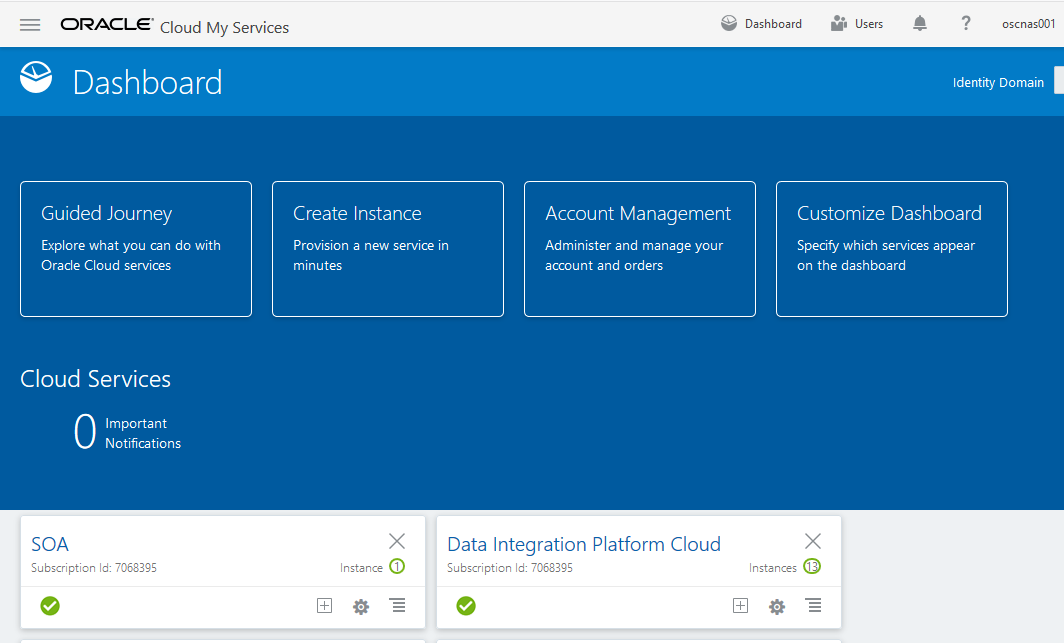
# Steps to configure agent in OAUTH mode (ADIPC)

## Register a trusted application in your Identity Domain

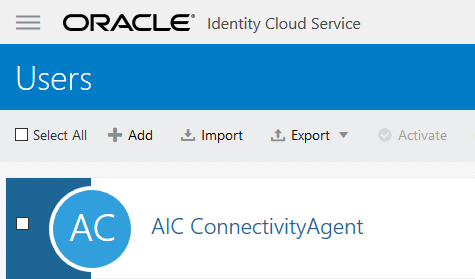
1. Log into the cloud
2. From the Dashboard click on the “Users” icon on top



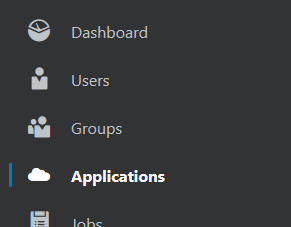
1. Click on “Identity Console” button



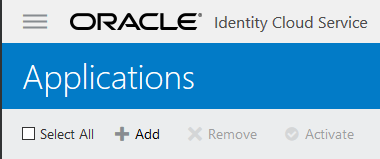
1. Using the left corner hamburger menu, open the panel



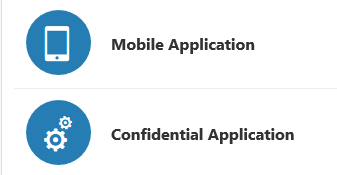
1. In the panel select “Applications”



1. Click on “Add” to create a new trusted application



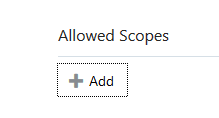
1. Select “Confidential Application”



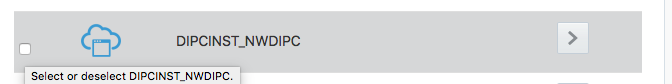
1. In the “Details” screen, provide the following information:
   1. A name for your application
   2. Description

Click on “Next” button

1. In the “Client” screen, select “Configure this application as a client now” and provide the following information:
   1. Allowed Grant Type: Resource Owner, Client Credentials, JWT Assertion, and Refresh Token
   2. Allowed Scopes
      1. Click on “+ Add”



* + 1. Select “DIPCINST\_NWDIPC” (it is the DIPC instance we created), click on the box



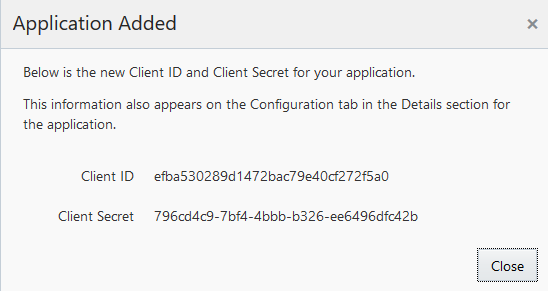
* + 1. Click in “Add” button



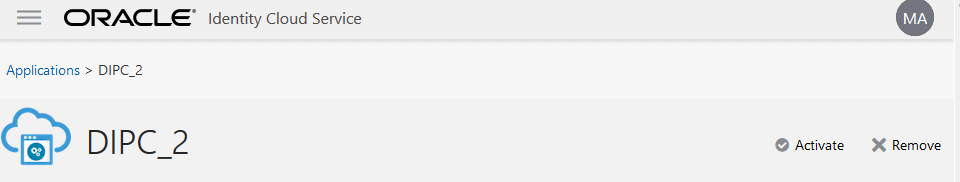
* + 1. Copy that URL and reserve it since you will need it later

Click on “Next” button

1. In the “Resources” screen, on the “Expose APIs to Other Applications” section, select “Skip for later”, and then click “Next” button
2. In the “Web Tier Policy” screen, in the “Web Tier Policy” section, select “Skip for later”, and then click “Next” button
3. In the “authorization” screen do not change anything and click “Finish” button.
4. A screen with the Client and the Secret will come up, copy and save it along the application URL you copied in step 9.b.iv and the URL to the ID server



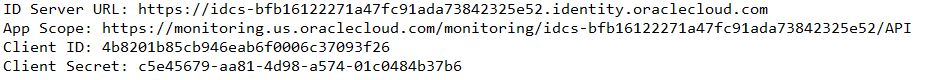
1. Click on “Close” button
2. The application has been added, now click on “Activate” hyperlink on top right



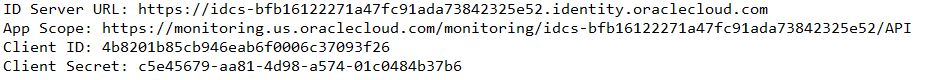
NOTE: At this point you should have a file with the following information:

* Id Server URL
* Secure Application URL
* Client ID
* Client Secret

It should look something like this

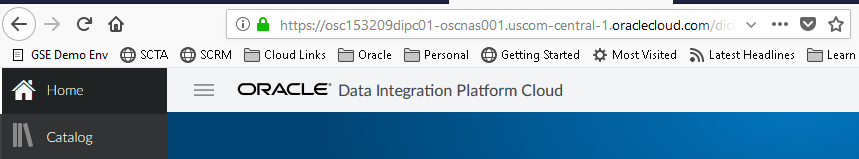


App Scope: https://289EF634259C46B7B5B698A9B41FC78C.adipc.ocp.oraclecloud.com:443urn:opc:resource:consumer::all

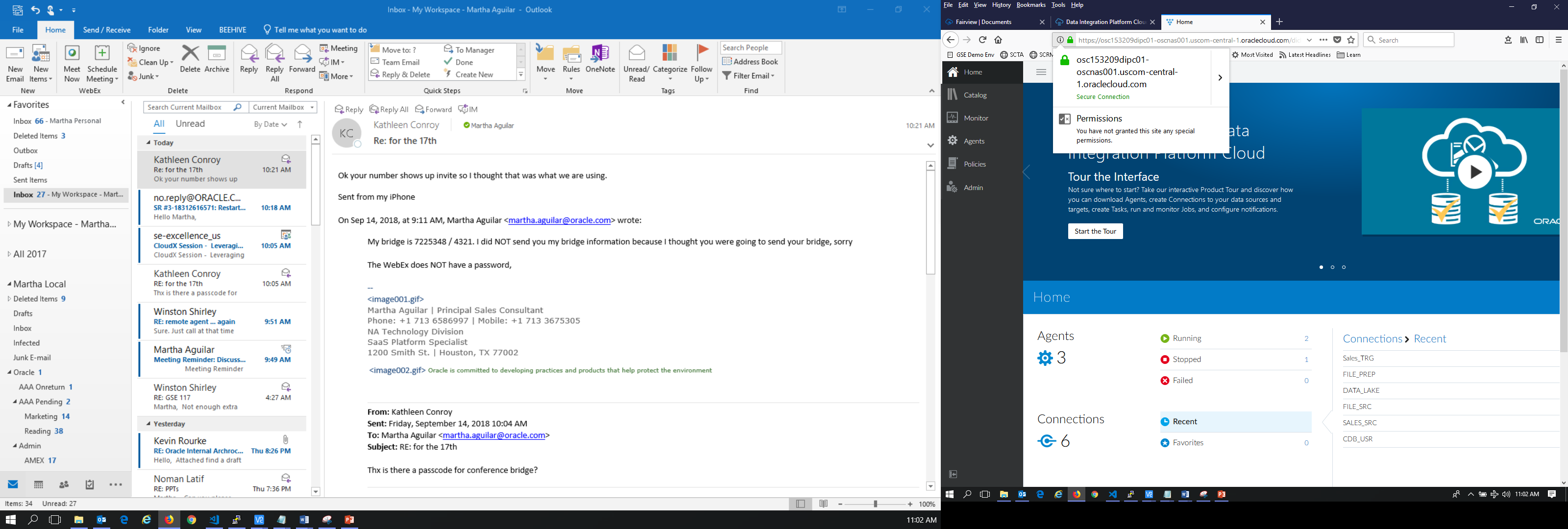


## Getting the ADIPC Server Certificate

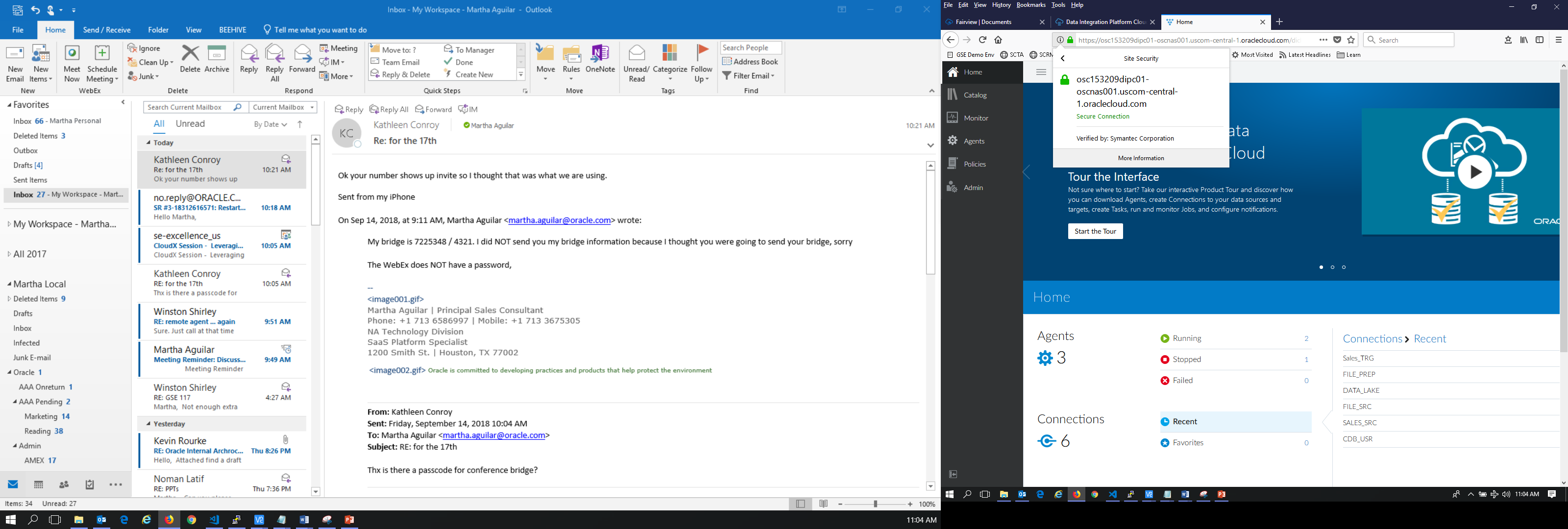
1. Log into your ADIPC server
2. Once in the “Home” page, click on the green padlock icon on the left of the address field of your browser



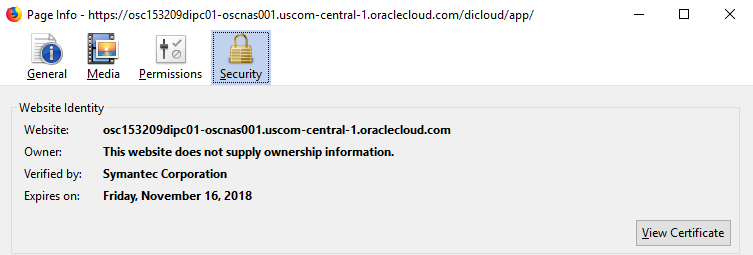
1. Click on the arrow on the right side of the listed secure connection



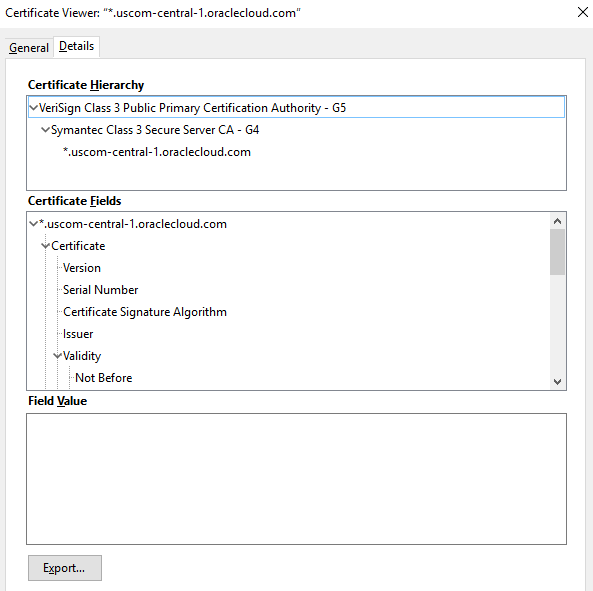
1. Click on “More Information” hyperlink of the Site Security pop-up



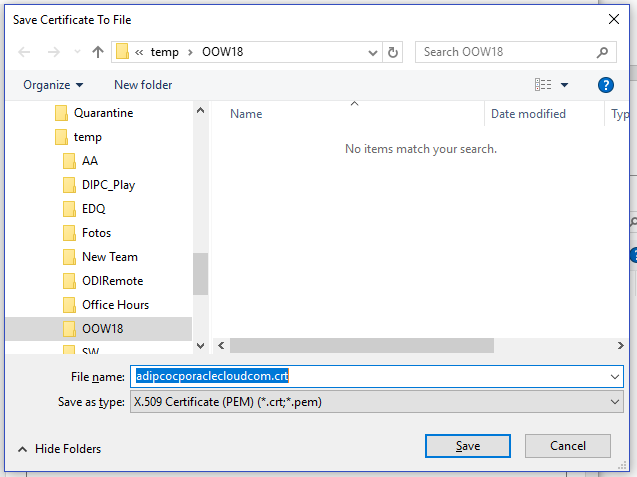
1. In the “Website Identity” section of the “Security” tab click “View Certificate” button



1. In the “certificate Viewer” applet in the “Details” tab, click “Export …” button



1. Browse to the directory you want to store the certificate and save the CRT file. Be sure to get rid of the “-“, located at the beginning of the default name. Click “Save’ button



1. Close all applets

## Add Certificate to Keystore

1. Log into the machine in which you will install the remote agent with the login you will use to install the remote agent
2. Set your JAVA\_HOME variable (to the directory where your JDK resides). For example:

export JAVA\_HOME=/u01/app/oracle/product/12.2.0/dbhome\_1/jdk

1. Import the client side certificate into the cacerts in your system. Execute:

$JAVA\_HOME/bin/keytool -import -alias <CERTIFICATE\_FILE> -keystore $JAVA\_HOME/jre/lib/security/cacerts -file /<PATH>/<CERTIFICATE\_FILE>

(For example: $JAVA\_HOME/bin/keytool -import -alias adipcocporaclecloudcom -keystore $JAVA\_HOME/jre/lib/security/cacerts -file /home/oracle/Certificate/ adipcocporaclecloudcom.crt)

1. Provide password for cecerts (the default password is “changeit”)
2. Answer “yes” to question “trust this certificate?”

## Unload Remote Agent

1. Log into the machine in which you will install the remote agent
2. Open a browser and Navigate to your ADIPC server
3. Login into your ADIPC server
4. Click on “Agents” (left part of your screen)
5. Click on "Download Installer" button
6. Open the dropdown menu and select the Operating System of your choice; in our case “Linux”
7. Once you have selected the operating system, you can choose the components that you would need in your remote agent. Select "Oracle 12c" and "Data Integrator (ODI)" then click on "Download" button.
8. Select “Save File” and the click “OK”, to download the file to your “on-premise” machine

## Install the Remote Agent

1. Create a directory for the agent’s files, execute:

mkdir ADIPCagent

1. Move the downloaded file to that new directory, execute:

mv Downloads/\* ADIPCagent

1. Move to the new directory, execute:

cd ADIPCagent

1. Unzip the file, execute:

unzip agent-linux.64.bit.zip

1. Move to the agent directory, execute:

cd dicloud

1. Execute command to install agent:

./dicloudConfigureAgent.sh -recreate -debug -dipchost=<YOUR\_ADIPC SERVER> -dipcport=443 -user=<YOUR\_USER> -password=<YOUR\_PASSWORD> -authType=OAUTH2 -idcsServerUrl=<YOUR\_ID\_SERVER> -agentIdcsScope=<YOUR\_SECURE\_APP>

-agentClientId=<CLIENT\_ID> -agentClientSecret=<CLIENT\_SECRET>

where:

<YOUR\_ADIPC SERVER> - Just the server portion of the URL to ADIPC. For example: osc153209ADIPC01-oscnas001.uscom-central-1.oraclecloud.com when the URL to ADIPC is [https://osc153209ADIPC01-oscnas001.uscom-central-1.oraclecloud.com/dicloud](https://osc153209dipc01-oscnas001.uscom-central-1.oraclecloud.com/dicloud) .

<YOUR\_USER> - This is the login you use to log into Oracle Cloud/ADIPC server

<YOUR\_PASSWORD> - This is the password of the login you use to log into Oracle Cloud/ADIPC server

<YOUR\_ID\_SERVER> - This is your ID Server URL, you got this information in the first section of this document

<YOUR\_SECURE\_APP> - This is your Secure Application URL, you got this information in the first section of this document

<CLIENT\_ID> - This is the Client ID you got in the first section of this document

<CLIENT\_SECRET> - This is the Client Secret you got in the first section of this document

For example:

./dicloudConfigureAgent.sh -recreate -debug -dipchost=nwdipc-nationwideoipa.adipc.ocp.oraclecloud.com  -dipcport=443 -user=Diamona@nationwide.com  -password=XXXXXXXXXXX   -authType=OAUTH2 -idcsServerUrl=https://idcs-6851a71771984f148c034326df545d32.identity.oraclecloud.com   -agentIdcsScope=https://289EF634259C46B7B5B698A9B41FC78C.adipc.ocp.oraclecloud.com:443urn:opc:resource:consumer::all    -agentClientId=760b54f8377e4e01aab60c5503fdd843  -agentClientSecret=4e201d10-83dc-4f01-a7fb-2dbe422fe4d6

1. New directories will be created, to look at then execute:

ls

1. Edit the “/home/oracle/dipcagent/dicloud/agent/dipcagent001/conf/agent.properties” file and we change the port in which this agent will talk to ADIPC.
2. Modify agent port "agentPort" in parameter file "agent.properties" to the value you prefer (for example 7010)
3. Save and close the file

## Execute the Agent

1. Move to the directory with the necessary commands to start the agent, execute:

cd agent/ADIPCagent001/bin

1. Start the agent by executing:

nohup ./startAgentInstance.sh &

1. Agent is now running. Go back to Firefox and look the “Agent” screen in ADIPC