

# Dell EMC OpenManage Enterprise Login with PingFederate

This technical white paper provides information about configuring OpenManage Enterprise (OME) and PingFederate to enable logging into OME using PingFederate.

## Abstract

OME 3.5 provides a method to log in using OpenID Connect (OIDC) providers—PingFederate. OIDC providers are the identity and user management software that allow users to securely access applications.

November 2020

## Revisions

Date	Description
Nov 2020	Initial release

## Acknowledgements

Author: Venkata Donepudi , Balaji Shanmugam and Manish Agrawal

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © November 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [11-Nov-20] [Technical White Paper] [Dell EMC OpenManage Enterprise Login with PingFederate | 454]

## Table of contents

Revisions.....	2
Acknowledgements.....	2
Table of contents .....	3
Executive summary.....	4
1 System Requirements & Prerequisites .....	5
2 OME and PingFederate Configurations .....	6
2.1 Configure Scope and Policy in PingFederate.....	6
2.2 Configure Time in PingFederate and OME .....	9
2.2.1 PingFederate time configuration.....	9
2.2.2 OME time configuration .....	9
2.3 Enable Dynamic Client registration in Ping Federate.....	10
3 OpenID Connect Provider Registration in OME.....	11
3.1 Register an OpenID Connect Provider with Username and Password in OME.....	11
3.2 Register an OpenID Connect Provider with Initial Access Token in OME .....	11
4 Configure OAuth Client for dx cua scope and signing algorithms in PingFederate .....	14
5 Login from OME using PingFederate Users .....	15
6 General Troubleshooting of Issues .....	18
A Related resources .....	19

## Executive summary

In this white paper, you will learn how to configure PingFederate and OpenManage Enterprise (OME) or OpenManage Enterprise-Modular (OME-M) to enable you to log into OME using PingFederate.

Integrating OME with PingFederate allows PingFederate users (Users associated to data store in PingFederate) to log into OME.

After OME is integrated with PingFederate, user authentication in OME will be delegated to PingFederate.

# 1 System Requirements & Prerequisites

The following are the system requirements:

- PingFederate version 10.1
- OpenManage Enterprise version 3.5 or later

The following are the prerequisites before integration of OME with PingFederate:

- User has prior knowledge of:
  - PingFederate
  - OpenManage Enterprise
  - OpenID Connect specifications
- PingFederate is installed and configured with:
  - LDAP or External Data Source
  - Access Token Management
  - Identity Provider Configuration
  - Policies and Grant Mappings
  - All prerequisites for Dynamic client registration

If these prerequisites are not met, see the PingFederate help guide(<https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html>) for fulfilling the prerequisites.

## 2 OME and PingFederate Configurations

This section describes the configuration required to enable user authentication in PingFederate.

### 2.1 Configure Scope and Policy in PingFederate

To enable OpenManage Enterprise OpenID Connect login using PingFederate, you must add and map a scope `dxcu` to the Client ID and define the user privileges. The Dell Extended Claim for User Authentication (`dxcu`) is necessary to identify the user roles and permissions required to manage OME.

To configure `dxcu` claim in PingFederate, do the following:

1. Log into PingFederate with administrative privileges.
2. Navigate to **System->OAuth Settings->Scope Management->Exclusive Scopes**
3. Set **Scope Value** to `dxcu` and **Scope Description** to **Dell Extended Claim for User Authentication** as shown below in Figure 1.

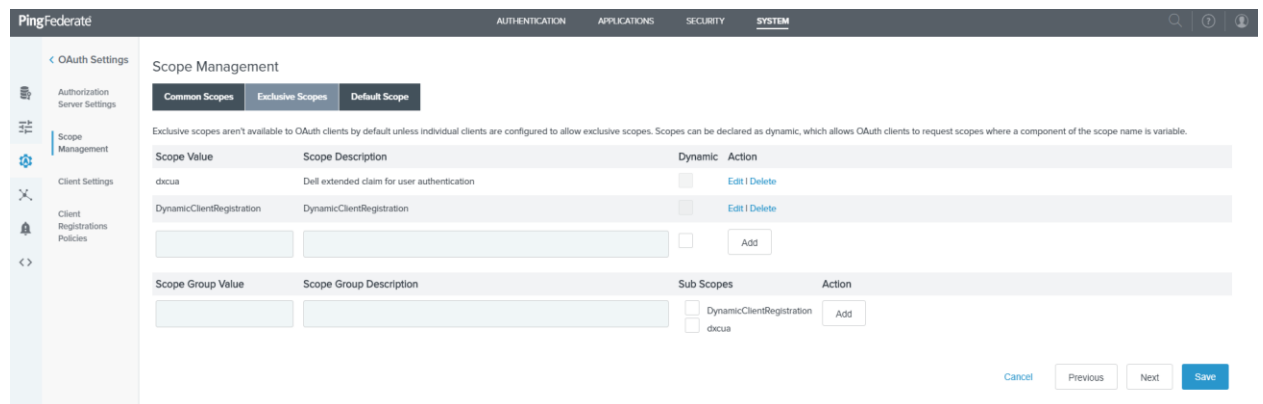


Figure 1 – PingFederate: Scope Management

After defining the `dxcu` scope, it is required to map `dxcu` to the PingFederate Policy.

To map “`dxcu`” scope to PingFederate Policy, do the following:

1. Navigate to **Applications -> OpenID Connect Policy Management-> Select Policy-> Manage Policy tab**.
2. Select the **INCLUDE USER INFO IN ID TOKEN** check box as shown in Figure 2.

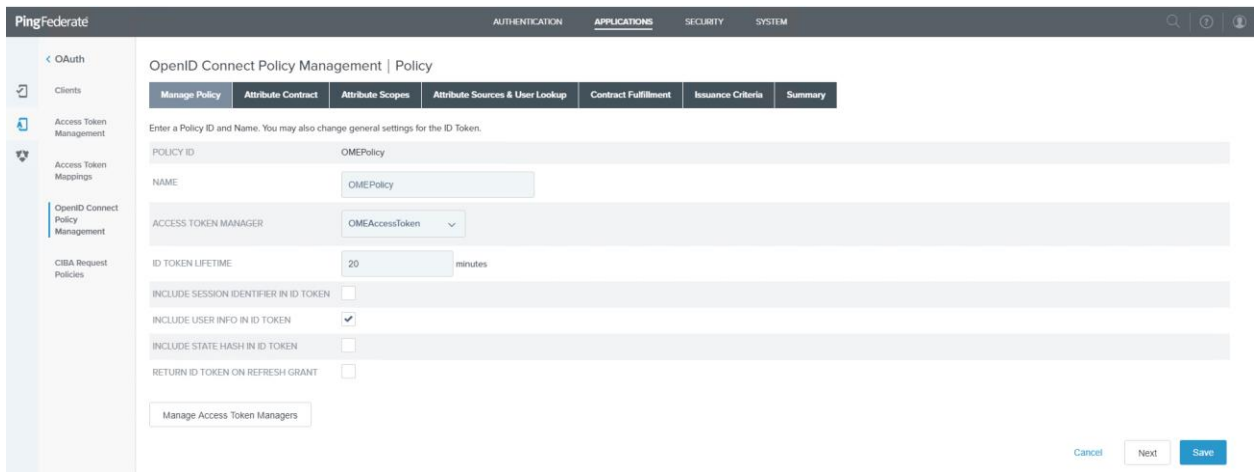


Figure 2 - PingFederate: OpenID Connect Policy Management -> Manage Policy

3. Navigate to **Attribute Scopes** tab and add the **dx cua** scope attribute as shown in Figure 3.

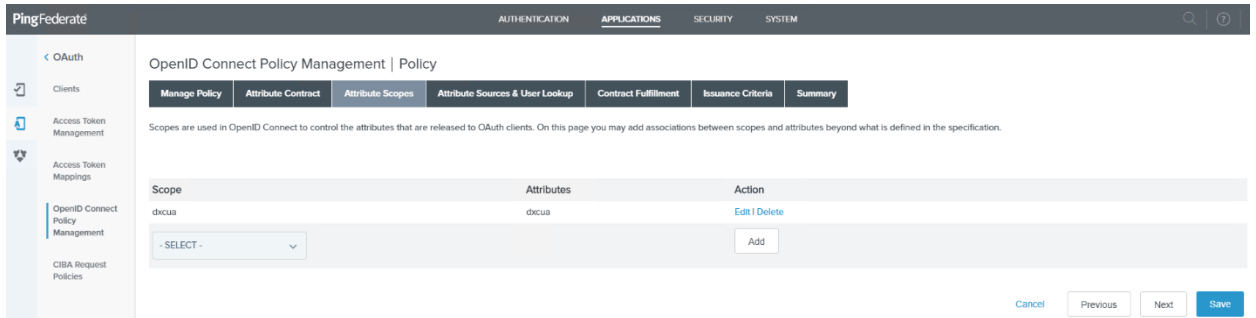


Figure 3 – PingFederate: OpenID Connect Policy Management -> Attribute Scopes

4. Navigate to **Contract Fulfillment** and:
  - a. Select **Text** as a source for the **dx cua** scope.
  - b. Add **[{"Role": "CA,AD"}]** for enabling administrator privileges in OME as shown in Figure 4.

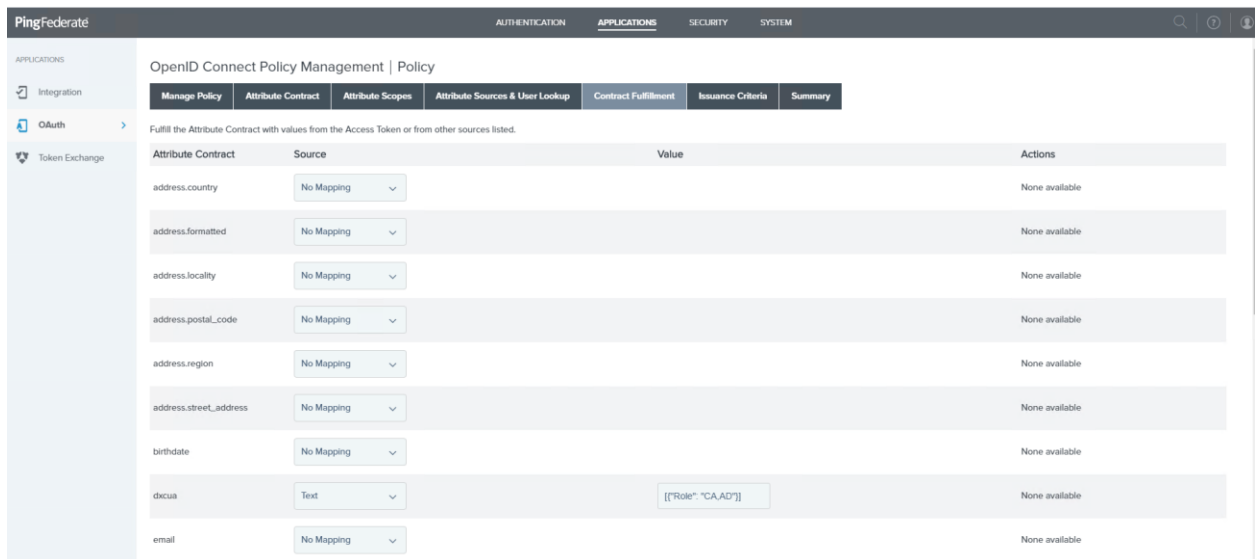


Figure 4 – PingFederate: OpenID Connect Policy Management -> Contract Fulfillment

The configuration in step-4 allows OAuth clients using the policy selected in step-4 to login users into OME with administrator privileges. OME supports other roles along with the administrator role.

The following are the dxua roles available in OME. See the OME User’s Guide for more information about each user role.

Role	Abbreviation
Administrator	AD
Device Manager	DM
Viewer	VE



The following are the dx cua roles available in OME-M. See the OME-M User's Guide for more information about each user role.

Role	Abbreviation
Chassis Administrator	CA
Computer Manager	CM
Fabric Manager	FM
Storage Manager	SM
Viewer	VE

## 2.2 Configure Time in PingFederate and OME

It is required that both OME and PingFederate should reflect the same time to avoid issues in validating Authorization Code, Access Token, and User ID token. Ensure that OME and PingFederate are pointing to the same time source.

### 2.2.1 PingFederate time configuration

See the PingFederate help guide (<https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html>) to sync time from Host Operating System.

### 2.2.2 OME time configuration

To configure time in OME, do the following:

1. Log into OME with administrative privileges.
2. Navigate to **Application Settings** -> **Network** -> **Time Configuration** and configure time either by selecting **Use NTP** or configure **Time and Time Zone** as shown in Figure 5.

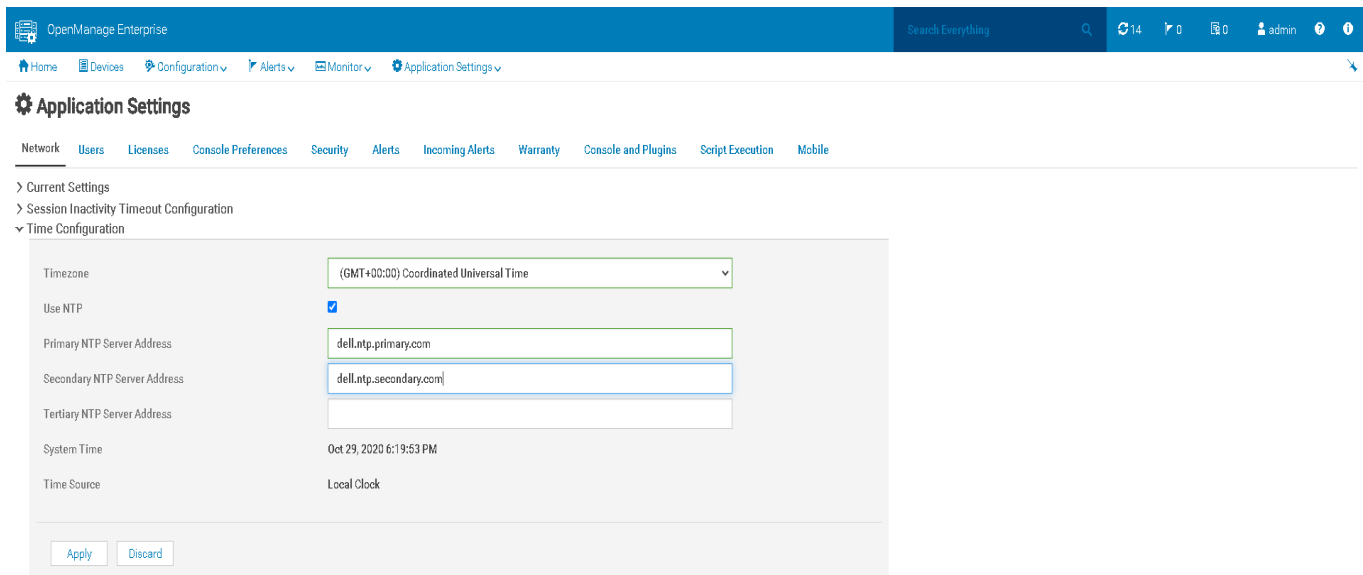


Figure 5 - OME: Time Configuration

## 2.3 Enable Dynamic Client registration in Ping Federate

Dynamic Client Registration allows OME to register clients on PingFederate via APIs either by using username and password or Initial Access Token. By default, Dynamic Client registration is disabled on PingFederate and is enabled only when external data sources such as an external database or AD/LDAP is configured in PingFederate.

To enable Dynamic Client Registration, do the following:

1. Log into PingFederate as an admin user.
2. Navigate to **System-> OAuth Settings -> Client Settings -> Dynamic Client Registration**.
3. Select all the check boxes of the fields as shown in Figure 6.
4. Select any existing scope for **INITIAL ACCESS TOKEN SCOPE** or create a new scope called **DynamicClientRegistration** scope similar to configuring dxdua in Configuration of Scope in PingFederate section.

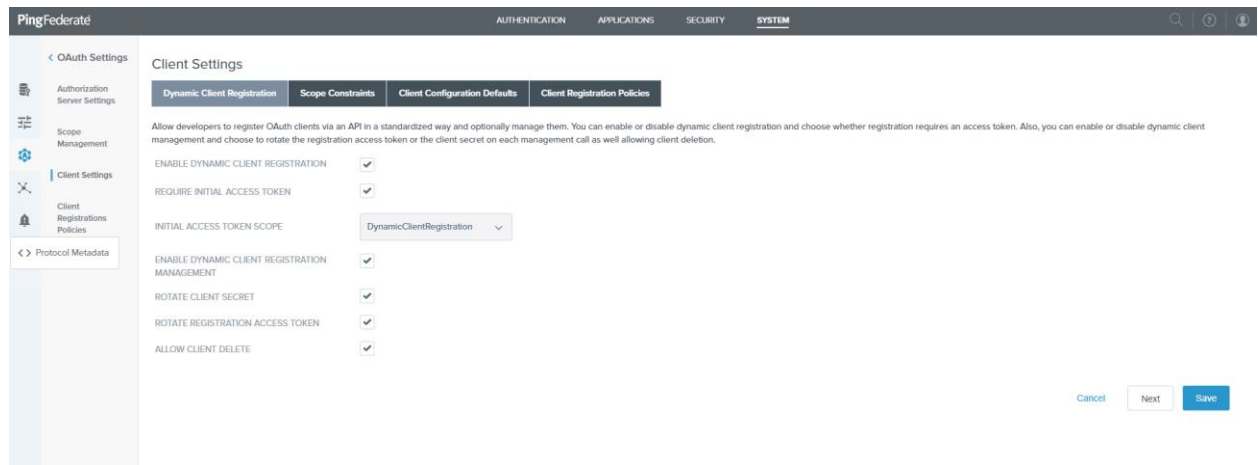


Figure 6 - PingFederate: Client Settings

It is recommended to select **ROTATE CLIENT SECRET** and **ROTATE REGISTRATION ACCESS TOKEN** which will change Client Secret and Registration Access Token when modifying or querying client registration.

PingFederate will not allow Dynamic OAuth client registration using both username and password and Initial Access Token at the same time. Disable **REQUIRE INITIAL ACCESS TOKEN** for username and password-based OAuth client registration to be successful. When **Require initial access token** is enabled, only access token will work for registration.

### 3 OpenID Connect Provider Registration in OME

When you register an OpenID Connect provider in OME using username and password or Initial Access Token, it generates an OAuth client in PingFederate.

#### 3.1 Register an OpenID Connect Provider with Username and Password in OME

To register OpenID, Connect Provider with username and password, do the following:

1. Log into OME with administrative privileges.
2. Navigate to **Application Settings** -> **Users** -> **OpenID Connect Providers** -> **Add**.
3. Enter information in the required fields as shown in Figure 7.

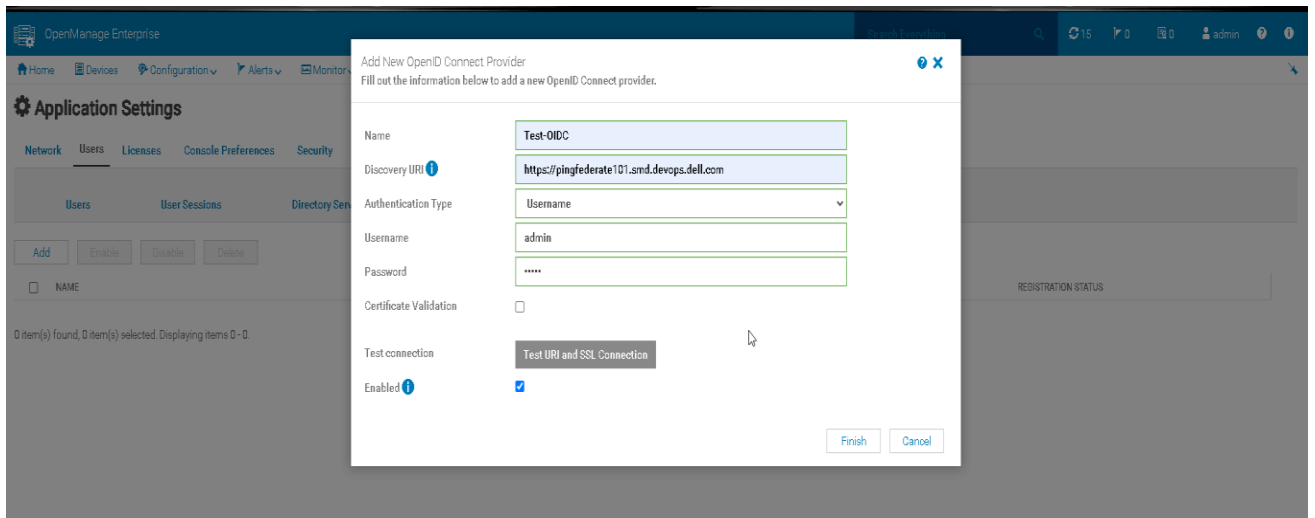


Figure 7 - OME: Add New OpenID Connect Provider using username and password

The user (local PingFederate User or AD/LDAP User in PingFederate) information used to register OpenID Connect Provider should have proper privileges to create OAuth client in PingFederate.

#### 3.2 Register an OpenID Connect Provider with Initial Access Token in OME

To register OpenID, Connect Provider with Initial Access Token, do the following:

1. Log into OME with administrative privileges.
2. Navigate to **Application Settings** -> **Users** -> **OpenID Connect Providers** -> **Add**.
3. Enter information in the required fields as shown in Figure 8.

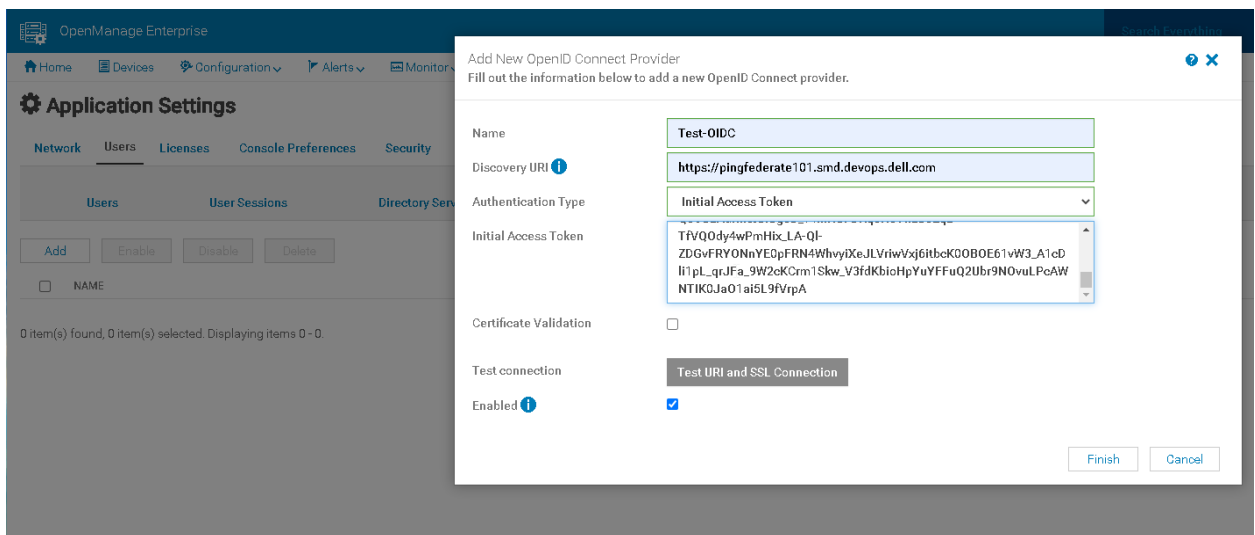


Figure 8 - OME: Add New OpenID Connect Provider using Initial Access Token

To get the Initial Access Token, see the guidelines mentioned in the PingFederate help guide (<https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html>)

For example: Create an OAuth Client in PingFederate and use that OAuth client to provide the Access Token.

The following are the sample request and response for getting initial access token using IMPLICIT flow.

**Request for Initial Access token:**

```
curl --location --request POST
/as/authorization.oauth2?client_id=DynamicClientRegistration&response_type=token&redirect_uri=https://<callback
url>&scope=DynamicClientRegistration' \

--header 'Authorization: Basic dGVzdDp0ZXN0'
```

**Successful Response:**

302

```
https://XXXX #access_token=
eyJhbGciOiJSUzI1NiIsImtpZCI6ImExOjMwOjZzOjUzOjVEOkJCOjE5OjU3IiwicGkuYXRtIjoieG1wdiJ9.eyJzY29wZSI6IkR5b
mFtaWNBdGllbnRSZWdpc3RyYXRpb24iLCJjbGllbnRfaWQiOiJlEeW5hb &token_type=Bearer&expires_in=7199
```

On successful registration of OpenID Connect provider in OME, the OIDC is displayed as shown in Figure 9.

The screenshot shows the OpenManage Enterprise interface. The top navigation bar includes 'Home', 'Devices', 'Configuration', 'Alerts', 'Monitor', and 'Application Settings'. The main content area is titled 'Application Settings' and has several tabs: 'Network', 'Users', 'Licenses', 'Console Preferences', 'Security', 'Alerts', 'Incoming Alerts', 'Warranty', 'Console and Plugins', and 'Script Execution'. Under the 'Users' tab, there are sub-tabs for 'Users', 'User Sessions', 'Directory Services', and 'OpenID Connect Providers'. The 'OpenID Connect Providers' sub-tab is active, showing a table with one entry: 'Test-OIDC'. The table has columns for 'NAME', 'ENABLED', and 'DISCOVERY URI'. The 'Test-OIDC' entry is checked in the 'ENABLED' column and has the discovery URI 'https://pingfederate101.smd.devops.dell.com'. There are also 'Add', 'Enable', 'Disable', and 'Delete' buttons above the table.

NAME	ENABLED	DISCOVERY URI
<input type="checkbox"/> Test-OIDC	<input checked="" type="checkbox"/> [✓]	https://pingfederate101.smd.devops.dell.com

Figure 9 - OME: Successful Registration

**Notes:**

- Discovery URI specified in OIDC configuration wizard should have valid endpoint of the provider listed.
- Test connection in configuration wizard is anonymous, the credentials or Initial access token specified is used for registration.
- When cert is used in OIDC configuration, the **Name of OIDC provider mentioned in Discovery URI** should match the OIDC providers **Issuer** endpoint name and the OIDC Providers SSL Certs "Subject CN" or "Subject alternative name" for OIDC login to work.
- OME supports only ClientID and Secret based client authentication.
- Maximum of 4 OIDC providers can only be used with OME.
- Test Registration status button is available to test the registration status of an OIDC configuration.

## 4 Configure OAuth Client for dx cua scope and signing algorithms in PingFederate

After OpenID Connect provider is registered in OME successfully, a new OAuth client is created in PingFederate. Dynamically registered OAuth client shall be configured to use the dx cua scope and OME compatible signing algorithm for ID Token.

To configure dx cua scope and signing algorithm, do the following:

1. Log into PingFederate with administrative privileges.
2. Navigate to **Applications** -> **OAuth Clients** -> Select **Client** and configure **Exclusive Scopes** and **ID Token Signing Algorithm** as shown in Figure 10.

EXCLUSIVE SCOPES

Allow Exclusive Scopes

dx cua

OPENID CONNECT

ID Token Signing Algorithm

RSA using SHA-256

Figure 10 - PingFederate: configuring Exclusive Scopes and ID Token Signing Algorithm in OAuth Client.

## 5 Login from OME using PingFederate Users

OME displays successfully registered OpenID Connect Providers on the login page. Users can choose to log into OME with username and password credentials of users local to OME or with any one of the registered OpenID Connect Providers.

To log into OME with PingFederate Users, do the following:

1. Navigate to the OME login page.
2. OME login page displays successfully registered OpenID Connect Provider(s) as shown in Figure 11.

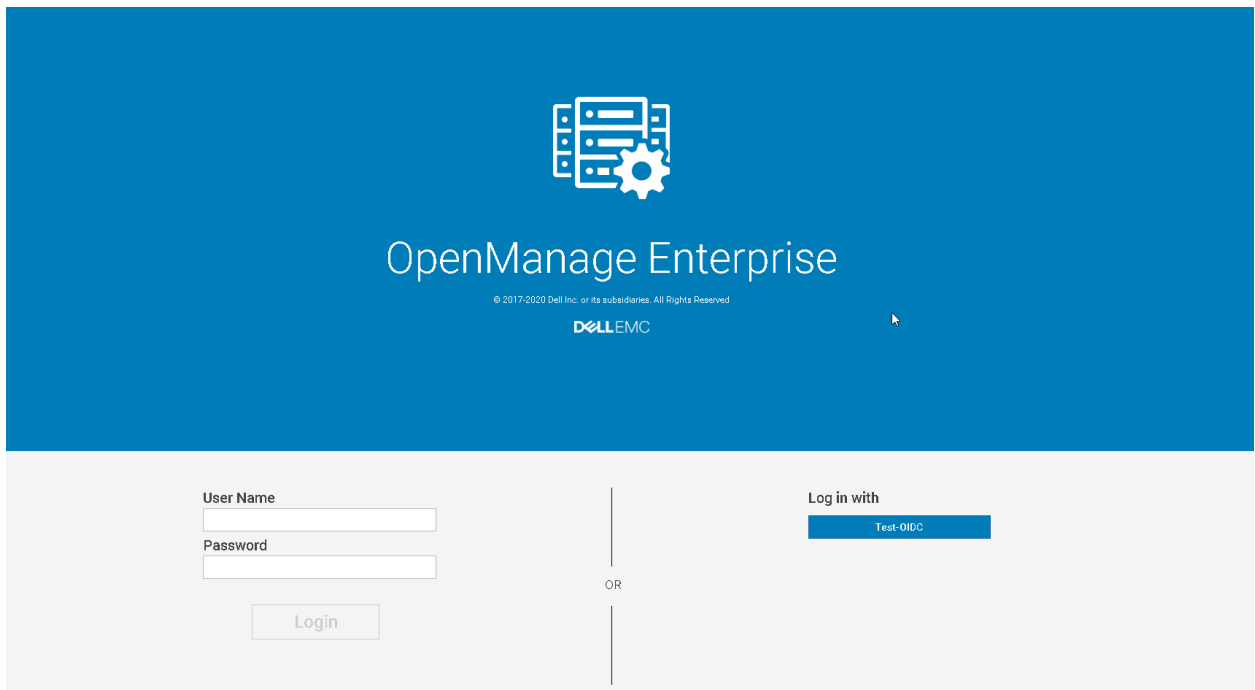
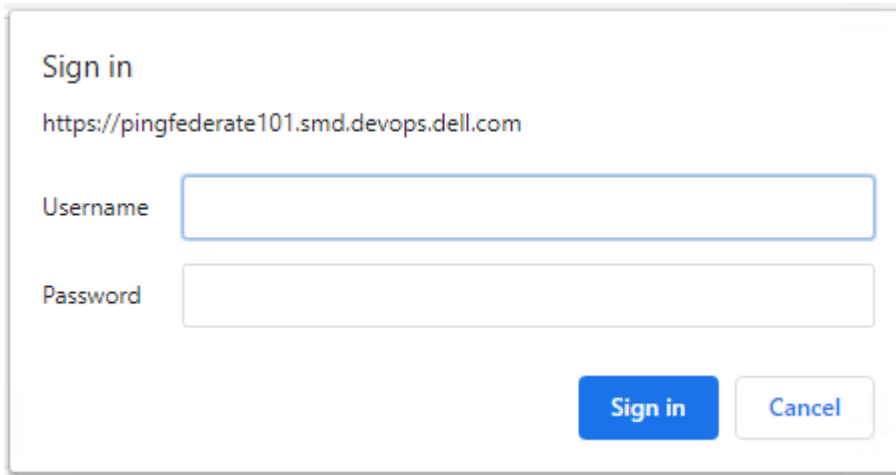


Figure 5 - OME: Login Screen

3. Select **Login with OpenID Connect Provider Name**.

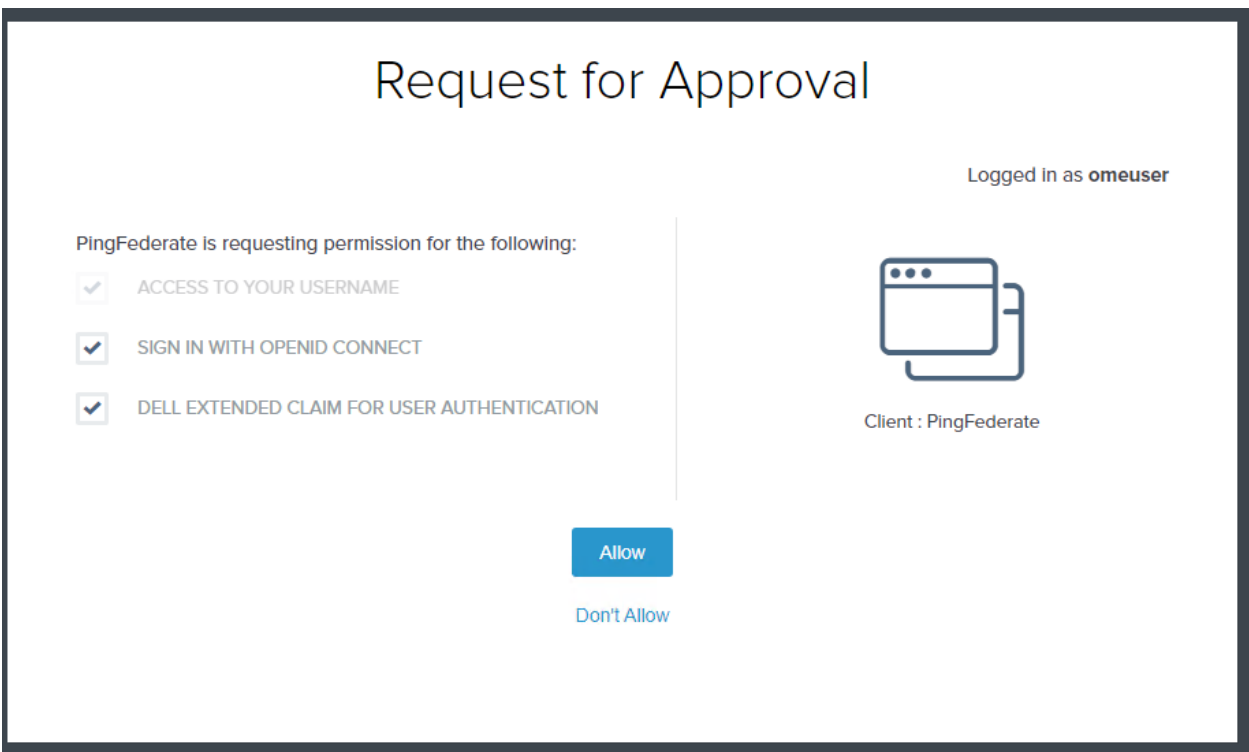
The browser is redirected to PingFederate website and challenge the user for credentials. If basic auth is enabled in PingFederate then following screen is displayed. Else the PingFederate admin console page is displayed.



The image shows a 'Sign in' dialog box. At the top, it says 'Sign in' followed by the URL 'https://pingfederate101.smd.devops.dell.com'. Below the URL are two input fields: 'Username' and 'Password'. At the bottom right, there are two buttons: a blue 'Sign in' button and a white 'Cancel' button with a blue border.

Figure 12 – PingFederate: Credentials Screen

After validating the credentials successfully, if user consent setting is enabled in PingFederate then user will be prompted to provide access permissions as shown in Figure 13.



The image shows a 'Request for Approval' screen. At the top, it says 'Request for Approval'. Below this, it says 'Logged in as omeuser'. On the left, there is a section titled 'PingFederate is requesting permission for the following:' with three items, each with a checked checkbox: 'ACCESS TO YOUR USERNAME', 'SIGN IN WITH OPENID CONNECT', and 'DELL EXTENDED CLAIM FOR USER AUTHENTICATION'. On the right, there is an icon of a computer monitor and a document, with the text 'Client : PingFederate' below it. At the bottom, there are two buttons: a blue 'Allow' button and a blue 'Don't Allow' button.

Figure 13 - PingFederate: Consent Screen

After providing the necessary permissions, the browser is redirected to OME and the user will be logged into OME based on the response from PingFederate.



After successful login to OME, information about the user is displayed in the upper right corner as shown in Figure 14.

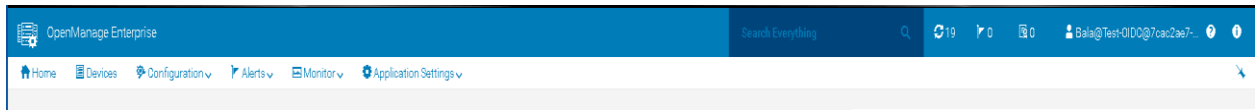
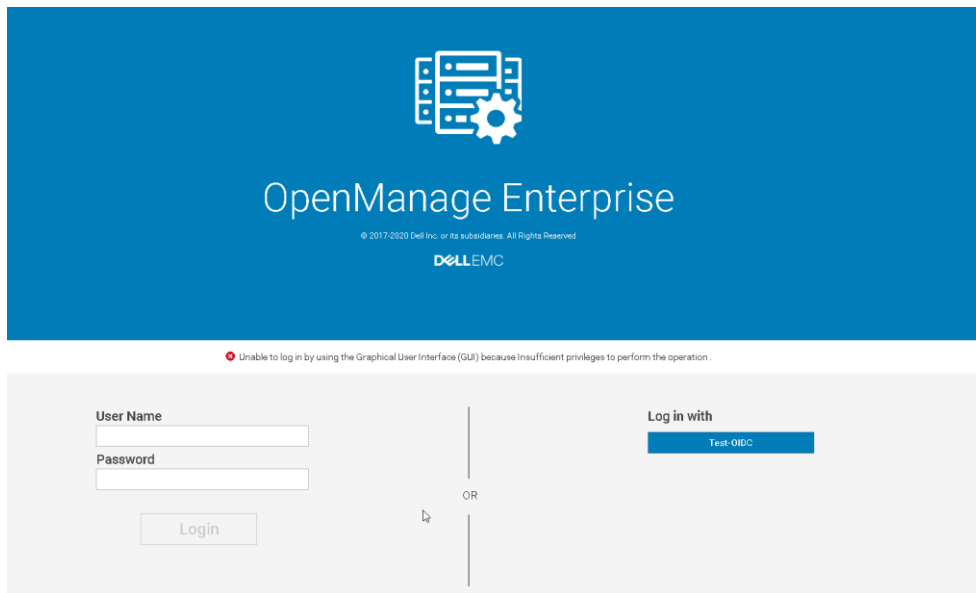


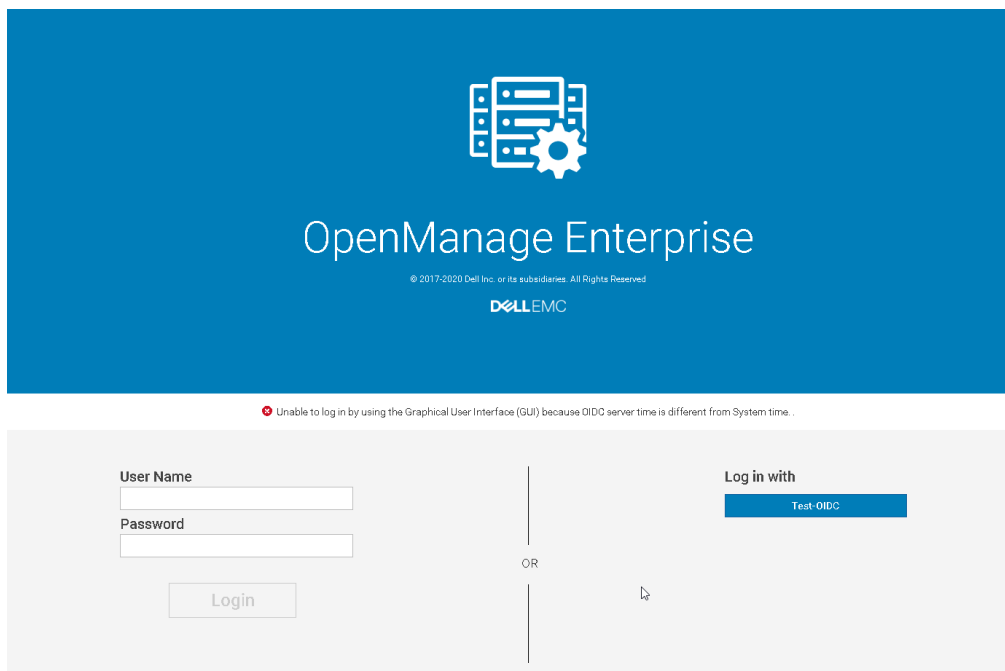
Figure 14 - OME: Successful Login

## 6 General Troubleshooting of Issues

1. If you see the error *'Unable to log in by using the Graphical User Interface (GUI) because Insufficient privileges'* while logging into OME then ensure that dx cua claim is added in Ping Federate Server.



2. If you see the error *'Unable to log in by using the Graphical User Interface (GUI) because OIDC server time is different from System time'* while logging into OME then ensure that OME and PingFederate Server are in the same time zone.



3. For any other issues see the PingFederate Server log.

## A Related resources

[Dell EMC OpenManage Enterprise documents](#)