Oracle Hospitality OPERA Cloud Identity Management

MFA and Network Perimeters Configuration Guide

Release 25.5
G47675-02
November 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management MFA and Network Perimeters Configuration Guide, Release 25.5

G47675-02

Contents

Notices

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
November 2025	Initial Publication

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.

> **Note**
>
> There are multiple methods to configure MFA in the Identity Domain. The instructions below illustrate one such approach.

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 **User Management**.
5. Under Groups, 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**.
9. On the Domain Details page, navigate to **Authentication** tab.
10. Under Factors, click **Enable or Disable factors.** Select each of the factors required to access the OPERA Cloud services. For an explanation of each factor, see Configuring Authentication Factors. Click **Save Changes**.

11. (Optional step) You can click **Edit** for each of the MFA factors you have selected to configure the factors. For instructions for each factor, see Configuring Authentication Factors.
12. (Optional step) Use the Trusted devices section to configure trusted device settings. Similar to "remember my computer," trusted devices do not require users to provide secondary authentication each time they sign in.
13. (Optional step) Under Sign-in rules, click **Edit** to set the maximum number of unsuccessful MFA attempts a user can make before being locked out.
14. 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. Navigate to the **Domain Policies** tab.
    b. Click the **Default Sign-on policy**.
    c. On the policy page, click the **Sign-on rules** tab.
    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 **Groups**, click the **Actions** menu and select **Add**. Search for and select the group created earlier in step 6 and then click **Add**.
    g. Under Actions, select **Allow access**. Enable the **Prompt for an additional factor** button and select **Specified factors only**.
    h. Enable the factors required.
    i. Select **Once per session or trusted device** under Frequency.
    j. Select **Required** under Enrollment.
    k. Click **Add**.
    l. On the Default Sign-On Policy page, click **Actions** under **Sign-on rules**. Select **Edit Sign-on rules priority.**
    m. Click the priority number of the newly created rule to ensure it is above the Default Sign-On Rule. For example ensure priority 1 is the newly created rule and priority 2 is the Default Sign-On Rule.
    n. Click **Save Changes.**
15. Test MFA with the user who is part of the newly created group (the group added in the sign-on rule).
16. 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.

2

IP Based Access Control

Create a Network Perimeter

1. Log in to the Oracle Cloud Infrastructure console and navigate to the relevant Identity Domain.
2. Go to **Security** tab, under **Network Perimeters**, click **Create Network Perimeter**.
3. Enter a **name** and then enter the exact **IP address** or **IP addresses**, **IP range**, or **masked IP address range** for the network perimeter. To learn about IP address formats, see Managing Network Perimeters.
4. Click **Create**.

   After defining a network perimeter, you can assign it to an existing sign-on policy and configure the policy to either allow or deny access for sign-in attempts from IP addresses included in that network perimeter. Alternatively, you can create a new sign-on policy and set the appropriate access control for the network perimeter as needed.

Update the Appropriate Sign-On Policy

The following example demonstrates how to update the Sign-on Policy to permit access for IP addresses within the specified network perimeter.

> **Note**
>
> There are multiple methods to configure IP-based access controls in the Identity Domain. The instructions below illustrate one such approach.

1. In the Oracle Cloud Infrastructure console, navigate to the relevant Identity Domain.
2. Navigate to the **Domain Policies** tab and click the **Sign-on policy** you want to update.
3. On the policy page, click the **Sign-on rules** tab. Click the three dots next to the Sign-on rule and choose **Edit Sign-on rule**.
4. Under the Filter by client IP Address section, select **Restrict to the following network perimeters** button and choose the network perimeter that you created.
5. Under Actions, verify the **Allow Access** button is selected. Click **Edit Sign-on rule**.