Hospitality OPERA Cloud Identity Management
MFA Configuration Guide

Release 24.3
G21104-02
March 2025

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management MFA Configuration Guide, Release 24.3

G21104-02

Contents

Notices

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 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" or "commercial computer software documentation" 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 and Java 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.

Preface

Purpose

This guide provides MFA Guidance for non-federated customers whose OPERA Cloud environment is being converted from SSD to OCIM.

Audience

This document is intended for OPERA Cloud Identity Management users.

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

http://docs.oracle.com/en/industries/hospitality/

Revision History

Table   Revision History

Date	Description of Change
December 2024	Initial Publication
March 2025	Revision to remove IP Based access control from document.

1
Multi-Factor Authentication

MFA Guidance for Non-Federated Customers

This guide provides MFA Guidance for non-federated customers whose OPERA Cloud environment is being converted from SSD to OCIM.

In Shared Security Domain (SSD), OPERA Cloud customers use MFA enabled users. Users enabled for MFA (this is enabled on their user profile in SSD's OIM) are triggered for email OTP based MFA during OPERA Cloud login. When an OPERA Cloud environment is converted from SSD to OCIM, all users, groups (roles), and their user group (role) memberships are migrated from SSD to OCIM. However, a customer's MFA settings are not migrated. Customers should use the self-service feature in OCI IAM Identity Domain of OCIM to configure MFA before or after conversion.

Configuring MFA in OCI IAM Identity Domain

MFA configuration is a policy driven configuration and OCI IAM allows you to create different rules for triggering MFA. These steps provide a simple approach for configuring MFA in a customer's OCI IAM Identity Domain with a default setting provisioned during OCIM. This approach is based on group membership where only members of a newly created group are triggered for MFA during OPERA Cloud services login and R&A login.

1. Log in to OCI Cloud console as an OCI cloud administrator user.

2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

3. Click the name of the identity domain in which you want to work. (You might need to change the compartment to find the domain that you want.)

4. On the Domain page, click **Groups**.

5. On the Groups page, click **Create Group**.

6. Enter a name for the group, for example: MFAENABLED.

7. Search and Add users as members of the group for which MFA is to be triggered during OPERA Cloud services login.

8. Click **Create** and go back to the Domain page.

9. On the Domain Details page, click **Security**.

10. On the Security page, click **MFA**.

11. Under **Factors**, select each of the factors required to access an identity domain. For an explanation of each factor, see Configuring Authentication Factors.

12. (Optional step) Click **Configure** for the MFA factors you have selected. For instructions for each factor, see Configuring Authentication Factors.

13. (Optional step) Set the Maximum number of enrolled factors users can configure.

14. (Optional step) Use the Trusted devices section to configure trusted device settings. Similar to "remember my computer," trusted devices do not require the user to provide secondary authentication each time they sign in.

15. (Optional step) Under Sign-in rules, set the maximum number of unsuccessful MFA attempts a user can make before being locked out.

16. Click **Save changes**, and then confirm the change.

17. Follow the below steps to configure new sign on rules to enable MFA in the default sign-on policy. This default sign-on policy will be available out of the box in a customer's OCI IAM Identity Domain.

    a. On the Security page for the domain, click **Sign-on policies**.

    b. On the Sign-on policies page, click **Default Sign-On Policy**.

    c. On the Default Sign-On Policy page, under **Resources**, click **Sign-on rules**.

    d. Click the **Add sign-on rule**, carefully read the confirmation, and click **Continue**.

    e. Enter the rule name, for example: Group based MFA.

    f. Under conditions, in **Group Membership**, add the group created earlier in step 6.

    g. Under **Actions**, select **Allow access**. Select the prompt for an additional factor and select **Specified factors only**.

    h. Select factors, we recommend Mobile app passcode, Mobile app notification, and Fast ID Online (FIDO) passkey authenticator.

    i. Select **Once per session or trusted device** under **Frequency**.

    j. Select **Required** under Enrollment.

    k. Click **Add sign-on rule**.

    l. On the Default Sign-On Policy page, click **Edit Priority.**

    m. Carefully read the confirmation and click **Continue**.

    n. Click the **priority number** of the newly created rule to ensure it is above the Default Sign-On Rule where **priority 1** is the newly created rule and **priority 2** is the **Default Sign-On Rule**.

    o. Click **Save Changes**.

18. Test MFA with the user who is part of the newly created group (the group added in the sign-on rule).

19. To learn more about registering for MFA using Mobile app passcode or Mobile app notification mode, watch this tutorial video Oracle Mobile Authenticator App Tutorial Video.