

JD Edwards EnterpriseOne Single Sign-On Using Oracle Identity Cloud Service

Configuration for Setting up Single Sign-On
(SSO) Using Oracle Identify Cloud Service
(IDCS) for JD Edwards EnterpriseOne

November, 2023, Version 1.0
Copyright © 2023, Oracle and/or its affiliates
Public

Purpose statement

This document describes the integration of the Oracle Identity Cloud Service (IDCS) with JD Edwards EnterpriseOne single sign-on (SSO) configuration to provide App Gateway header-based authentication.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Purpose statement	2
Disclaimer	2
Purpose	4
Introduction	4
Overview	5
Create the IDCS Enterprise Application for JD Edwards EnterpriseOne SSO	6
Set Up an Oracle IDCS App Gateway	10
Download and Extract the App Gateway Binary File	10
Register an App Gateway	12
Configure the App Gateway Server	15
Configure the JD Edwards EnterpriseOne HTML Server for Oracle IDCS App Gateway	18
Test the Integration	20
Using IDCS App Gateway URL	20
Using the IDCS My Apps Feature	20
Conclusion	20

Purpose

This document describes how to integrate the Oracle Identity Cloud Service (IDCS) with JD Edwards EnterpriseOne single sign-on (SSO) configuration to provide App Gateway header-based authentication.

Introduction

Security is of paramount importance to JD Edwards customers. It is important for customers to keep their JD Edwards systems secure and one of the ways to achieve this is by providing a secure way of authentication and authorization of users who access the JD Edwards applications. This ensures that the applications are used by users who have the right privileges and access to the information and prevents any security breach. It can be achieved by configuring Single Sign-On (SSO) access to JD Edwards to ensure authorized access. Oracle provides Oracle Identity Cloud Service (IDCS) as a solution for Single Sign-on (SSO) requirements and addressing the authentication and authorization needs of customers.

Oracle Identity Cloud Service (IDCS) provides identity management, single sign-on (SSO), and identity governance for on-premises applications, in the cloud, or for mobile devices. Employees and business partners can access applications at any time, from anywhere, and on any device in a secure manner.

Oracle Identity Cloud Service is commonly used as either an Identity Provider (IdP) or a Service Provider (SP) for applications. An identity provider provides identifiers for users who want to interact with Oracle Identity Cloud Service using a website that's external to Oracle Identity Cloud Service. A service provider is a website that hosts applications. One can enable an identity provider and define one or more service providers, enabling users to access the applications hosted by the service providers directly from the identity provider.

Integrating JD Edwards EnterpriseOne with Oracle Identity Cloud Service provides the user with a seamless experience by offloading the business logic to secure applications and enable users to access application through single sign-on (SSO).

JD Edwards EnterpriseOne supports App Gateway as a reverse proxy, protecting web applications by restricting unauthorized network access to them. App Gateway is a software appliance that enables you to integrate applications hosted either on a compute instance, in a cloud infrastructure, or in an on-premises server with Oracle Identity Cloud Service for authentication purposes.

This document describes the steps and the configuration required to setup single sign-on for JD Edwards using Oracle Identity Cloud Service (IDCS)

Overview

The integration of Oracle Identity Cloud Service for Single Sign-On with JD Edwards EnterpriseOne provides enhanced security, user experience, and operational efficiency. By centralizing user management and enforcing robust authentication measures, organizations can confidently embrace this integrated solution, poised for sustained success in today's dynamic business environment.

To support Single Sign-On (SSO) with JD Edwards EnterpriseOne using Oracle Identity Cloud Service, below components are involved:

- Oracle Identity Cloud Service (IDCS) configured as Identity Provider as well as Service Provider.
- Oracle App Gateway acting as the SSO provider to JD Edwards EnterpriseOne.

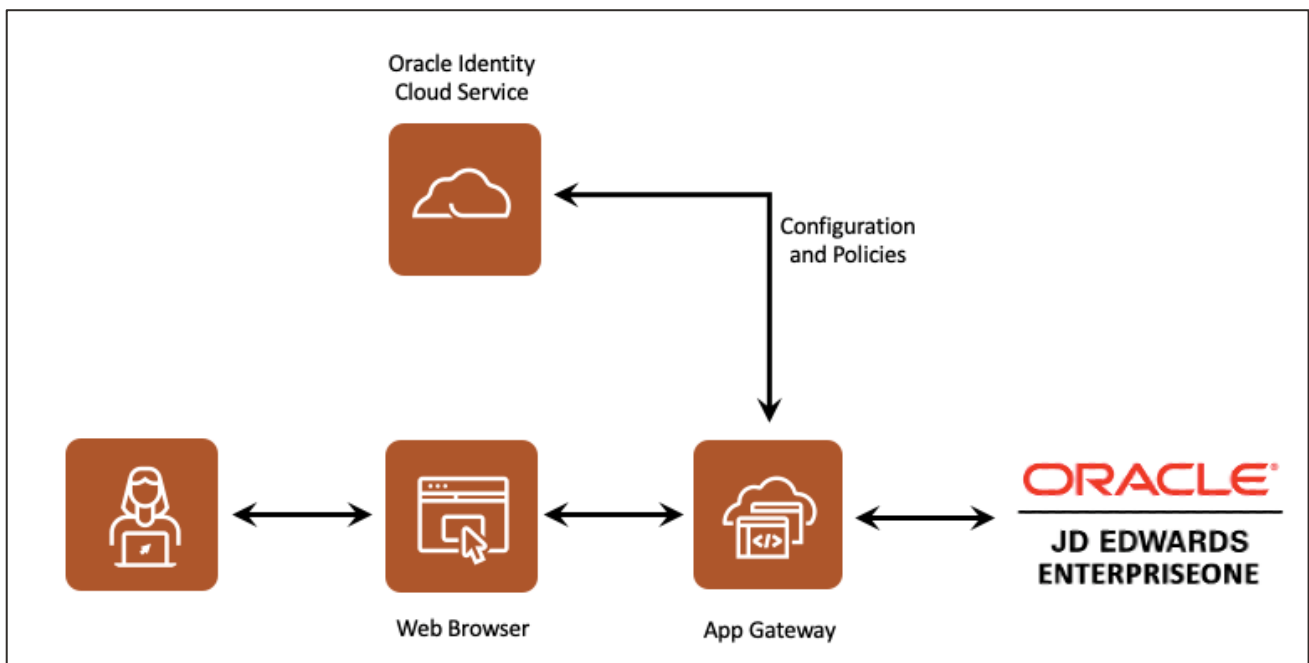


Figure 1. Architecture diagram

Configuring Oracle Identity Cloud Service as a Single Sign-On (SSO) provider using OAuth involves several high-level steps. Here is an overview of the key steps involved:

1. Access Oracle IDCS Console.
2. Create an Enterprise Application in IDCS.
 - a. Configure OAuth settings, redirect URIs and Authentication Policies.
3. Set up and configure Oracle IDCS App Gateway server.

Create the IDCS Enterprise Application for JD Edwards EnterpriseOne SSO

Use this procedure to configure the Oracle IDCS Enterprise Application for JD Edwards EnterpriseOne.

1. Log in to IDCS administrative console.
2. Click the Menu icon in top left corner.
3. From **Applications** menu, select **Add Application**, and then select **Enterprise Application**.

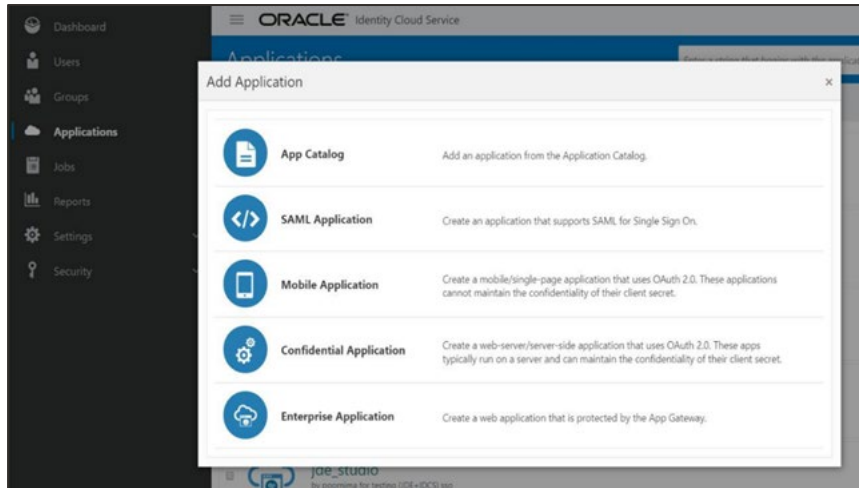


Figure 2. Add Enterprise application

4. Enter the application name and required details; select **Display in My Apps** check box.

Application URL: Enter `https://<app_gateway_hostname>:<sso_port>/jde/E1Menu.maf?jdeowpBackButtonProtect=PROTECTED`

Where `/jde/E1Menu.maf?jdeowpBackButtonProtect=PROTECTED` is the JDE application homepage URL.

NOTE: `<app_gateway_hostname>` is machine FQDN where App Gateway setup is done.


Details OAuth Configuration SSO Configuration Import Users Groups

Details

Application Type: Enterprise Application

* Name: JDE_Dev2oci

Description: IDCS_JDE dev2oci testing

Application Icon:  Upload

* Application URL:

Custom Login URL:

Custom Logout URL:

Custom Error URL:

Linking callback URL:

Tags

Add tags to your applications to organize and identify them. A tag consists of a key-value pair.

+ Add Tag

Settings

Display in My Apps

User can request access

User must be granted the app

Figure 3. Enterprise application details

5. Click **Next**.
6. Expand the **Client Configuration** section.
7. Select the **Configure this application as client now** option.
8. In the Authorization section, complete the following:
 - Select Resource owner, Client Credentials and Refresh token for Allowed Grant Types.
 - Select Client Type as Confidential.
 - Select Introspect as Allowed Operation.
 - For Allowed Client IP Address, select Anywhere.
 - In the Token Insurance Policy:
 - Select Specific as Authorized resources.
 - Select Add App Roles check box.
 - Click **Add Role**.
 - Select **Authenticator Client** role.

The screenshot displays the 'OAuth Configuration' page for an Enterprise application. The navigation tabs include 'Details', 'OAuth Configuration', 'SSO Configuration', 'Import', 'Users', and 'Groups'. The main content is organized into sections: 'Resource Server Configurations', 'General Information', and 'Client Configuration'. Under 'Client Configuration', there are radio buttons for 'Configure this application as a client now' (selected) and 'Skip for later', with a 'Save' button. The 'Authorization' section includes options for 'Allowed Grant Types' (Resource Owner, Client Credentials, JWT Assertion, SAML2 Assertion, Refresh Token, Authorization Code, Implicit, Device Code, TLS Client Authentication), 'Allow non-HTTPS URLs', 'Redirect URL', 'Logout URL', 'Post Logout Redirect URL', 'Client Type' (Trusted, Confidential, Public), 'Certificates' (Import), 'ID Token Encryption Algorithm' (None), 'Allowed Operations' (Introspect, On behalf Of), and 'Allowed Client IP Address' (Anywhere, In one or more of these network perimeters). The 'Token Issuance Policy' section has radio buttons for 'Authorized Resources' (All, Tagged, Specific) and a table for 'Grant the client access to Identity Cloud Service Admin APIs'.

Resource	Protected	Scope
No data to display.		

App Roles	Protected	
Authenticator Client	No	X

Figure 4. OAuth Configuration details for Enterprise application

9. Click **Next**.
10. In the SSO Configuration tab, expand the **Resources** section.
11. Click **Add** to add values and select the following resources:

Resource 1

- Resource name – `jde`
- Resource URL - `/jde/.*`
- Select Use regex expressions check box.
- Click **Add Resource**.

The 'Add Resource' dialog box contains the following fields and options:

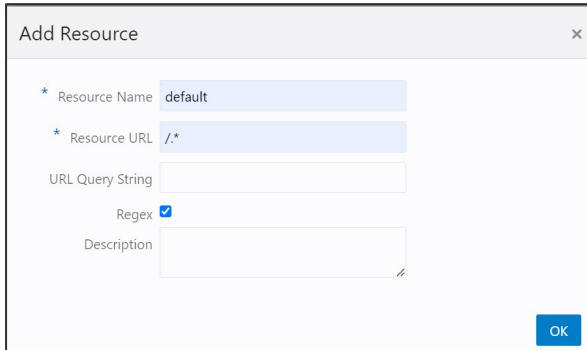
- Resource Name:** `jde`
- Resource URL:** `/jde/.*`
- URL Query String:** (Empty)
- Regex:**
- Description:** (Empty)

An 'OK' button is located at the bottom right of the dialog.

Figure 5. Add jde Resource details

Resource 2

- Resource Name – default
- Resource URL - /.*
- Select Use regex expressions check box.
- Click **OK**.



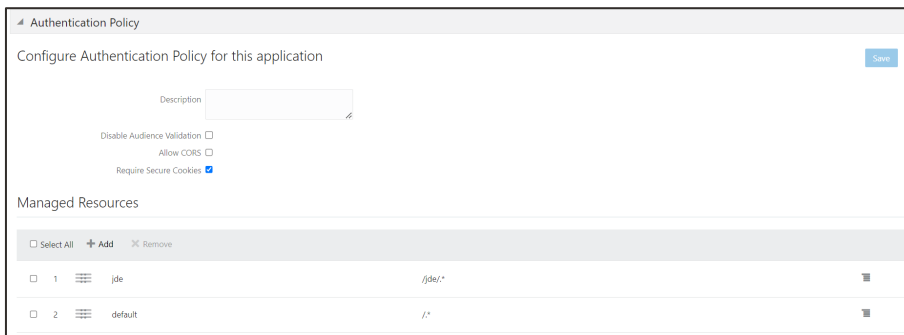
The screenshot shows a dialog box titled "Add Resource". It contains the following fields and controls:

- * Resource Name: default
- * Resource URL: /.*
- URL Query String: (empty)
- Regex:
- Description: (empty)
- OK button

Figure 6. Add default Resource details

12. Expand the Authentication Policy Section and add the below details:

- Select the **Require Secure Cookies** check box.



The screenshot shows the "Authentication Policy" configuration page. It includes a "Save" button in the top right. The "Configure Authentication Policy for this application" section contains a "Description" field and three checkboxes: "Disable Audience Validation" (unchecked), "Allow CORS" (unchecked), and "Require Secure Cookies" (checked). Below this is a "Managed Resources" section with a table:

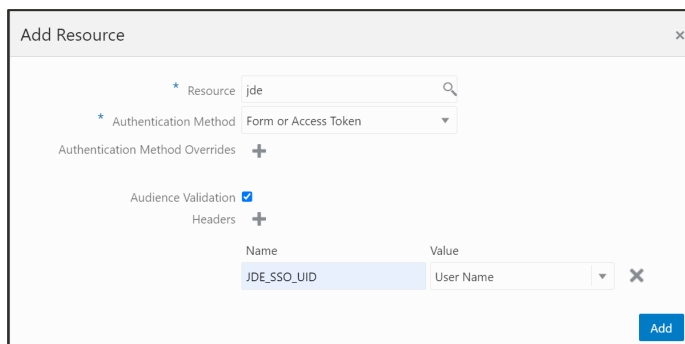
ID	Name	URL
1	jde	/jde/*
2	default	/*

Figure 7. Add Authentication Policy details

- Click **Add** and add the following two policies:

Priority 1

- Resource – jde
- Authentication Method – Form or Access Token
- Select the Audience Validation check box
- In the Headers section, pass custom header JDE_SSO_UID and map it to User Name



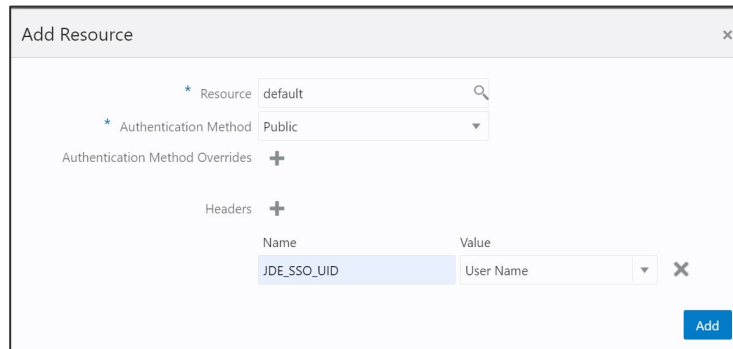
The screenshot shows the "Add Resource" dialog box for the "jde" resource. It contains the following fields and controls:

- * Resource: jde
- * Authentication Method: Form or Access Token
- Authentication Method Overrides: +
- Audience Validation:
- Headers: +
- Name: JDE_SSO_UID
- Value: User Name
- Add button

Figure 8. Add authentication method for jde resource

Priority 2

- Resource – default
- Authentication Method – Public
- Select the Audience Validation check box
- In the Headers section, pass custom header, select JDE_SSO_UID and map it to User Name



The screenshot shows a window titled "Add Resource" with a close button (x) in the top right corner. Inside the window, there are several fields and sections:

- Resource:** A text input field containing "default" with a search icon on the right.
- Authentication Method:** A dropdown menu showing "Public".
- Authentication Method Overrides:** A section with a plus sign (+) icon.
- Headers:** A section with a plus sign (+) icon.
- Header List:** A table with two columns: "Name" and "Value". The first row has "JDE_SSO_UID" in the "Name" column and "User Name" in the "Value" column. There is a close icon (x) to the right of the table.
- Add Button:** A blue button labeled "Add" at the bottom right.

Figure 9. Add authentication method for default resource

Note: JDE_SSO_UID is a mandatory attribute to perform SSO. You must map JDE_SSO_UID to the IDCS User name, and ensure same user exists in JD Edwards EnterpriseOne Java Application Server (JAS) application as well.

13. Save and activate the application.
14. When the application is activated, a client ID and client secret are generated in the General Information section of OAuth Configuration tab.
15. In the Groups and Users section, assign users and groups that must have access to the application.

Set Up an Oracle IDCS App Gateway

This section of the document contains a subset of the complete information provided by Oracle in:

[Set Up an App Gateway.](#)

Download and Extract the App Gateway Binary File

The App Gateway binary file you download from Identity Cloud Service console is a compressed (.zip) file. This file contains an Open Virtual Appliance (.ova) file which you use to install the App Gateway server.

To download and extract the App Gateway binary file:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Downloads**.

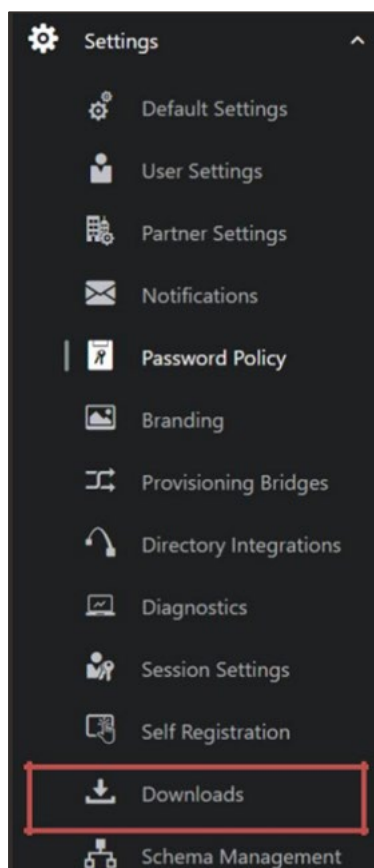


Figure 10. IDCS admin console settings

2. In the Downloads page, click **Download** to the right of **App Gateway for Identity Cloud Service**.

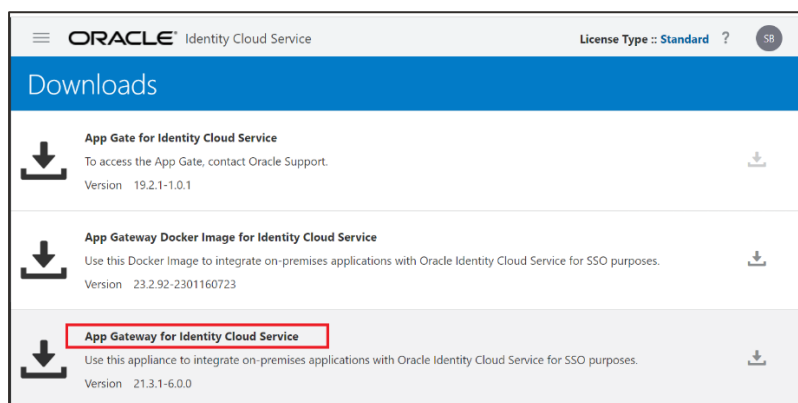


Figure 11. Download App Gateway for Identity Cloud Service

3. Verify that a Success status appears to the right of **App Gateway for Identity Cloud Service**.
4. Extract the content of the compressed (.zip) file you downloaded to a location on your desktop. For Example, `c:\temp`.

The `c:\temp\app-gateway-<version>.ova` file will be created.

Important: Before installing the binary file for App Gateway, you must register it as described in the *Register an App Gateway* section of this document.

Note: As described in the Oracle documentation for [Administering Oracle Identity Cloud Service](#), in the section [Set Up an App Gateway](#), the App Gateway can be set up using below methods:

- Install App Gateway on Oracle Cloud Infrastructure
- Install App Gateway using Oracle VM Virtual Box Software
- Deploy the Oracle App Gateway Docker Container

Register an App Gateway

Before installing the binary file for App Gateway that appears on the Downloads page, you must register your App Gateway using the Identity Cloud Service console.

To register an App Gateway, you must add hosts and associate each host to an enterprise application your App Gateway will protect:

In the **Hosts** pane, you define host identifiers. Each host identifier represents a domain name and port number App Gateway uses to proxy an enterprise application.

In the **Apps** pane, you associate an enterprise application with a host identifier.

To register an App Gateway, you must be assigned to either the **Identity Domain Administrator** role or the **Security Administrator** role.

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Security**, then click **App Gateways**, and click **Add**.
2. In the **Details** pane, specify the name of your App Gateway, and then click **Next (>)**.

Figure 12. Add App-Gateway

3. In the **Hosts** pane, click **Add**.
4. In the **Add Host** dialog, provide a name in the **Host Identifier** field.
5. Enter the **Host** and **Port** values that the App Gateway server will use to respond to HTTP requests.

The port number you provide in this step is used by the App Gateway server to respond to HTTP requests.

6. To have your App Gateway listen to HTTP requests in secure mode (HTTPS), select the **SSL Enabled** check box. Otherwise, clear this check box and your App Gateway will listen to non-secure HTTP requests only.
7. If you select the **SSL Enabled** check box, then complete the **Additional Properties** field with the following values to specify the certificate key pair the App Gateway server will use, protocols and ciphers for SSL:

Copy

```
ssl_certificate /usr/local/example.com.rsa.crt;
```

```
ssl_certificate_key /usr/local/example.com.rsa.key;  
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
ssl_ciphers HIGH:!aNULL:!MD5;
```

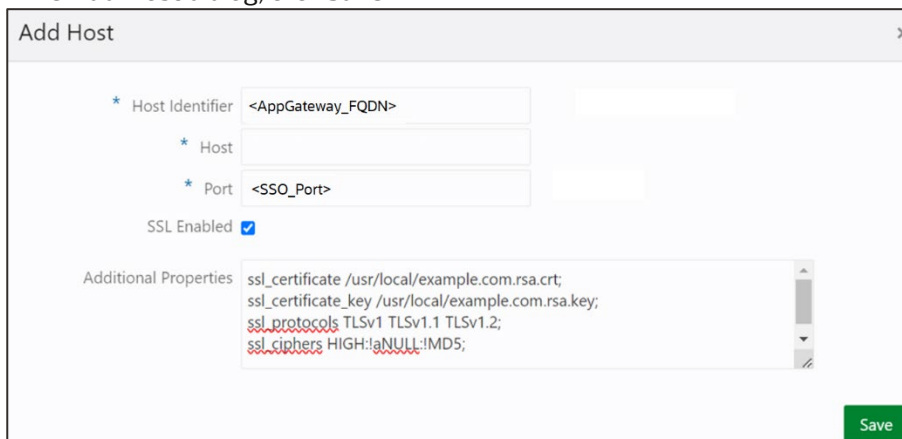
The **/usr/local/example.com.rsa.crt** is the full path of a certificate file in the App Gateway server. The **/usr/local/example.com.rsa.key** is the secret key of that certificate file. You must upload both files to the App Gateway server after you install the App Gateway binary file.

Note: Starting with App Gateway OVA version 20.4.1-4.0.0, App Gateway will work only in SSL/HTTPS mode. Users must leverage their preferred methods and processes when generating keys and certificates.

Note the following considerations:

- a. If there is no load balancer in front of App Gateway, then complete the **Additional Properties** as specified above.
- b. If App Gateway is configured to be running behind a load balancer, then the load balancer must be listening over SSL/HTTPS.
- c. If the load balancer is listening over SSL/HTTPS and SSL is not enabled in the App Gateway settings, then the load balancer must pass the header (Name: `is_ssl` Value: `ssl`) to App Gateway.

8. In the **Add Host** dialog, click **Save**.



The screenshot shows the 'Add Host' dialog box. It has the following fields and settings:

- Host Identifier:** <AppGateway_FQDN>
- Host:** (empty field)
- Port:** <SSO_Port>
- SSL Enabled:**
- Additional Properties:** `ssl_certificate /usr/local/example.com.rsa.crt;
ssl_certificate_key /usr/local/example.com.rsa.key;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers HIGH:!aNULL:!MD5;`
- Save:** A green button at the bottom right.

Figure 13. App Gateway host details

9. In the **Hosts** pane, click **Next >**.

10. If you have previously registered an enterprise application in Oracle Identity Cloud Service, then in the **Apps** pane, click **Add**.

11. In the Assign an App to gate window, map App Gateway to an enterprise application using the values below, and then click **Save**.

- a. **Application:** Select the enterprise application you want to protect using this App Gateway.
- b. **Select a Host:** Select the host identifier to which the App Gateway will proxy the enterprise application.
- c. **Resource Prefix:** Enter the URL prefix used by App Gateway to proxy the enterprise application.
- d. **Origin Server:** This is the actual base URL where the application is hosted. If the application is not directly accessible, but accessible through a web proxy, then enter the URL of the web proxy.

Note: Origin Server should be in form of - <protocol>://<ip/hostname>:<port>

- e. **Additional Properties:** This is an optional field. For more information, see [Assign an Enterprise Application to an App Gateway](#).

12. Click **Finish**.

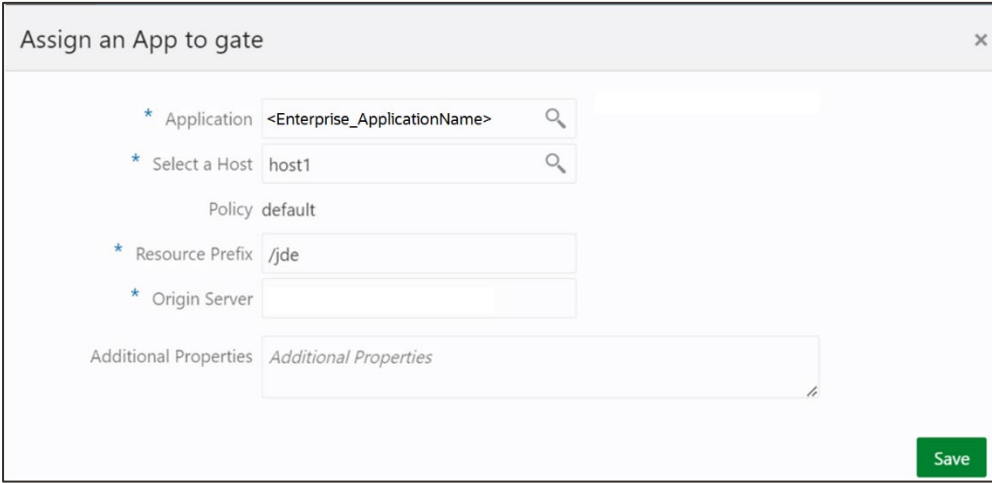


Figure 14. Assign Enterprise application to App Gateway host

13. In the **App Gateway Details** page, note the value of the **Client ID**.

14. Click **Show Secret** and note the value of the **Client Secret**.

The **Client ID** and **Client Secret** are equivalent to a credential (for example, an ID and password) that your App Gateway server uses to communicate with Oracle Identity Cloud Service. You will need these values when you configure the App Gateway server.

15. In the **Navigation Drawer**, click **App Gateways**.

16. In the **App Gateways** page, select your App Gateway, click **Activate**, and then click **OK** in the **Confirmation** window to activate your App Gateway.

Configure the App Gateway Server

This section of the document contains a subset of the complete information provided by Oracle in:

[Configure the App Gateway Server.](#)

Before you start the App Gateway server for the first time, you need to configure the server to connect with Oracle Identity Cloud Service.

1. Use a SSH client such as PuTTY and the following credentials to log in to the App Gateway server.
 - **Localhost login:** oracle
 - **Password:** cloudgateR0X!
You are required to change the provisioned password on the first login.
2. Run the `sudo yum updateinfo list security all` command and provide sudo password. This command lists the security errata for your App Gateway Oracle Linux server. To update all packages for which security-related errata are available to the latest versions of the packages, enter `sudo yum --security update`.
3. Run the `telnet <idcs-tenant>.identity.oraclecloud.com` command to confirm that the App Gateway server can reach the Oracle Identity Cloud Service instance.
4. Restart the App Gateway server after applying the updates.
5. Navigate to the `/scratch/oracle/cloudgate/ova/bin/setup` folder, and then edit the `cloudgate-env` file present in this folder (`vi cloudgate-env`).
6. Enter values for the following parameters, and then save the file:
 - **IDCS_INSTANCE_URL:** The URL of your Oracle Identity Cloud Service instance. For example, `https://idcs-123456789.identity.oraclecloud.com`
 - **CG_APP_TENANT:** The tenant name of the Oracle Identity Cloud Service instance. For example, `idcs-123456789`
 - **CG_APP_NAME:** The client ID value that you noted during the App Gateway registration in Identity Cloud Service console.
 - **CG_APP_SECRET:** The client secret value that you noted during the App Gateway registration in Identity Cloud Service console.
 - **CG_CALLBACK_PREFIX:** If App Gateway is configured in SSL mode (HTTPS), then set the value to `https://%hostid%`. Otherwise, use `http://%hostid%` as the value for this parameter.

Note: Starting with App Gateway OVA version 20.4.1-4.0.0, the **CG_CALLBACK_PREFIX** value must be `https` (`https://%hostid%`).

```

IDCS_INSTANCE_URL="https://idcs-abcd1234abcd1234abcd1234abcd1234.identity.oraclecloud.com"

# Cloud Gate Callback Prefix
#
# The URL prefix used to construct the "callback" URL that Cloud Gate passes to
# IDCS. IDCS will redirect browsers to Cloud Gate using this URL - eg: to
# complete the OAuth Browser Login Flow.
#
# This may be a valid URL - eg: http://my-cloudgate.my-domain.com
# or it may be a template URL
# - eg: https://%tenant%.my-domain.com
#     - where Cloud Gate will replace %tenant% with the appropriate IDCS
#       Tenancy.
# - eg: http://%hostid% or https://%hostid%
#     - where Cloud Gate will replace %hostid% with the value of the Host
#       request header.
#
# Note: the protocol (http vs. https) must be set correctly.
CG_CALLBACK_PREFIX="https://%hostid%"

# Cloud Gate Application / OAuth Client details
#
# The IDCS Tenancy that contains the Cloud Gate Application.
CG_APP_TENANT="idcs-34567890123456789012345678901234"
# The Name (or Client ID) of the Cloud Gate Application.
CG_APP_NAME="cg-987654321098765432109876543210"
# The secret of the Cloud Gate Application.
CG_APP_SECRET="0/c31f3-2c7z-4feb-96fb-3c16543bd049"

```

Figure 15. Configure Cloudgate-env file

7. Confirm that the resolver entry in `/usr/local/nginx/conf/nginx-cg-sub.conf` has the right DNS server IP address.

Run the `nslookup <your_identity_cloud_service_domain>` command and note Server IP Address.

```

[oracle@appgateway-stripes ~]$ nslookup idcs-abcd1234abcd1234abcd1234.identity.oracle.com
Server:
Address:

```

Figure 16. Run nslookup command for idcs domain

Update resolver entry in the `/usr/local/nginx/conf/nginx-cg-sub.conf` with Server IP address you noted in previous step.

```

[oracle@appgateway-stripes ~]$ cat /usr/local/nginx/conf/nginx-cg-sub.conf
#####
# Cloud Gate: Supplementary Configuration - Nginx Edition - nginx-cg-sub.conf
#####
#
# This file contains required configuration for Cloud Gate subrequests.
# This file must be included by nginx-cg.conf inside each subrequest block.
# You must configure the first section according to your network environment.
#
#####
#
# Subrequest Networking Configuration (MUST BE CONFIGURED FOR ENVIRONMENT)
#
#####
# DNS Server - Used to resolve upstream hostnames i.e. IDCS URL
resolver                127.0.0.1;

```

Figure 17. Update resolver details in nginx-cg-sub.conf file

8. Navigate to the location (`cd /scratch/oracle/cloudgate/`) and upload certificates generated, change the ownership of certificate to Oracle user.

```
[oracle@localhost cloudgate]$ ls
21.3.1-6.0.0 88 wallet appgate.rsa.crt appgate.rsa.csr appgate.rsa.key home INSTALLED_VERSION c
You have new mail in /var/spool/mail/oracle
[oracle@localhost cloudgate]$ pwd
/scratch/oracle/cloudgate
```

Figure 18. Upload certificates

9. In the `/scratch/oracle/cloudgate/ova/bin/setup` folder, run `./setup-cloudgate` command. When prompted, enter `y` to proceed with the configuration.

Note: For OVA version 20.4.1-4.0.0 and greater, after running the `./setup-cloudgate` command, the values for `CG_APP_NAME` and `CG_APP_SECRET` are automatically deleted for security reasons.

The App Gateway service and agent service will start after the configuration is complete.

Configure the JD Edwards EnterpriseOne HTML Server for Oracle IDCS App Gateway

Use this procedure to configure the JD Edwards EnterpriseOne HTML Server.

1. Log in to JD Edwards EnterpriseOne Server Manager Console.

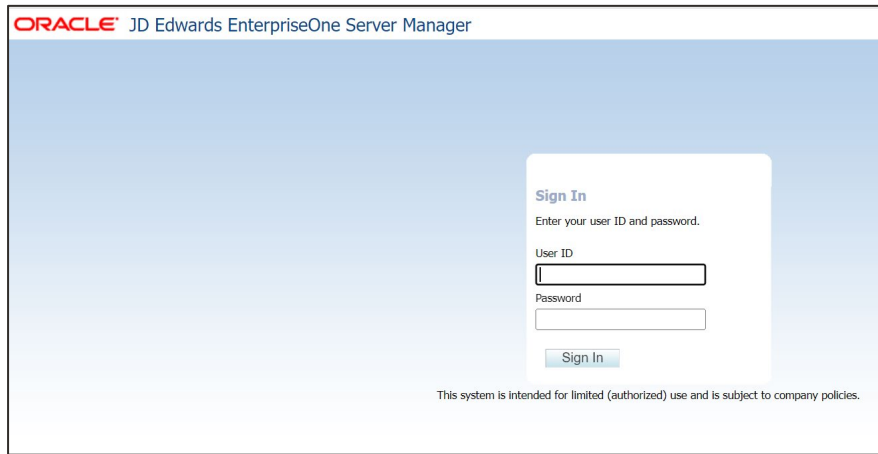


Figure 19. JDE Server manager console Log in

2. Navigate to Select Instance and select **EnterpriseOne HTML Server**.

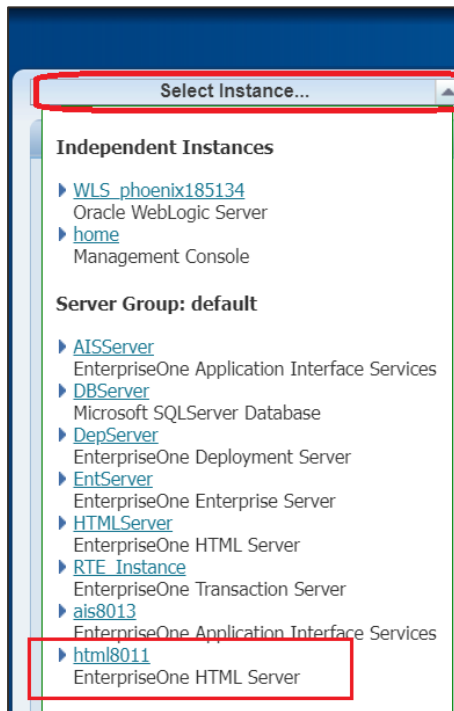


Figure 20. JAS instance

3. Navigate to Configuration, Select **Advanced view** and click **Security**.

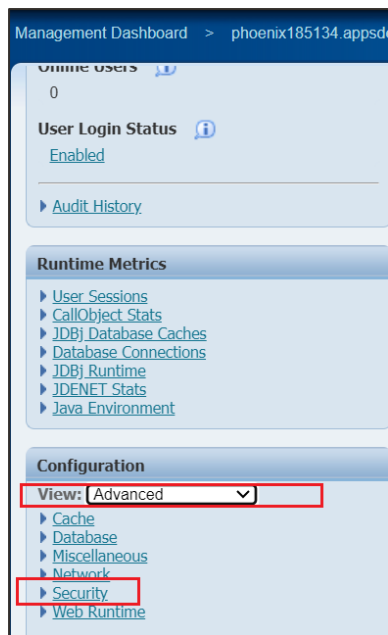


Figure 21. Advanced security configuration

4. Click the Security Options and select the below check boxes:

- a. Select the Enable Oracle Access Manager option.
- b. Provide the App Gateway log out URL. For example:

`https://<appgateway_hostname>:4443/cloudgate/logout.html`

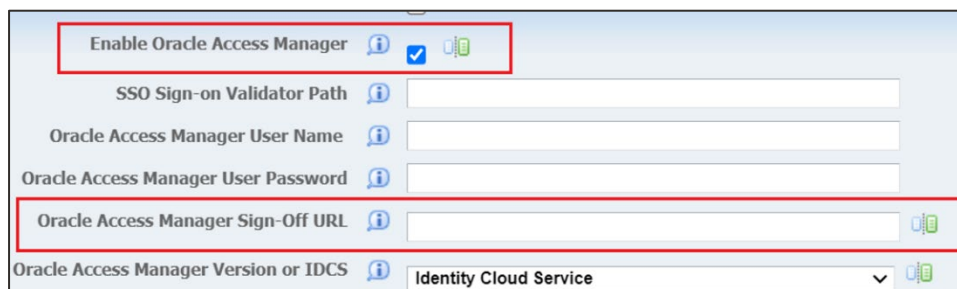


Figure 22. Configure JAS with IDCS details

5. Click **Apply** to save the configuration.
6. Stop and start the JAS server to restart the JDE Server.

Test the Integration

Using IDCS App Gateway URL

To test the setup for this integration of IDCS App Gateway to JD Edwards, use this procedure.

1. Access the application using Application URL that is configured in the Enterprise application in IDCS-

`https://<appgateway_hots>:<sso_port>/jde/E1Menu.maf?jdeowpBackButtonProtect=PROTECTED`

2. Above URL will redirect to IDCS login page.
3. Enter User Name and Password and click **Sign-in**.
4. Approve the second factor of authentication (if configured).
5. User will be redirected to JAS dashboard page.
6. On JAS dashboard page, click Menu in top right corner.
7. Click **Sign Out**.
8. User will be redirected to the IDCS login page.

Using the IDCS My Apps Feature

Prerequisites: Select **Display in My Apps** check box in the Details tab of Enterprise Application and User is added to enterprise application user and groups section.

1. Log in to the IDCS administrative console.
2. In the top right corner of the administrative console, click Menu.
3. Click **My Apps**.
4. On **My Apps** page, click the **Enterprise Application** under test.
5. The JD Edwards HTML (JAS) application opens in a new tab.
6. The user should be displayed with JAS dashboard page.
7. On JAS dashboard page, click Menu in top right corner.
8. Click **Sign Out**.
9. User will be redirected to the IDCS login page.

Conclusion

Oracle JD Edwards EnterpriseOne customers can leverage the capabilities of Oracle Identity Cloud Service to enable Single Sign-On on their JD Edwards environment. This provides higher level of authentication and authorization of users who access the system, making the system more secure and improving the security posture of the organization.

Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

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

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120