[http://myexelon.exeloncorp.com/_layouts/1033/Exelon/IMAGES/logo.png](http://myexelon.exeloncorp.com/)

AGS - Compliance Project

AGS Operation Run Book

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approval History**

| **Date** | **Version** | **Description** | **Approver** | **Status** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Contents**

[1. Application Monitoring Manager – Daily Operations Checklist Process 4](#_Toc74150530)

[2. Encrypt password to update in Application Monitoring Manager 7](#_Toc74150531)

[3. Stopping ePeople instance in DST 7](#_Toc74150532)

[Step 1: Epeople Services 9](#_Toc74150533)

[Validate the status of EpeopleDataLoadScheduler job of EWSDATAHUB 9](#_Toc74150534)

[Stop EpeopleDataLoadScheduler job 9](#_Toc74150535)

[Start EpeopleDataLoadScheduler job 9](#_Toc74150536)

[Validate the status of EpeopleAtomFeedConnector job of EWSDATAHUB 9](#_Toc74150537)

[Stop EpeopleAtomFeedConnector job 9](#_Toc74150538)

[Start EpeopleAtomFeedConnector job 9](#_Toc74150539)

[Validate the status of Activemq job for the Atomfeed connector 9](#_Toc74150540)

[Stop Activemq job for the Atomfeed connector 9](#_Toc74150541)

[Start Activemq job for the Atomfeed connector 9](#_Toc74150542)

[Validate the status of tomcat server 9](#_Toc74150543)

[Stop tomcat server 10](#_Toc74150544)

[Start tomcat server 10](#_Toc74150545)

[4. Flat file Reconciliation Process 10](#_Toc74150546)

[5. Management Console Reconciliation Process 10](#_Toc74150547)

[6. Role/Entitlement/Access Policy Maintenance Tasks & Processes 10](#_Toc74150548)

[**a)** **How to retry Failed Task** 10](#_Toc74150549)

[**b)** **How to cancel retried task from resource history** 11](#_Toc74150550)

[**c)** **How to Run Active Directory AdHoc Reconciliation** 12](#_Toc74150551)

[**d)** **Adhoc Reconciliation from HRPC Staging Table to AGS** 14](#_Toc74150552)

[**e)** **Bulk Drop Users From Roles** 17](#_Toc74150553)

[7. Steps to Remove access for terminated user with in 24 hours for NERC access if something is still provisioned 17](#_Toc74150554)

[8. Certificate Management 17](#_Toc74150555)

[9. DB Queries 17](#_Toc74150556)

[10. How to raise CHG request to run update queries on DB 19](#_Toc74150557)

[11. Process to verify Db queries outputs 19](#_Toc74150558)

[12. DB Archival and Logs archival 19](#_Toc74150559)

[**1)** **Cleaning up LOG files** 19](#_Toc74150560)

[13. OIM Admin Email Verification steps 21](#_Toc74150561)

[14. Email Notifications & Verification Process 21](#_Toc74150562)

[**14.1.** OIM ADMIN Email Verification Steps 21](#_Toc74150563)

[15. Process to check Scheduled BI Reports status. 21](#_Toc74150564)

[16. Service Accounts Creation & Password Change Process 21](#_Toc74150565)

[a) AGS ADMIN Account 21](#_Toc74150566)

[17. Governance/management of service accounts 25](#_Toc74150567)

[18. Performance improvement 25](#_Toc74150568)

[19. Onboarding Steps for new team member 25](#_Toc74150569)

[20. REVOKE AGS ADMIN ACCESS 25](#_Toc74150570)

1. **Application Monitoring Manager – Daily Operations Checklist Process**
2. Login to Utility Server

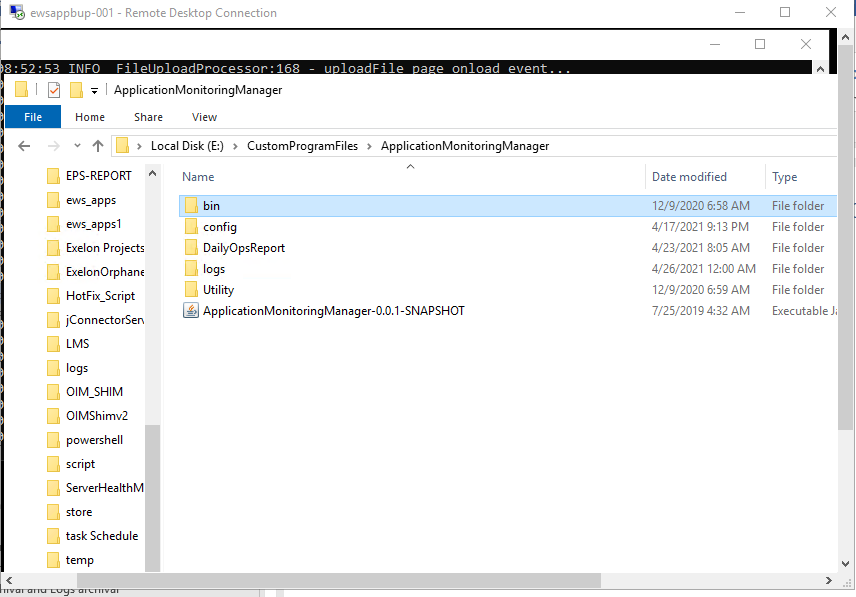
**Host:** EWSAPPBUP-001

**Username:** svc\_EWSSecTomcat\_P

**Passowrd:** <Fetch from cyberark>

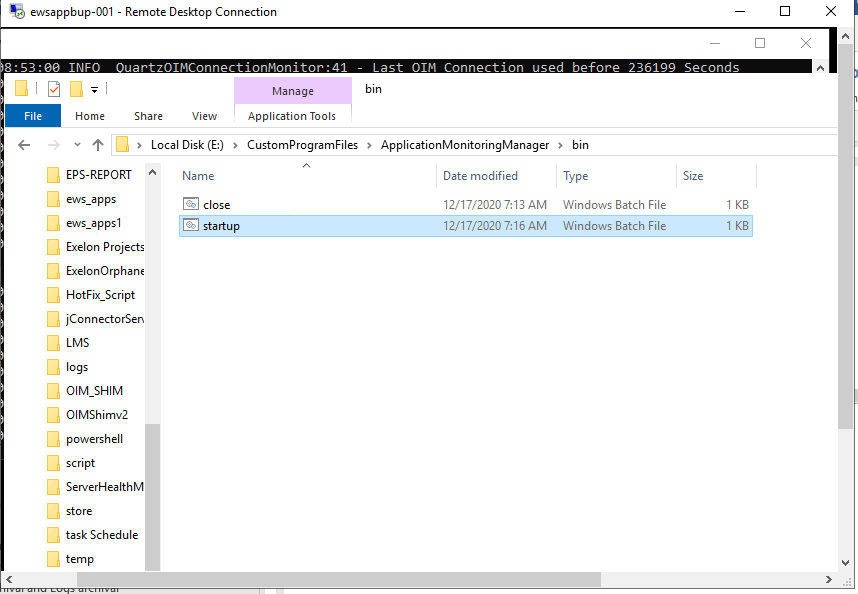
1. Go to Application Monitoring Manager Service

E:\CustomProgramFiles\ApplicationMonitoringManager



1. Start this service

Go to **bin** folder and open **start.bat** file



\*\* We don’t need to run this service daily. Once it starts running, it will keep generating DailyOperationChecklist report every day until servers are rebooted or someone logoff.

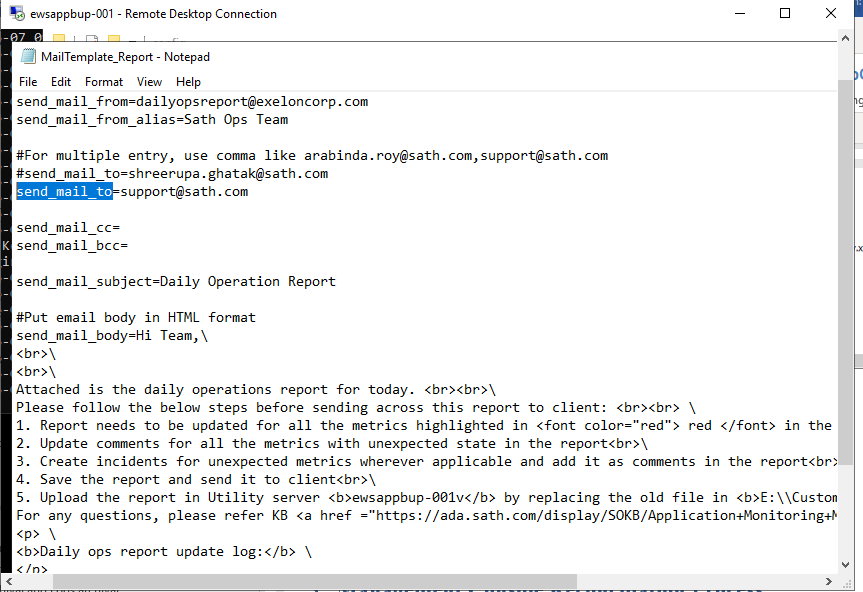
Report will be generated twice in a day at 5:30 PM IST & 6:30 PM IST. We need to consider latest report. If system doesn’t generate 1st report at given time then we need to debug the issue with the service.

1. Reports will be sent on mail. To change receiving mail id and email template

* Open **MailTemplate\_Report.txt** in **config** folder



* Change value in field **send\_mail\_to**

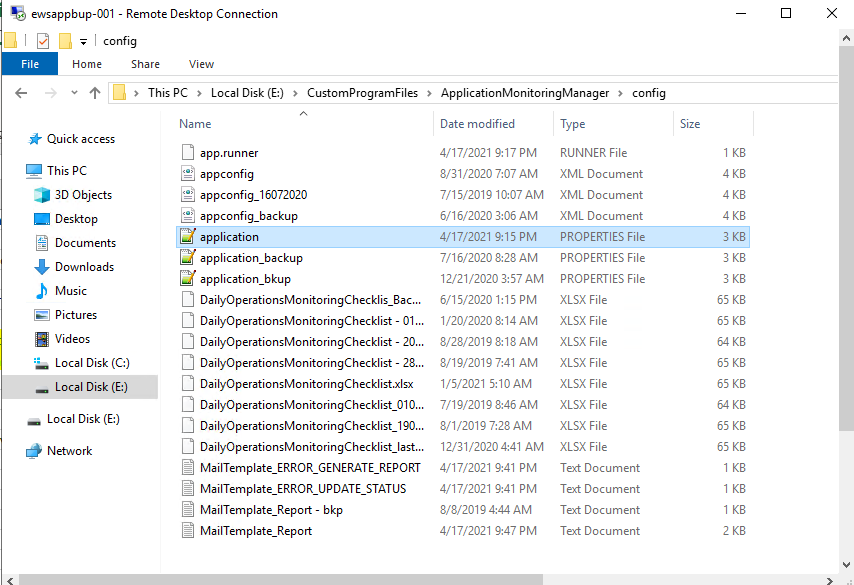


After receiving report, need to process that before sending it to client.

1. Report is generating data from Zabbix interface and some below mentioned DBs

* **Zabbix URL:** <https://ewsreport.exeloncorp.com/zabbix/index.php>
* **AGS DB (IAM\_OIM)**
* **ACAS DB (OIMDBUSER)**
* **Reporting DB (EWSAPP)**
* **Zabbix DB (Mysql://iammntr-ccc-01v.exelonds.com:32769/zabbix)**

1. In case of password change of DB accounts, need to update encrypted passwords in **application.properties** file.



1. **Encrypt password to update in Application Monitoring Manager**
2. **Stopping ePeople instance in DST**

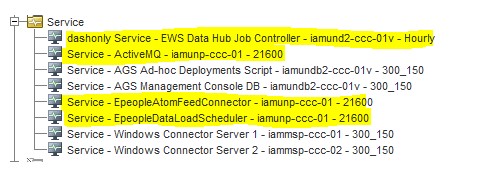
We need to restart ePeople instances during Daylight Savings Time (DST). This section provides a step by step approach to start/stop ePeople instance & AGS / ACAS Scheduler services during DST begin at 2:00 A.M. CST and end after 3:00 A.M. CST. Stop the processes before the DST Start. Once you confirm the time has switched you may proceed with the start processes.

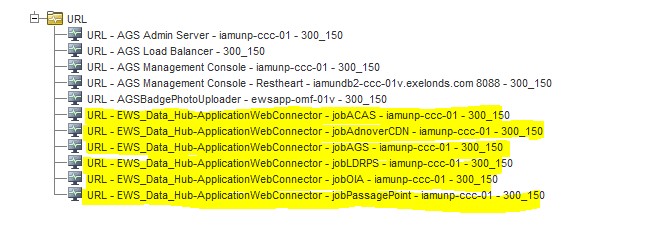
***Schedule:***

* 1st week of March
* 1st week or last week of October

***Process:***

**Before proceeding with the steps, please shut down the following monitors for AGS . Start the monitors back up once done with the steps.**





Step 1: Epeople Services

* Validate the status of EpeopleDataLoadScheduler job of EWSDATAHUB

1. Logged in to iamunp-ccc-01 server using "appserver" sudo access
2. run the command ps -ef | grep EpeopleDataLoadScheduler.jar

* Stop EpeopleDataLoadScheduler job

1. run the command ps -ef | grep EpeopleDataLoadScheduler.jar
2. kill -9 <ProcessID>

* Start EpeopleDataLoadScheduler job

1. cd /apps/EWSDATAHUB/PROD/EPEOPLE\_TO\_EWSDATAHUB
2. export JAVA\_HOME=/apps/EWSDATAHUB/PROD/jdk1.8.0\_201 export PATH=$PATH:$JAVA\_HOME/bin
3. nohup java -jar EpeopleDataLoadScheduler.jar &

* Validate the status of EpeopleAtomFeedConnector job of EWSDATAHUB

1. Logged in to iamunp-ccc-01 server using "appserver" sudo access
2. run the command ps -ef | grep EpeopleAtomFeedConnector.jar

* Stop EpeopleAtomFeedConnector job

1. run the command ps -ef | grep EpeopleAtomFeedConnector.jar
2. kill -9 <ProcessID>

* Start EpeopleAtomFeedConnector job

1. cd /apps/EWSDATAHUB/PROD/ATOMFEED\_SCHEDULER
2. export JAVA\_HOME=/apps/EWSDATAHUB/PROD/jdk1.8.0\_201 export PATH=$PATH:$JAVA\_HOME/bin
3. nohup java -jar EpeopleAtomFeedConnector.jar &

* Validate the status of Activemq job for the Atomfeed connector

1. Logged in to iamunp-ccc-01 server using "appserver" sudo access
2. run the command ps -ef | grep activemq

* Stop Activemq job for the Atomfeed connector

1. run the command ps -ef | grep activemq
2. kill -9 <ProcessID>

* Start Activemq job for the Atomfeed connector

1. cd /apps/EWSDATAHUB/PROD/apache-activemq-5.15.0/bin
2. export JAVA\_HOME=/apps/EWSDATAHUB/PROD/jdk1.8.0\_201 export PATH=$PATH:$JAVA\_HOME/bin
3. ./activemq start

* Validate the status of tomcat server

1. Logged in to iamunp-ccc-01 server using "appserver" sudo access
2. run the command ps -ef | grep tomcat

* Stop tomcat server

1. run the command ps -ef | grep tomcat
2. kill -9 <ProcessID>

* Start tomcat server

1. cd /apps/EWSDATAHUB/PROD/tomcat/apache-tomcat-8.0.46/bin
2. ./startup.sh

1. Run the <http://iamunp-ccc-01.exelonds.com:9090/EWS_Data_Hub-ApplicationWebConnector/faces/JobController.xhtml>2. Click on start all jobs



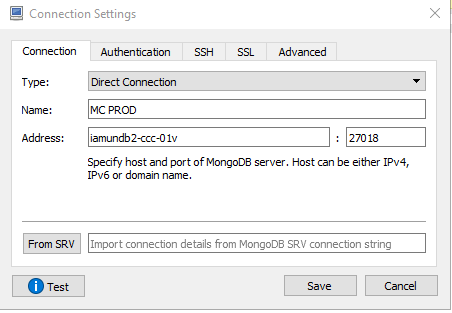
[http://iamuns-omf-01.exelonds.com:8090/EWS\_Data\_Hub-ApplicationWebConnector/faces/JobController.xhtm](http://iamuns-omf-01.exelonds.com:8090/EWS_Data_Hub-ApplicationWebConnector/faces/JobController.xhtml)

[l](http://iamuns-omf-01.exelonds.com:8090/EWS_Data_Hub-ApplicationWebConnector/faces/JobController.xhtml)

1. **Flat file Reconciliation Process**
2. **Management Console Process**

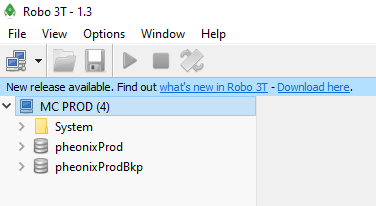
## How to add user into the Management console

1. Download the Robo 3T from the below URI and install it on your VPC
   1. <https://robomongo.org/download>
2. Launch the Robo 3T and click on create on MongoDB Connections
3. Provide the MongoDB connection details as follows and save it.

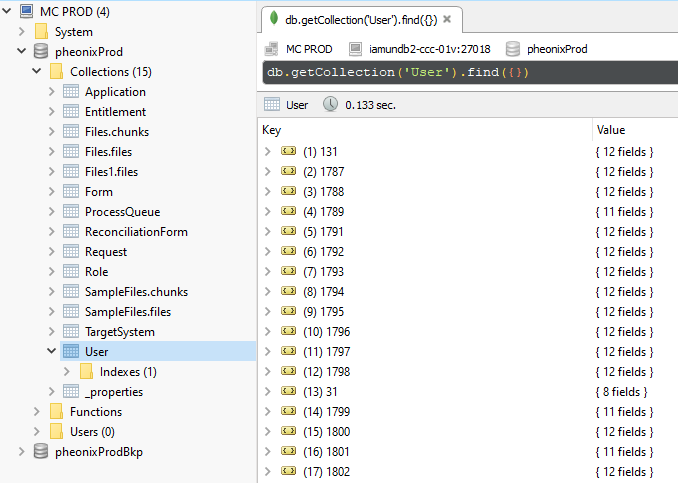


Note: The port 27018 is used for PROD, you can add multiple connections based on other environments.

1. Click on connect, and you will get the below screen, upon successful connection.



1. Navigate to phoenix Prod > Collections > User directory



1. Right click on the User collection and select “Insert Document” and add the following details with your **firstName**, **Login**, **lastName**, **Status**, **employeeNumber**, **displayName as per the AGS.**

Note: Please leave the “\_id” field blank

{

"\_class" : "com.sath.backend.dto.UsrDTO",

"firstName" : "",

"login" : "",

"lastName" : "",

"status" : "",

"employeeNumber" : "",

"displayName" : "",

"roles" : [

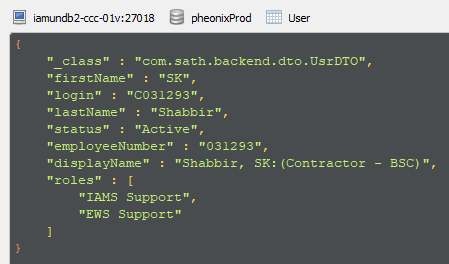
"IAMS Support",

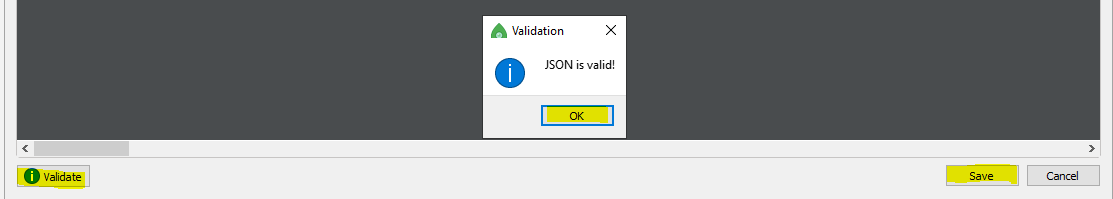
"EWS Support"

]

}

1. Click on validate and save.



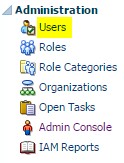


1. Now login into the Management console with your C key and the same network account password.
2. **Role/Entitlement/Access Policy Maintenance Tasks & Processes**
3. **How to check entitlements associated with a role for WF task**
4. **How to retry Failed Task**

* Login to the OIM Identity Console as AGS\_ADMIN using the following URL

**https://ags.exeloncorp.com/identity**

* Navigate to **Users** under the **Administration** section



* Search for the concerned user with User Login information



* Click on the User to open up user information from search result
* Navigate to the Accounts tab of the user



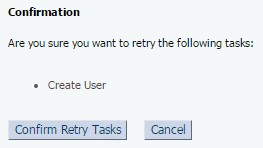
* Select the concerned Application Instance and open **Resource History**



* Select the “**Rejected**” task and click on “**Retry**”



* Click on “Confirm **Retry Tasks**”



* Verify whether the task got completed successfully. The status of the task should change to "**Completed**"

1. **How to cancel retried task from resource history**

**Perform the following steps:**

* Identify the Application Instance.
* Open resource history for the Application Instance and identify the task which is being failing.
* Connect to SQL developer as IAM\_OIM user.
* Identify the APP\_INSTANCE\_KEY of the Application Instance, run below query to identify: **select \* from IAM\_OIM.APP\_INSTANCE where APP\_INSTANCE\_NAME like '%Email%';**
* Run the below query to identify the ORC\_KEY:

**select \* from OIU where usr\_key in (select usr\_key from usr where usr\_login='C08173') and APP\_INSTANCE\_KEY=39;**

* Run the below query to identify the failed task which is being rejected,

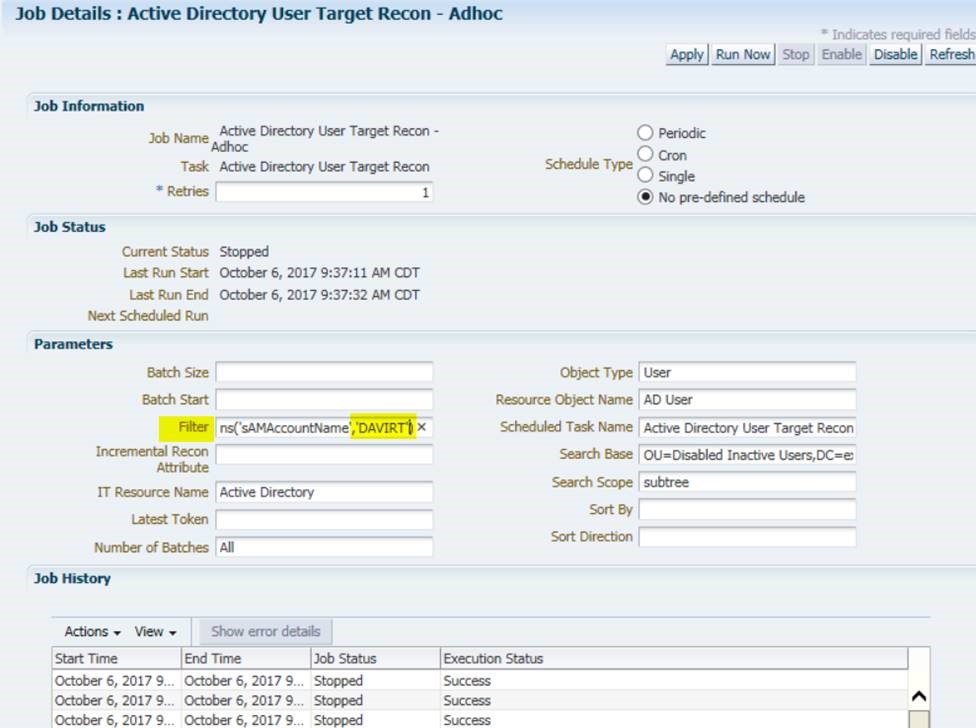
**select osi.sch\_key, osi.orc\_key, osi.mil\_key, to\_char(osi.osi\_assigned\_date,'dd-mon-rrrr hh24:mi:ss') ,to\_char(OSI.OSI\_UPDATE,'dd-mon-rrrr hh24:mi:ss'), osi.rsc\_key, sch.sch\_status, sch.sch\_data, mil.mil\_name, SCH.sch\_update,to\_char(sysdate,'dd-mon-rrrr hh24:mi:ss') from osi, sch, mil where osi.sch\_key = sch.sch\_key and osi.mil\_key = mil.mil\_key and osi.orc\_key in (ORC key you found in step 5) order by sch.sch\_update desc;**

* Match the count of that particular task from AGS identity as well.
* Run the below query to update the required filed that needs to be change,

**UPDATE SCH SET SCH\_STATUS='X' where SCH\_KEY IN SELECT SCH.SCH\_KEY FROM OIU, APP\_INSTANCE, ORC, OSI, SCH, MIL, USR, OS WHERE OIU.USR\_KEY = USR.USR\_KEY AND OIU.APP\_INSTANCE\_KEY = APP\_INSTANCE.APP\_INSTANCE\_KEY AND OIU.ORC\_KEY = ORC.ORC\_KEY AND ORC.ORC\_KEY = OSI.ORC\_KEY AND OSI.SCH\_KEY = SCH.SCH\_KEY AND MIL.MIL\_KEY = OSI.MIL\_KEY and oiu.ost\_key = OST.OST\_KEY and MIL.MIL\_NAME ='Disable User' AND OIU.ORC\_KEY =ORC Key you found in step 5);**

* Verify the changes from AGS identity console that rejected task has been canceled.

1. **How to Run Active Directory AdHoc Reconciliation**
   * Login to **AGS Sysadmin** console using Admin credentials (AGSADMIN account or xelsysadm). The credentials as well as environment specific URL can be found in KeePass.
   * Click on Scheduler
   * Search for ‘Active Directory User Target Recon – Adhoc’. Alternatively, in the search bar, you can also type ‘\*Active\*’, which will list out all the AD Recon Jobs. Then you can select the Adhoc job from that list.
   * In the Filter field, put the Login ID (which you will get from the spreadsheet attached), within single quotes as show below:



* + NOTE: This job can only recon one user at a time, so you need to provide the next Login ID, once the instance of job for a particular user is completed.
  + Click on Apply



* + Click on Run Now



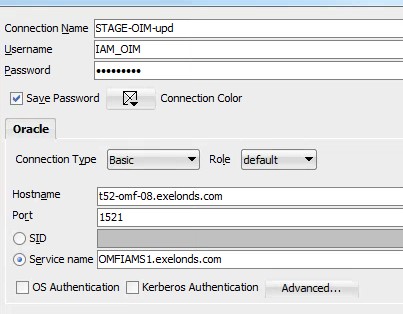
* + Hit Refresh until you see in the Job History that the running instance is successful.



* + Check the user’s AD accounts in the Identity console.

1. **Adhoc Reconciliation from HRPC Staging Table to AGS**

* Open SQL Developer in Exelon network
* Login to the DB of the corresponding environment (i.e. DEV, DEV2, TST, STG) as IAM\_OIM user. Refer to the following connection information sample for the Exelon STG environment



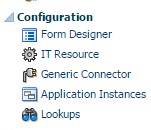
* Run the following query (Note: This is for listing the users who are ready to be brought into AGS from HRPC)

***select emplid, first\_name,last\_name,empl\_status,ce\_action\_flag,manager\_id,ce\_manager\_name,l astupddttm,ce\_comp\_access from ps\_ce\_iamp\_tbl@hrlink where ce\_action\_flag in ('DIS') and empl\_status='9';***

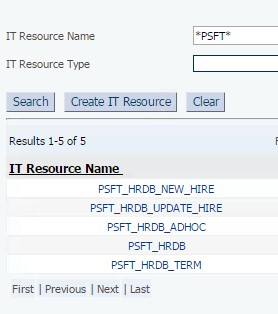
* Update the user attributes as per the requirement (**Note:** Following sample query is for general assistance only)

***update ps\_ce\_iamp\_tbl@hrlink set empl\_status = 'A' ,ce\_action\_flag = 'HIR', manager\_id = '621426',ce\_manager\_name = 'Paparella,Elisabetta',lastupddttm = sysdate,ce\_comp\_access = 'N' where emplid in ('<Emp\_ID>');***

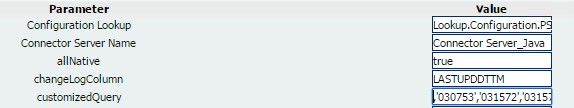
* Login to the **System Administration Console** of corresponding environment with your **AGS\_ADMIN** Id
* Select **IT Resource** from the **Configuration** section



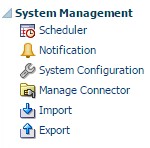
* Search for the IT Resource using **\*PSFT\***



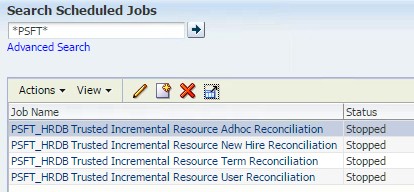
* Select PSFT\_HRDB\_ADHOC
* Click Edit
* Edit customizedQuery with the employee Id information (Note: The Emp\_ID should be enclosed using single quotes as shown below)



* Click Update to save the changes
* Select Scheduler from the System Management



* Search for the **PSFT\_HRDB Trusted Incremental Resource Adhoc Reconciliation** using **\*PSFT\***



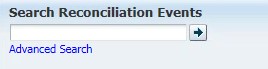
* **DO NOT** delete the **Sync Token** under the **Parameters** section and change the timing to a time, say, 30 minutes before the current CDT/EDT time



* Click Apply
* Click Run Now
* Wait till the Execution Status becomes Success under the Job History section
* Navigate to the Event Management tab



* Click on search icon →



* The reconcile event will show up like the one listed below



1. **How to find Approval Group and**
2. **Bulk Drop Users From Roles**

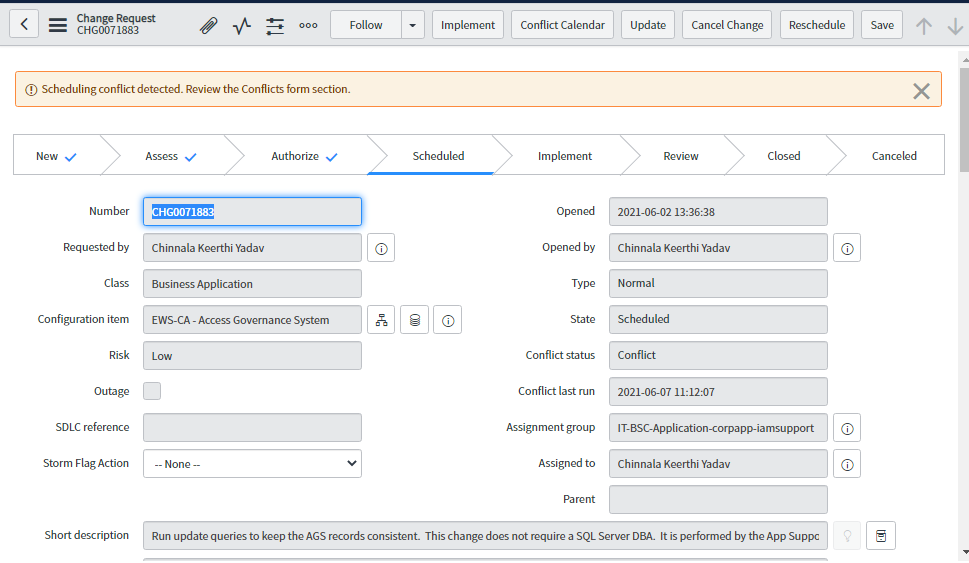
<https://teams.microsoft.com/l/file/3A153DB5-FC85-416A-BB78-24DDA7527BA1?tenantId=600d01fc-055f-49c6-868f-3ecfcc791773&fileType=docx&objectUrl=https%3A%2F%2Fexeloncorp.sharepoint.com%2Fsites%2FExelonDeloitteEWSOperate%2FShared%20Documents%2FGeneral%2FAGS%2FBulk%20Drop%20Users%20from%20Roles-User%20Guide.docx&baseUrl=https%3A%2F%2Fexeloncorp.sharepoint.com%2Fsites%2FExelonDeloitteEWSOperate&serviceName=teams&threadId=19:c932ca13d925457e9b04d8148c27d247@thread.tacv2&groupId=10cd0e60-d9d5-4c85-bfe2-ba40302c0bed>

1. **Steps to Remove access for terminated user with in 24 hours for NERC access if something is still provisioned**
2. **Certificate Management**
3. **DB Queries**

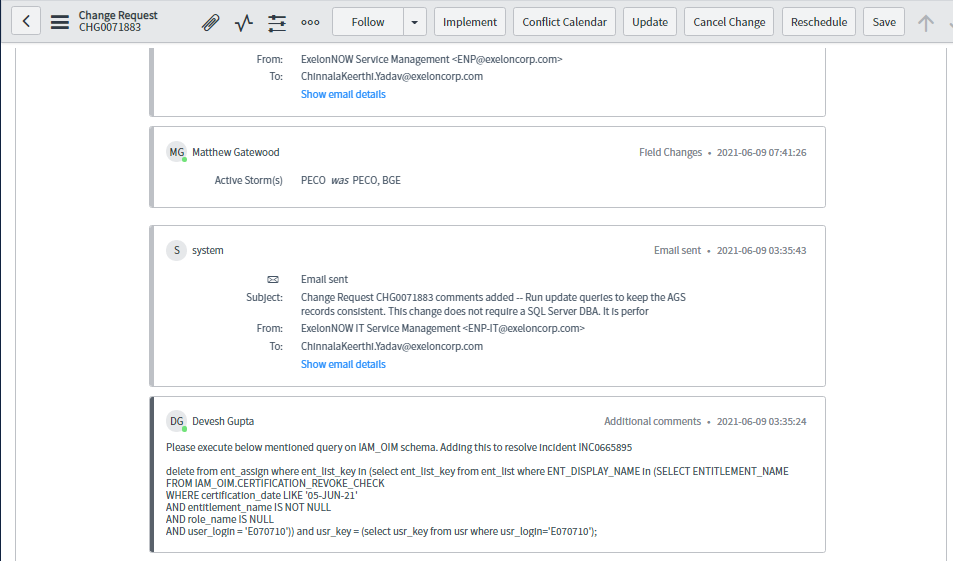
|  |  |  |
| --- | --- | --- |
|  | query on termination validations, there could be some false positives returned due to rehires. I limited the updatedtm to the 3 days of the weekend. | select usr.usr\_login, usr.usr\_status as AGS\_Status, hub.\* from DATAHUBADMINPROD.DATAHUBTRACKER hub, USR where (UPDATEDTM like '21-SEP-18%' or UPDATEDTM like '22-SEP-18%' or UPDATEDTM like '23-SEP-18%' or UPDATEDTM like '24-SEP-18%') and CHANGEDFIELD='EMPLOYEESTATUS' and NEWVALUE='T' and hub.employeeid = usr.usr\_emp\_no and usr.usr\_status = 'Active' order by updatedtm desc; |
|  | query can be used to confirm updates to the hub have also taken place in AGS. Not sure of a query specific for new hires. | select USR.USR\_FIRST\_NAME as "First Name", USR.USR\_LAST\_NAME as "Last Name", USR.USR\_EMP\_NO as "Employee Number", USR.USR\_LOGIN as "User Login", UPA\_FIELDS.FIELD\_NAME as "AGS Field Name", UPA\_FIELDS.FIELD\_OLD\_VALUE as "AGS Old Value", UPA\_FIELDS.FIELD\_NEW\_VALUE as "AGS New Value", UPA\_FIELDS.CREATE\_DATE as "AGS Change Time", DATAHUB.CHANGEDFIELD as "DataHub Field Name", DATAHUB.OLDVALUE as "Datahub old value", DATAHUB.NEWVALUE as "Datahub New Value", DATAHUB.UPDATEDTM as "DataHub Update Time" from UPA\_FIELDS, UPA\_USR, USR, DATAHUBADMINPROD.DATAHUBTRACKER DATAHUB where UPA\_USR.UPA\_USR\_KEY = UPA\_FIELDS.UPA\_USR\_KEY and UPA\_USR.USR\_KEY = USR.USR\_KEY and UPA\_FIELDS.CREATE\_DATE > '21-SEP-18' and USR.USR\_EMP\_NO=DATAHUB.EMPLOYEEID and UPA\_FIELDS.FIELD\_OLD\_VALUE = DATAHUB.OLDVALUE and UPA\_FIELDS.FIELD\_NEW\_VALUE = DATAHUB.NEWVALUE and (DATAHUB.UPDATEDTM like '21-SEP-18%' or DATAHUB.UPDATEDTM like '22-SEP18%' or DATAHUB.UPDATEDTM like '23-SEP-18%' or DATAHUB.UPDATEDTM like '24- SEP-18%') order by DATAHUB.UPDATEDTM ; |
|  | Find all the users with a specific Application Instance account in Enabled or Provisioned status | select \* from ENT\_ASSIGN, ENT\_LIST, USR where USR.USR\_KEY = ENT\_ASSIGN.USR\_KEY and ENT\_LIST.ENT\_LIST\_KEY = ENT\_ASSIGN.ENT\_LIST\_KEY and  OBJ\_KEY = (select object\_key from app\_instance where app\_instance\_key = (select entity\_key from catalog where entity\_display\_name = '<Application instance display name>'))  and ENT\_STATUS like '%<desired status>%'; |
|  | To fetch Request details | SELECT r1.requester\_key,  u1.usr\_login,  r1.request\_id,  r1.request\_model\_name,  r1.request\_status,  r1.request\_justification,  r1.request\_creation\_date,  r1.request\_model\_name,  r1.request\_isparent  FROM request r1  INNER JOIN usr u1  ON r1.requester\_key = u1.USR\_KEY  WHERE request\_id IN ('983179','983181')  ORDER BY request\_creation\_date DESC; |
|  | To Identify SOA task and composite for a request | SELECT r1.request\_id,  rben.RBE\_ENTITY\_TYPE,  rben.RBE\_ENTITY\_NAME,  w1.approvers,  w1.customattributestring1,  w1.outcome,  w1.state,  w2.assignee,  w1.componentname,  w1.TASKDEFINITIONID,  w2.numberofassignments,  w2.taskid  FROM IAM\_oim.request r1  INNER JOIN IAM\_oim.usr u1  ON r1.requester\_key = u1.USR\_KEY  INNER JOIN IAM\_oim.REQUEST\_BENEFICIARY\_ENTITIES rben  ON r1.request\_key = rben.RBE\_REQUEST\_KEY  INNER JOIN IAM\_SOAINFRA.wftask w1  ON upper(r1.request\_id)= upper(w1.IDENTIFICATIONKEY)  INNER JOIN IAM\_SOAINFRA.wfassignee w2  ON w1.taskid = w2.taskid  AND (r1.REQUEST\_ID = '2119076')  --AND (w1.TASKDEFINITIONID LIKE ‘%DisconnectedProvisioning!2.0%’)  --AND RBE\_ENTITY\_TYPE = ‘ApplicationInstance’  --AND w1.state NOT IN (‘STALE’, ‘WITHDRAWN’)  ORDER BY request\_creation\_date DESC; |
|  |  |  |
|  |  |  |

1. **How to raise CHG request to run update queries on DB**

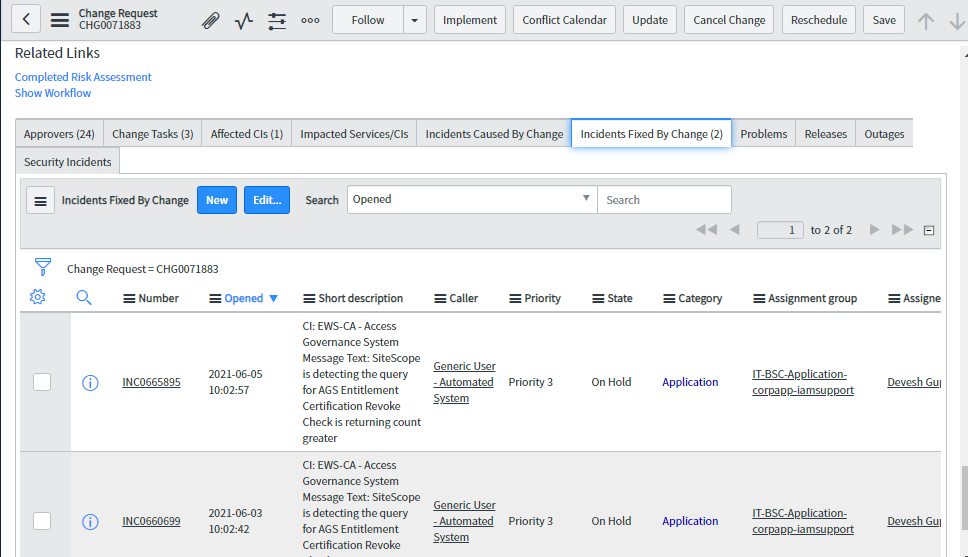
* Open change request **CHG0071883** in service now.



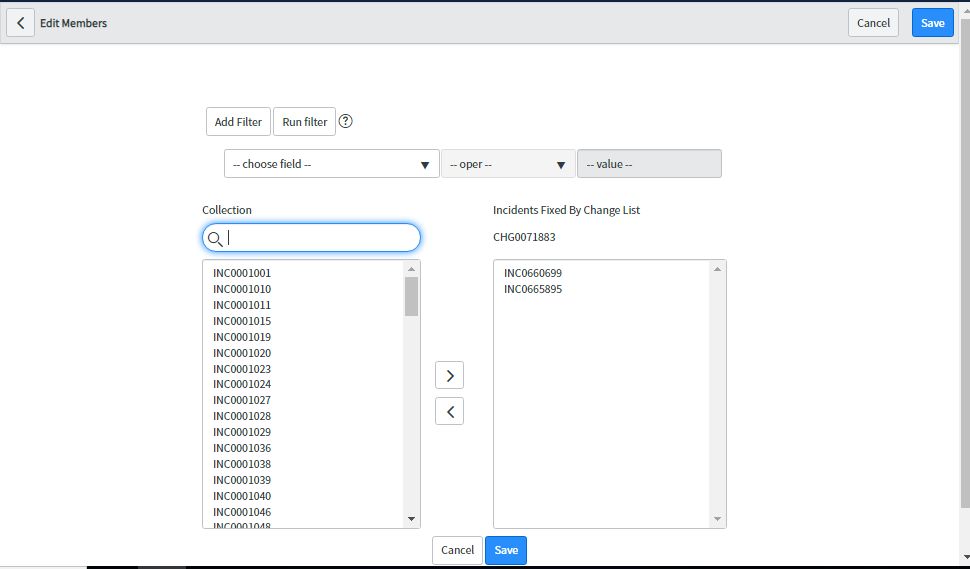
* Add SQL query to run in notes.



* At the end of CHG, click on tab **Incidents Fixed By Change.**



* Click on edit button and move incident from left to right.



* Click on **Save** button.

1. **Process to verify Db queries outputs**
2. **DB Archival and Logs archival**
3. **Cleaning up LOG files**

**PROBLEM SUMMARY:**

This document provides a step by step approach to cleanup LOG files from the UNIX host machine to free up disk space utilization

**REFERENCE:**

**Incident#** -IM001469573 SOLUTION:

**Assumptions:**

Please replace the **<ENV>** with the appropriate environment directory name (i.e. Dev, Test, Stage ). For DEV2 environment, remove the <ENV> from the below mentioned path.

* **Clean up SOA server log files**
* To clean up the SOA server logs, login to the corresponding UNIX host machine with your Exelon network credentials.
* Run the following command to login as “appserver”

**/usr/bin/sudo su – appserver**

Enter your user login password (i.e. C/E-key password)

* Navigate to the following location

cd /apps/Oracle/<ENV>/Middleware/user\_projects/domains/idm/servers/soa\_server1/logs

* Use the following command to monitor the SOA server logs files to free up disk space

find . -mtime +<N> -exec rm {} \

where <N> stands for the number of days beyond which the LOG files will be deleted) (Example 30 will delete logs older than 30 days)

* Check the latest disk utilization space using df -h
* Proceed to close the incident if the disk space utilization is less than 85%
* **Clean up OIM server log files**
* To clean up the OIM server logs, login to the corresponding UNIX host machine with your Exelon network credentials.

Run the following command to login as **“appserver”**

**/usr/bin/sudo su – appserver**

Enter your user login password (i.e. C/E-key password)

* Navigate to the following location

**cd /apps/Oracle/<ENV>/Middleware/user\_projects/domains/idm/servers/oim\_server1/logs**

* Use the following command to monitor the SOA server logs files to free up disk space

**find . -mtime +<N> -exec rm {} \**

where <N> stands for the number of days beyond which the LOG files will be deleted) (Example 30 will delete logs older than 30 days)

* Check the latest disk utilization space using **df -h**
* Proceed to close the incident if the disk space utilization is less than **85%**
* **Clean up ADMIN server log files**
* To clean up the OIM server logs, login to the corresponding UNIX host machine with your Exelon network credentials.

Run the following command to login as **“appserver”**

**/usr/bin/sudo su – appserver**

Enter your user login password (i.e. C/E-key password)

* Navigate to the following location

**cd /apps/Oracle/<ENV>/Middleware/user\_projects/domains/idm/servers/AdminServer/logs**

* Use the following command to monitor the SOA server logs files to free up disk space

**find . -mtime +<N> -exec rm {} \**

where <N> stands for the number of days beyond which the LOG files will be deleted) (Example 30 will delete logs older than 30 days)

* Check the latest disk utilization space using **df -h**
* Proceed to close the incident if the disk space utilization is less than **85%**

1. **OIM Admin Email Verification steps**
2. **Email Notifications & Verification Process**
   1. OIM ADMIN Email Verification Steps
3. **BI Publisher Reports**
4. **Generate BI Publisher Report**

**Assumptions:**

The purpose is to document the report generation process for the EPS application in AGS STG environment. The URL and credential information for other AGS environments can be found from the CyberArk.

**Stage URL:** http://iamuns-omf-01.exelonds.com:9714/xmlpserver

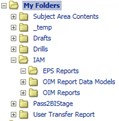
* Login to the BI Publisher Console of the corresponding environment, the credential information for which can be found from the KeePass
* Click **Catalog**



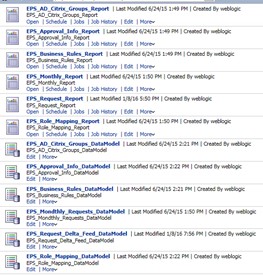
* Expand **My Folders** in the left pane under **Folders**



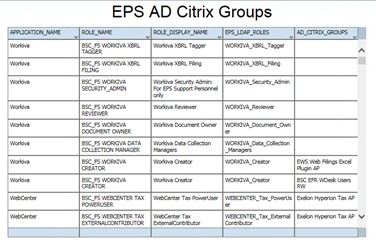
* Expand **IAM**



* Click **EPS Reports**, a window opens in the right pane with the reports



* Click on the report name to generate the report (for ex. **EPS\_AD\_Citrix\_Groups\_Report**)

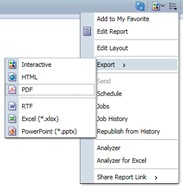


* Once the report has been generated, take an export of the same for future references, the steps for which is given below:

**Note:** For large reports, it will take a few minutes to generate the report

1.1. Export Report

* Click on the **Action** menu → **Export** → **Excel (\*.xlsx)**



* Save the **\*.xlsx** file

1. **Process to check Scheduled BI Reports status**
2. **Service Accounts Creation & Password Change Process**

Several accounts that AGS uses and we maintain.

**NOTE**: In order to see the AGS accounts in CyberArk, you need to log in using your C-key.

Your C-key needs to be a member of the following groups:

* **EWS-Security AGS CyberArk Prod**
* **EWS-Security AGS CyberArk Dev**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Account Name | Environme  nt | Type | Description | Used on | Expirati on |
| *XELSYSADM* | *Production* | *Local*  *AGS*  *Accou*  *nt* | *The master account of the application. Use little and use carefully.* | *AGS*  *Identit y*  *AGS*  *Admin Conso*  *le* | *-* |
| *weblogic* | *Production* | *Local*  *AGS*  *Accou*  *nt* | *The*  *account is used to access the weblogic console to restart servers and configure.* | *AGS*  *Weblo*  *gic*  *Conso*  *le* | *-* |
| *AGSADMIN\_########* | *Production* | *Local*  *AGS*  *Accou nts* | *These accounts are the ones with administrati ve rights into the application. They are* | *AGS*  *Identit y*  *AGS*  *Admin Conso*  *le* | *-* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | *used to*  *manage*  *and*  *configure multiple things in AGS. All follow the same naming format by replacing the ###### with the persons' C-key or E-key.* |  |  |
| *appserver* | *Production* | *Unix* | *This account is used to access the Unix servers that host the application. It has administrati ve rights.* | *Unix Server s* | *-* |
| *EPS\_REQUESTS* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* | *DB* |  |  |  |
| *OIMCCURE* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* |  |  |  |  |
| *OIMDBUSER* | *Production,*  *Disaster*  *Recovery,*  *Stage,* | *DB* | *This account has*  *Read*  *Rights into the OIM DB.* |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | *Developme nt,*  *Test* |  |  |  |  |
| *CCURE\_IAM* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme nt,*  *Test* | *Windo ws* |  |  |  |
| *IAM\_BIPLATFORM* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* |  |  |  |  |
| *IAM\_MDS* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* |  |  |  |  |
| *IAM\_IOM* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* |  | *This is the DB account with Read*  *and Write*  *rights into the OIM*  *Database.* |  |  |
| *IAM\_OPSS* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme*  *nt,*  *Test* |  |  |  |  |
| *IAM\_ORASDPM* | *Production,*  *Disaster*  *Recovery,*  *Stage,* |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | *Developme nt,*  *Test* |  |  |  |  |
| *IAM\_SOAINFRA* | *Production,*  *Disaster*  *Recovery,*  *Stage,*  *Developme nt,*  *Test* |  | *This is the DB account with Read and Write rights into the SOA*  *Database.* |  |  |
| *svc\_IAMExelonDS\_D* | *Stage,*  *Developme*  *nt,*  *Test* | *Windo ws* | *This is the service account that runs the Connector*  *Service for ExelonDS.* |  |  |
| *svc\_IAMExelonDS\_P* | *Production* | *Windo ws* | *This is the service account that runs the Connector*  *Service for ExelonDS.* |  |  |
| *svc\_IAMWindowsAdmin* | *Stage,*  *Developme nt,*  *Test* | *Windo ws* |  |  |  |
| *svc\_IAMWindowsAdminP* | *Production* | *Windo ws* | *This is the service account to connect to the Connector*  *Server for*  *ExelonDS.* |  |  |
| *svc\_EWSDataHub\_ATOM* | *Production,*    *Stage,*  *Developme*  *nt* | *Local ePeop*  *le*  *Accou*  *nt* | *Used by the EWSDataH*  *ub to integrate with ePeople with the*  *Atom Feed that runs every 6 hours.* | *Config*  *file in*  *Unix server s.* |  |
| ***svc\_EWSDataHubHR\_PII*** | *Production* | *Windo ws* | *Used by the EWSDataH*  *ub to integrate* | *Config*  *file in*  *Unix* |  |
|  |  |  | *with ePeople for Production.* | *server s.* |  |
| ***svc\_EWSHRDev\_PII*** | *Stage,*  *Developme*  *nt* | *Windo ws* | *Used by the EWSDataH*  *ub to integrate with ePeople for Stage and Dev.* | *Config*  *file in*  *Unix server s.* |  |
| ***DataHubAdmin*** *&* ***DataHu bAdminUpd*** | *Developme*  *nt* | *Oracle* | *Used by the*  *EWSDataH ub*  *integration for*  *Developme nt. Not Stage or Test.* | *Config file in*  *Unix server s.* |  |
| ***DATAHUBADMINPRODUP D*** | *Production* | *Oracle* | *Used by the*  *EWSDataH ub*  *integration for*  *Production.* | *Config*  *file in*  *Unix server s.* |  |
|  |  |  |  |  |  |

1. **Info Only: AGS Unix Accounts Exceptions**

Accounts filed for exceptions due to non-existend change process. Exception Number in Exelon: 6466

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



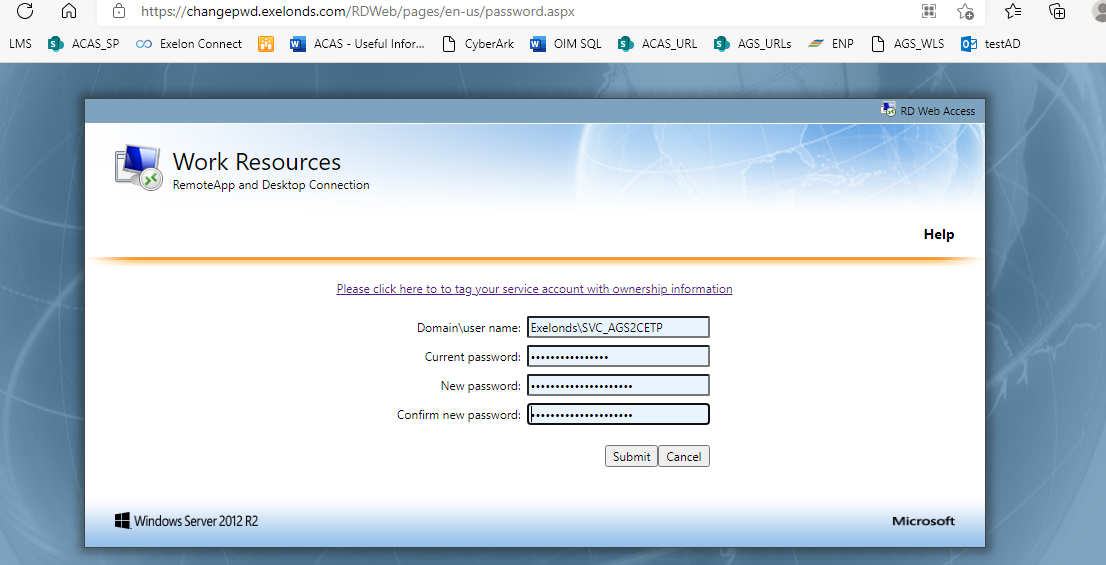
1. **SVC\_AGS2CETD and SVC\_AGS2CETP Service Account Password Change**

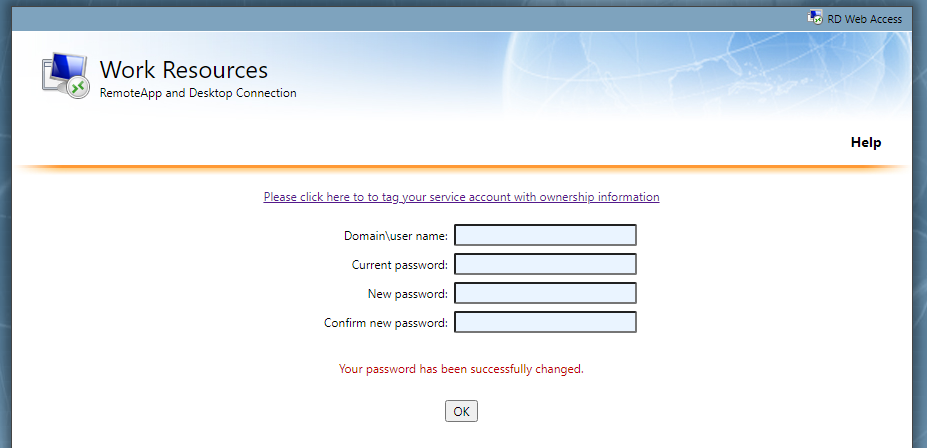
Password change for **SVC\_AGS2CETD (Non-Prod) & SVC\_AGS2CETP (Prod).**

**Guide**

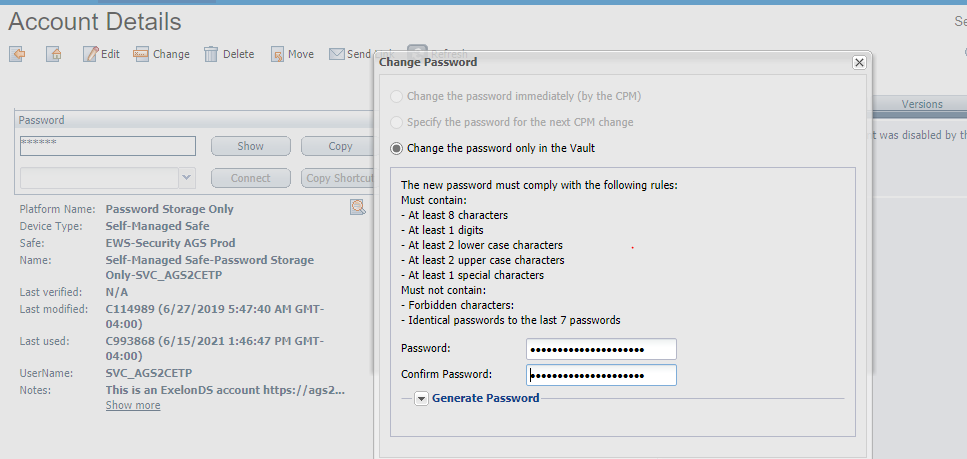
For **SVC\_AGS2CETD (Non-Prod)/ SVC\_AGS2CETP** (Prod) below are the instructions.

* First get the existing password from **KeePass/CyberArk.**
* Click into the **URL** [RD Web Access (exelonds.com)](https://changepwd.exelonds.com/RDWeb/pages/en-us/password.aspx) to reset the Password.
* Search “**SVC\_AGS2CETD/ SVC\_AGS2CETP**” and click on **Change Password.**
* Enter the Current Password and New Password twice.



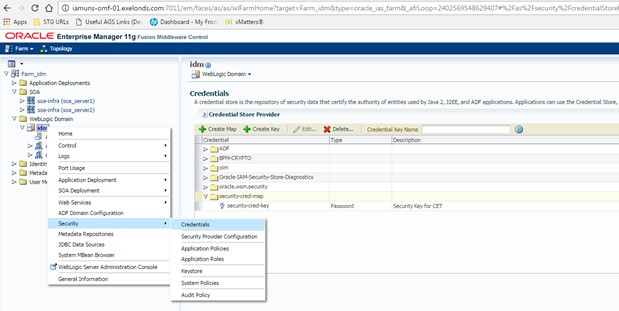


**NOTE: Update the changed password in CyberARk**

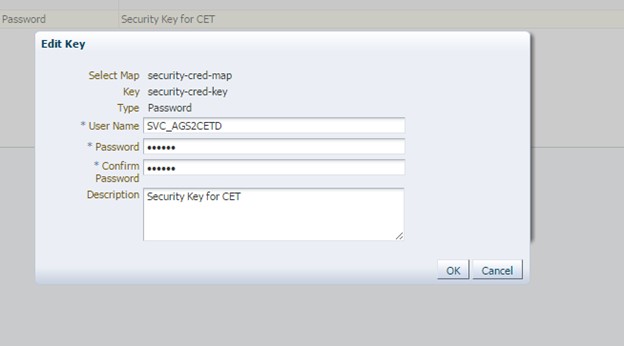


* Login to EM Console in all the Non Prod Servers and Go To **WebLogic**

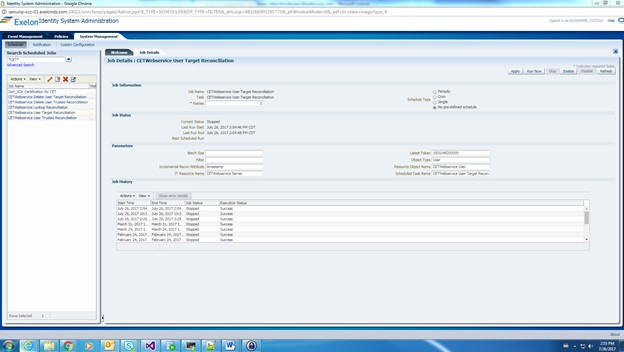
**Domain>IDM>Right Click** on **IDM** and Go To **Security>Credential>Security-Cred-Map.**



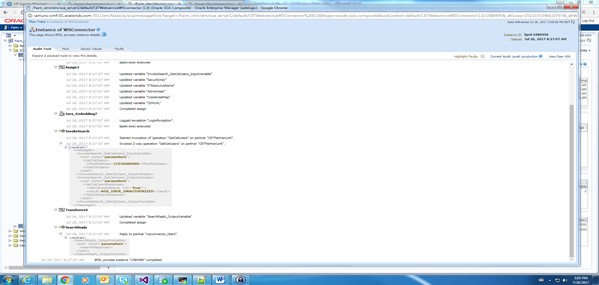
* Click on **Security-Cred-Map** and **Click** on **Edit** on the top and change the Password.



* Once the Password is changed in EM Console, Run Recon **“CETWebservice User Target Reconciliation”** to verify process running fine or not.



* If the Recon is successful then it is working fine.
* Also verify the Latest Instance ID and Payload in EM Console (Under SOA INFRA) just to check whether new password change successful or not.



1. **CUSTOMDBUSER and CUSTOMDBUSERUPD Password Change**

:

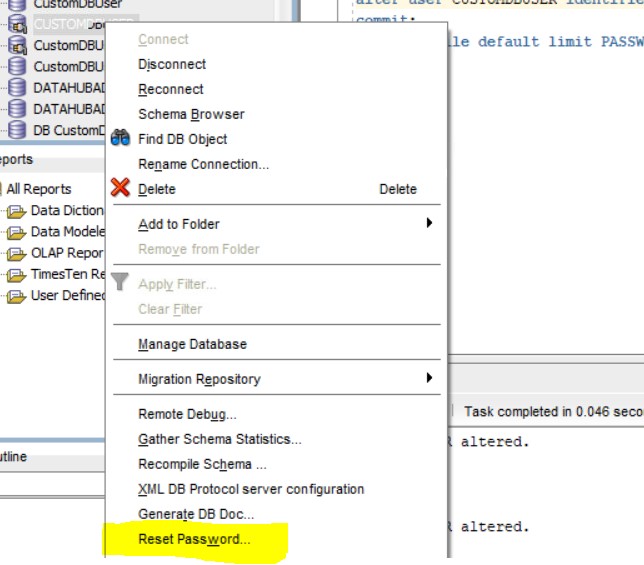
|  |  |  |  |
| --- | --- | --- | --- |
| ***BSCIAMD1.EXELONDS.COM*** | ***CUSTOMDBUSER*** | ***No***  ***npr od*** | ***EWS-CA - Access Governance System*** |
| ***OMFIAMT1.EXELONDS.COM*** | ***CUSTOMDBUSER*** | ***No npr od*** | ***EWS-CA - Access Governance System*** |
| ***BSCIAMD1.EXELONDS.COM*** | ***CUSTOMDBUSERUP D*** | ***No***  ***npr od*** | ***EWS-CA - Access Governance System*** |
| ***OMFIAMT1.EXELONDS.COM*** | ***CUSTOMDBUSERUP D*** | ***No***  ***npr od*** | ***EWS-CA - Access Governance System*** |
| ***OMFIAMS1.EXELONDS.COM*** | ***CUSTOMDBUSERUP D*** | ***No***  ***npr od*** | ***EWS-CA - Access Governance System*** |

Two ways to change a DB password (Please Note: This is applicable only when we have the exsisting password)

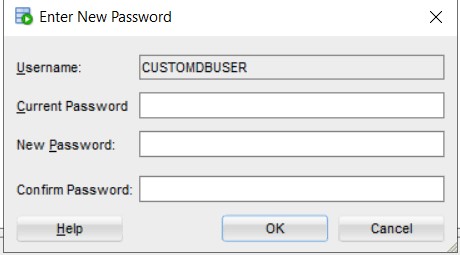
* Login to SQL and connect to the respective DB account(Password and connection details are available in CyberArk) o Run the query : ***alter user <user> identified by "<newpassword>" replace***

***"<currentpassword>";*** o After successful password change, you will be notified with:

* + Verify the connection in SQL, connection status should reflect "Success" with the new password.
* Also, password can be changed through "Reset Password" option.
  + Right click on the account and click Reset Password.



Change the password:

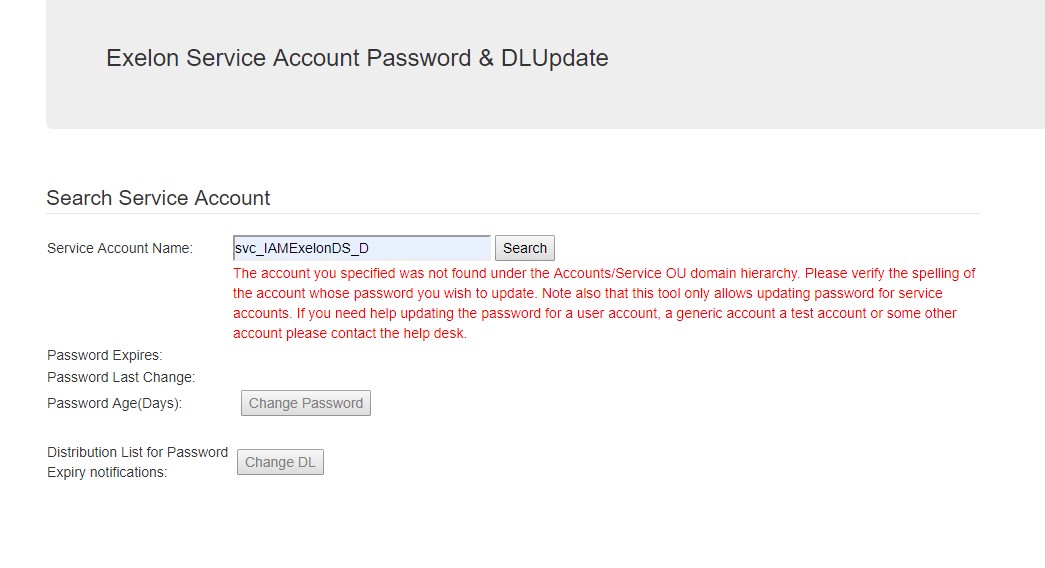


Validate the connection.

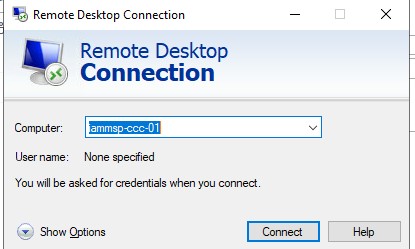
**Please Note : For the same username in production, we might need to contact DB team and create EDM for them to change the password, though we can perform the task from our end. Because there might be multiple dependencies, hence it is recommended to contact DB team for production password change.**

1. **svc\_IAMExelonDS\_P password change**

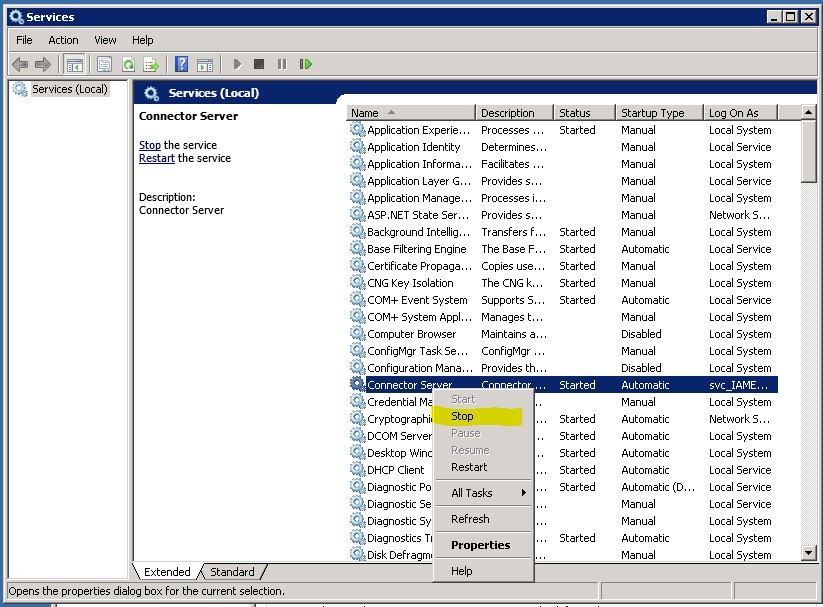
* Change the password from the link beside: https://adsearch.exeloncorp.com/adsearch/ServiceAccountUpdate



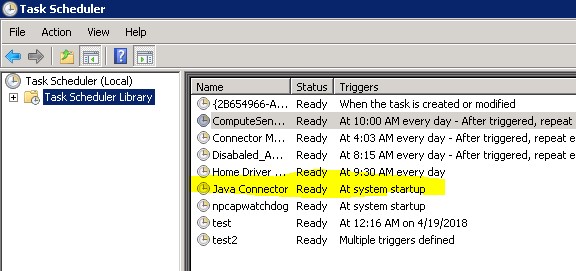
* Perform the following steps on **BOTH** connector servers one at a time.
* Update the password in the connector server, login to **iammsp-ccc-01** and **iammsp-ccc-02** via remote desktop. with the service account "**svc\_IAMExelonDS\_P"** and new password that was changed above.



* Navigate to start and search for services. In services select "**Connector Service**", right click and stop.

● 

* Navigate to start and search for task scheduler. Select task scheduler library in the left most panel. Find "**Java Connector Service**" in the middle panel and start this task and refresh.

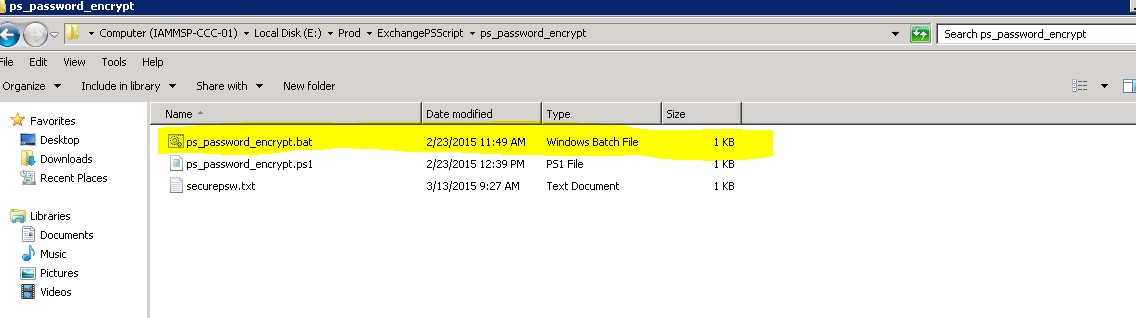
● 

* ***Differences Between Servers***
* ***iammsp-ccc-01*** *and* ***iammsp-ccc-02*** *differ slightly. Server 1 requires you run the .bat or .ps1 script with admin permissions, this will fail if run with admin on server 2.*
* *The securepsw.txt file must be deleted on server 2 in* ***E:\Prod\ExchangePSScript\ps\_password\_encrypt*** *before running the script, not the case on server 1.*

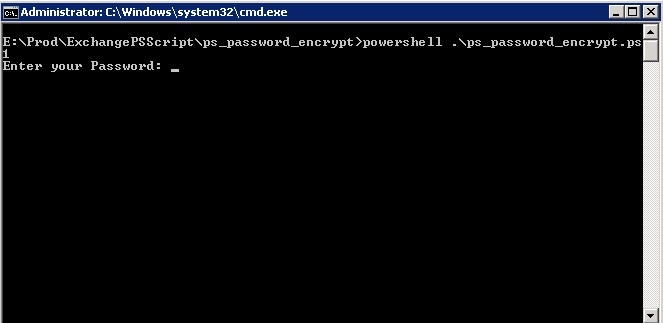
|  |  |
| --- | --- |
| *●* | *The .ps1 script may need to be run if the .bat change is unsuccessful.* |

* Navigate to ***E:\Prod\ExchangePSScript\ps\_password\_encrypt*** folder and run

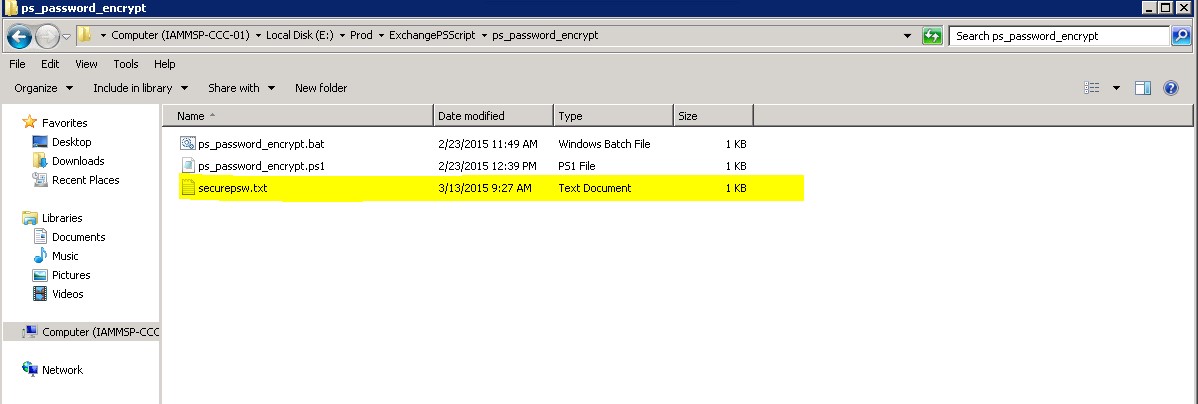
"**ps\_password\_encrypt.bat**" batch file to change the password in the exchange ps scripts.



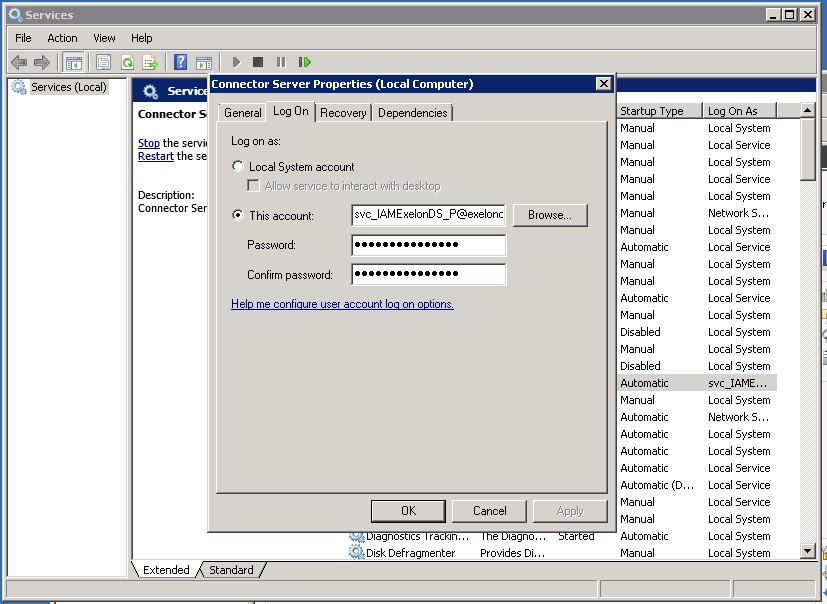
* Type the current password and press enter.



* In the location ***E:\Prod\ExchangePSScript\ps\_password\_encrypt****, there will be a "****securepsw.txt****"* file (encrypted *password), after changing the password* validate whether the file is reflecting current date.



* Copy the file *"****securepsw.txt****"* in ***E:\Prod\ExchangePSScript*** and overwrite the old one. Make a backup of the old before overwriting.
* Navigate to start and search for services. In services select "**Connector Service**", right click and properties. In properties navigate to the Login tab and update the password in this field. Then exit properties and right click to start the connector service.

● 

* Navigate to start and search for task scheduler. Select task scheduler library in the left most panel. Find "**Java Connector Service"** in the middle panel and start this task and refresh.
* Update the password in the IT Resource of AD and Exchange ● Login into the AGS Sys Admin Console.
* IT Resource name : **Active Directory** and **Exchange IT Resource**, ● Update password in the respective IT Resource.
* The Recon step that follows only needs to be run on one Admin console.
* Validate successful change by running the "**Active Directory Target User Recon - Adhoc**" under the scheduler by replacing your C-key in the filter, applying the setting, running the recon and refreshing until it shows successful.
* Update the password in the IT Resource of SecDB ● Login into the AGS Sys Admin Console.
* IT Resource name : **SecDB**
* Update the new password in the IT Resource
* Validate successful change by running the "**SecDB Target Resource User Reconciliation**" under the scheduler by applying the setting, running the recon and refreshing the job until it shows successful.

***Validating .bat Script***

*The only way to validate the .bat script is successful*

*is to observe the*

*logs at*

***E:\Prod\ExchangePSScript\logs.***

*Look for any*

*log with*

*'\*e-key\*\_aftercreatemailbox\_\*date\_time\_after\_change\*.txt'*

*and review for*

*any errors. If no errors occur the change is successful.*

*A new user with a email account in provisioning state*

*and no email in AD*

*can be provisioned by retrying the create user task*

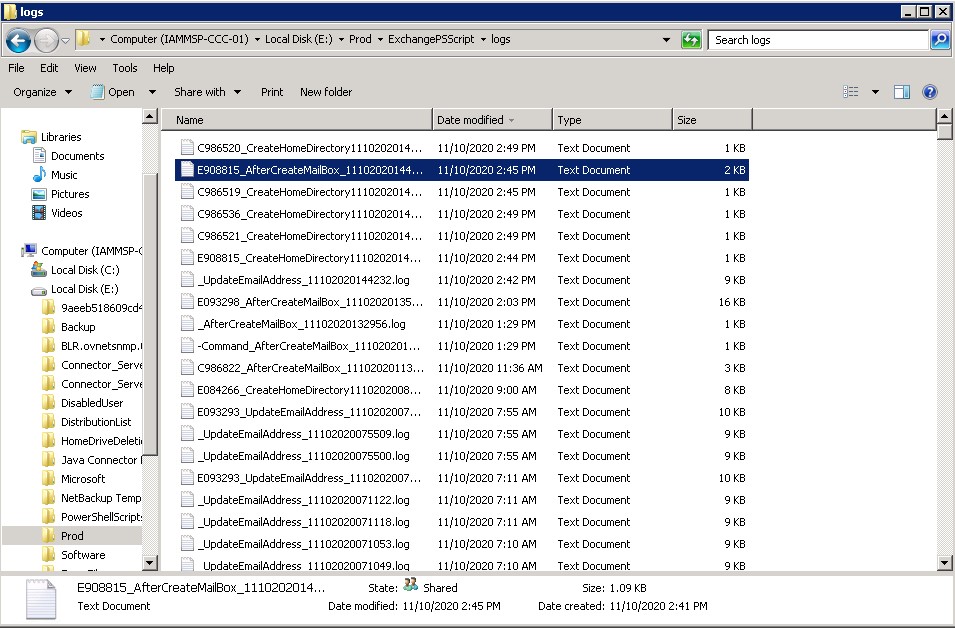
*in their AGS resource*

*history. This will trigger the mailbox create task*

*and a log will be created*

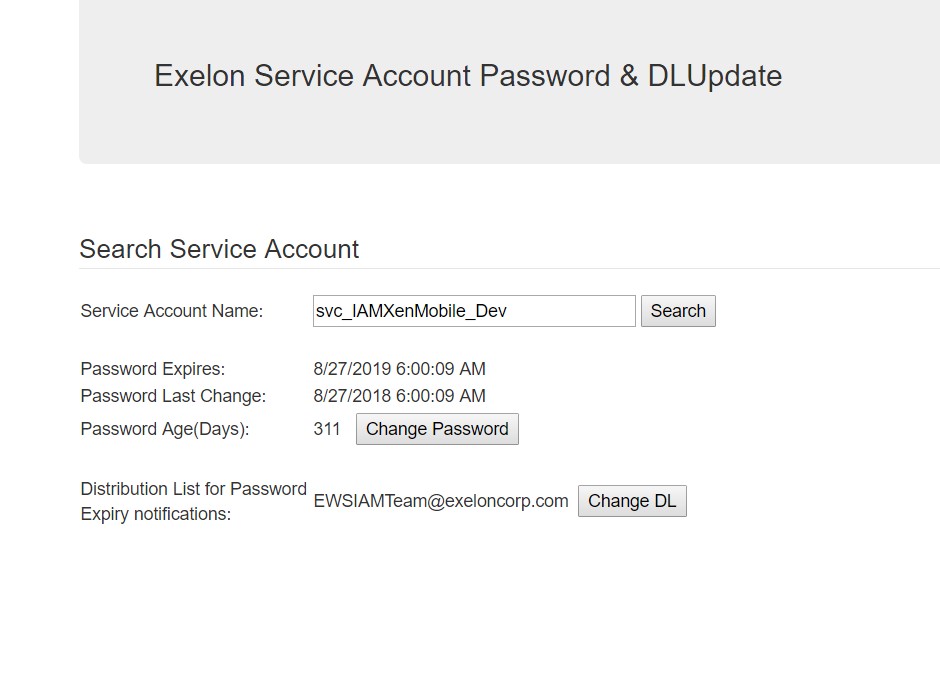
*to verify the change was successful via the above*

*logs.*

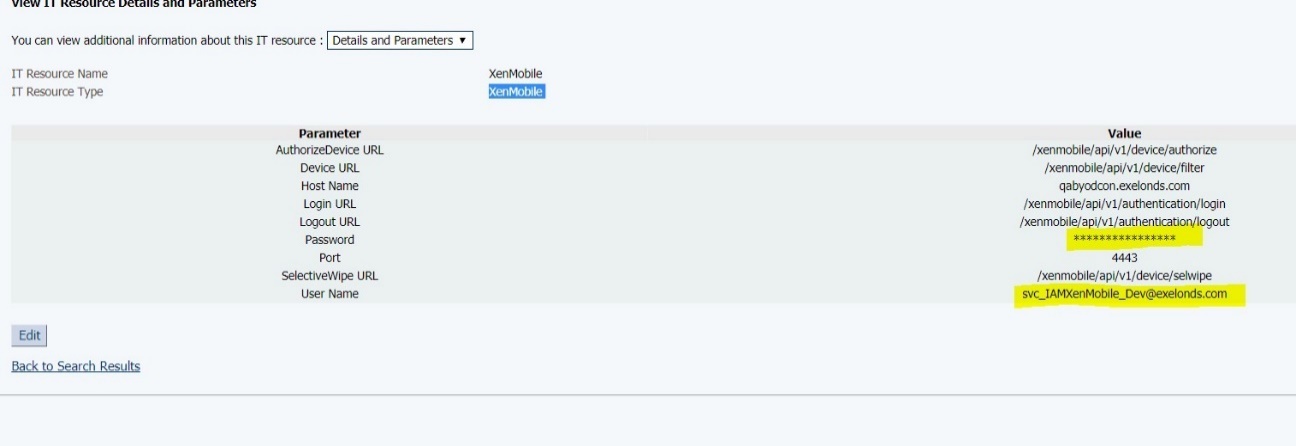


1. **svc\_IAMXenMobile\_Dev and svc\_IAMXenMobile\_PRD Password Change**

* Collect the correct password from CyberArk
* Open the link https://adsearch.exeloncorp.com/adsearch/ServiceAccountUpdate to reset the password



* After changing the password, update the password in the respective IT Resource
* IT Resource name : **XenMobile**
* Update the password in CyberArk.



**Note : For production "svc\_IAMXenMobile\_PRD" as well approach would be the same.**

And, if there is an issue with the current password, contact AD team to reset the password

1. **Creating AGS ADMIN Account**

The Process Of the Catalogue Item

→



→ **Manager Approval**→**AGS Admin Access Authorizer**→**AGS Management Approver**→**AGS Admin Access Fulfiller (EWS Support Group) Note:**

|  |
| --- |
| *While requesting for* ***AGS Admin Account*** *in* ***PROD*** *and* ***STAGE*** *Environment. The requester needs to request it from his/her C-key account to receive their* ***AGSADMIN\_XXXXXXX*** *credentials.*  *The Catalogue item using which the account will be requested is* ***AGS Admin Access*** *as shown in the picture.* |

**Solution:**

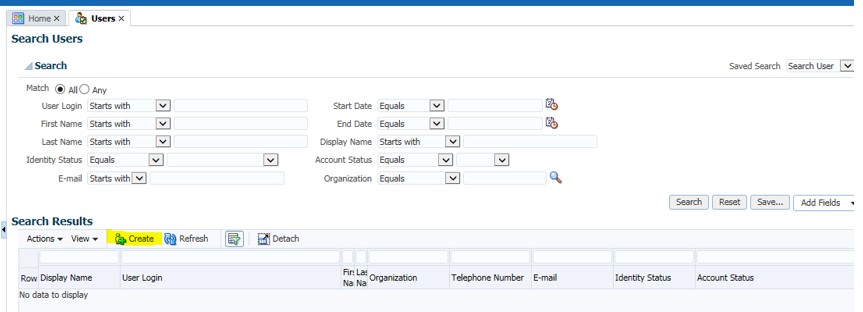
Create a new AGS\_ADMIN Account by following the instructions below.

*The fulfiller must have an AGS\_ADMIN account in order to create a new one for the beneficiary.*

*If you don't have an AGSADMIN account, login with* ***xelsysadm*** *account whose password can be found in CyberArk. Make sure, you have access of CyberArk at first.*

*Please follow the hyperlink to get the password for any specific environment from CyberArk (*[*Update a Password in CyberArk*](https://ada.sath.com/display/SOKB/Update+a+Password+in+CyberArk)*).*

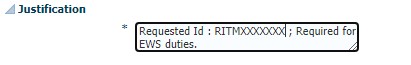
* Login to AGS with your AGSADMIN account
* Go to **Users**. Click Create

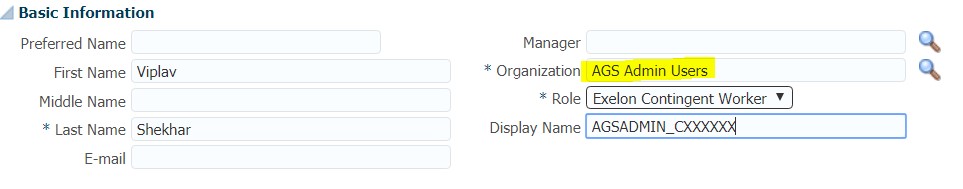


* Only enter info mentioned below.

|  |  |
| --- | --- |
| ***Justification*** | *Enter the RITMXXXXXXX (Need to create a Service Request in*  *EXELONNOW)* |
|  | *Beneficiary's first name* |
| ***Last Name*** | *Beneficiary's last name* |
| ***Organization*** | *AGS Admin Users* |
| ***Role*** | *Exelon Contingent Worker* |
| ***User Login*** | *AGSADMIN\_XXXX, where XXXX is the primary account of the beneficiary* |
| ***Password*** | ***ExelonAdm1nPswd!*** *(Keep this as default password , as discussed with client)* |
| ***Display Name*** | *Same as* ***User Login*** |
| ***Auto Provision Indicator*** | *X* |

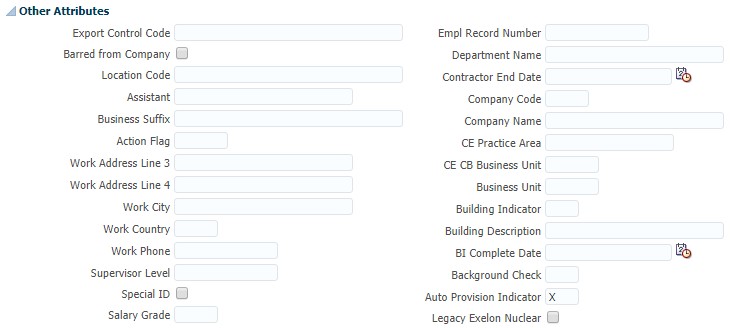
* When complete, Press **Submit.**





**Note: Not necessary to write e-mail address. You will get an error if you do, as the e-mail address was used to create the C-key. Leave e-mail blank.**

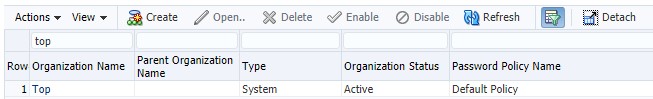




* Go to **Administration > Organizations**



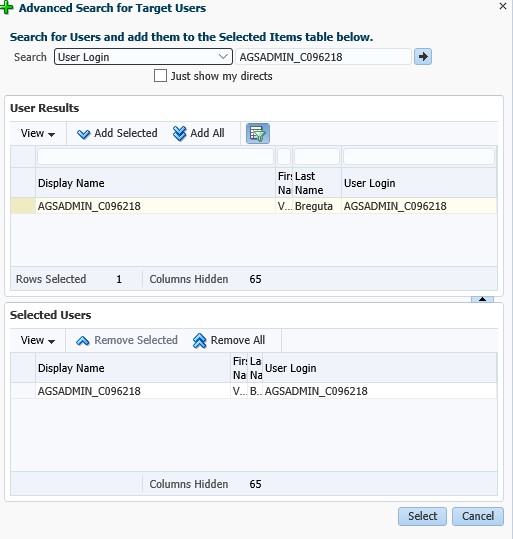
* Enter **Top** into the search field above **Organization Name.** Press **Enter**
* Select **Top**



* Go to the **Admin Roles** Tab
* Select System **Administrator.** Press **Assign**



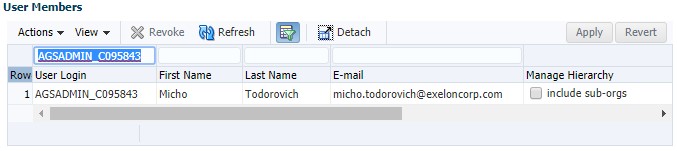
* Search for the user that was created.
* Select the user to and press **Add Selected**



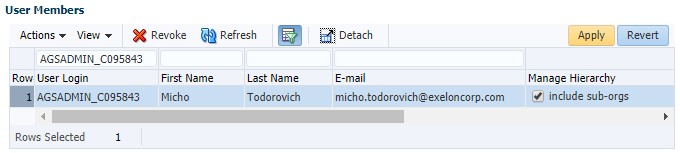
* Press **Select**
* Ensure **Query By Example** () is selected



* Enter the **User Login** you just created in the search field above **User Login**



* Set the **Include Sub Org** flag to true (checked) for the user you created.
* Click **Apply.**



* Refresh the data and ensure the flag was actually set.

1. **AGS DEV2 LB URI Certificate Renewal steps**
2. AGS application using the Internal CA certificate authority, and in order to get the new certificate, we need to place a service request using the SNOW. Before, placing the SR for the newer certificate, we need to generate a CSR (Certificate Signing request) using the existing certificate.
   1. Login to the IAMUND-CCC-01 serer using the “appserver” account.
   2. Navigate to the **/apps/Oracle/Middleware/wlserver\_10.3/server/lib** dire ctory and ran the following command to find the existing certificate, which resides in the **DemoTrust.jks** KeyStore.

**keytool -list -v -keystore DemoTrust.jks**

(You will be promoted for the password, which can be fetch from the CyberArk).

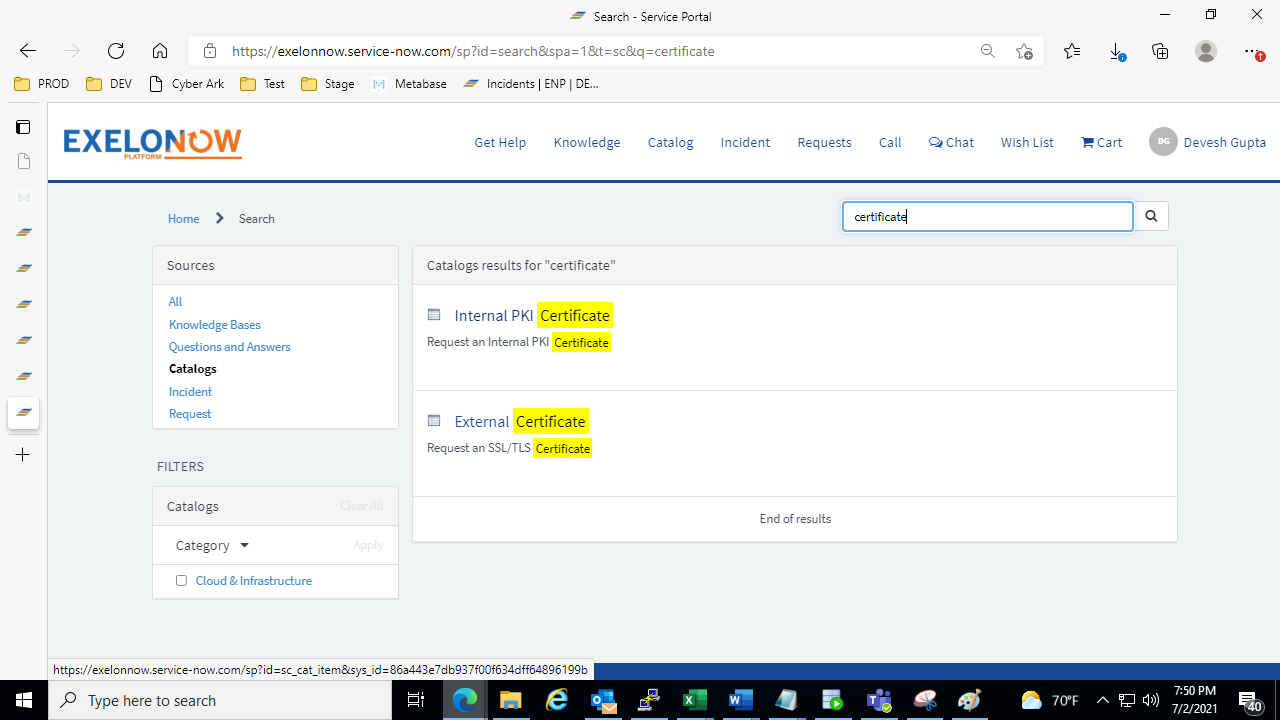
* 1. Validate the **alias** name and certificate details.
  2. Generate a CSR using the following command. (Optional)

**keytool -certreq -alias <alias name> -file dev2ags.pem -keystore /apps/Oracle/Middleware/wlserver\_10.3/server/lib/DemoTrust.jks**

Enter the keystore password form the CyberArk.

Copy the file into your home directory and download into your VPC, to be uploaded in the SNOW request for the renewal.

1. Raise a SNOW request for the Internal Certificate in (**.~~cer/.pem/.p7b~~**) **(.pfx)** format using the csr (we will connect, and I will guide on this)



Add details as mentioned in RITM0097151

1. Contact the LB team to make the changes in the their LB tools (Reach out to Todd & Alla to get the LB team Information) – Raise a Service request to LB team to change certificate.
2. Upon receiving the certificate, download and place it into your home directory and execute below command to install the certificate.
   1. Shutdown the AGS DEV2 environment (SOA>OIM>Admin) server
   2. Copy the certificate file from your /home/<ckey>/<certificate file name> directory to /apps/Oracle/Middleware/wlserver\_10.3/server/lib/DemoTrust.jks
   3. Navigate to the /apps/Oracle/Middleware/wlserver\_10.3/server/lib/ and take a backup of the existing **DemoTrust.jks** KeyStore.
   4. Remove the old certificate using the below command
      1. **keytool -delete -alias <alias name> -keystore DemoTrust.jks -storepass** <password from the CyberArk>
   5. Nowinstall the new certificate using the below command

**keytool -importkeystore -srckeystore <CertificateFileName>.pfx -srcstoretype pkcs12 -srcalias <Alias name mentioned in certificate File> -destkeystore DemoTrust\_071221.jks -deststoretype jks -destalias dev2ags -srcstorepass <certificate Password> -deststorepass <Password of DemoTrust>**

**\*\* Run this command to fetch alias in Certificate file**

**keytool -list -v -keystore <CertificateFileName>.pfx -storetype pkcs12 -storepass <Certificate Password>**

* 1. Validate the new certificate installed successfully by executing the below command.

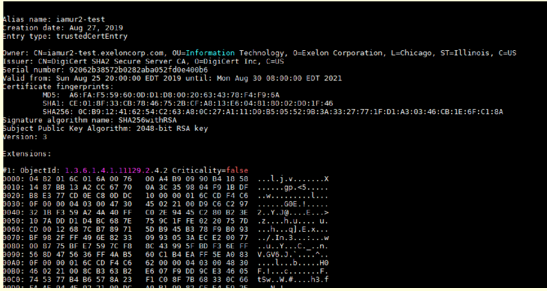
**keytool -list -v -alias dev2ags -keystore DemoTrust.jks -storepass <password from the CyberArk>**

1. Start the AGS application in this order (Admin > SOA > OIM)
2. Validate the dev2ags.exeloncorp.com/identity URI is accessible and contains the new certificate.
3. **AGS TEST Digicert Certificate Renewal steps**
4. *Generate the CSR, following the below mentioned command.*
   1. Navigate to **/apps/Oracle/Test/Middleware/wlserver\_10.3/server/lib/**
   2. Check in **DemoTrust.jks** and **DemoIdentity.jks** for the specific certificate which is required to be renewed exists **(normally for AGS all the trusted certificate resides in DemoTrust.jks)**

**keytool -list -v -keystore DemoTrust.jks**

**keytool -list -v -keystore DemoIdentity.jks**

*\*\***You will be then prompted with a password, just ignore and press Enter*



* 1. *Verify the expire date.*
  2. Generate CSR (New certificate will be replica of the existing one hence the details mentioned in the existing certificate should match while creating a new **CSR**)
  3. Type the following command to get the new CSR:

***openssl req -new -newkey rsa:2048 -nodes -keyout <CSR name>.key -out <CSR name>.csr***

*Now enter the following information like "Country Code", "OU", "CN", replicate the same as mentioned in the existing certificate.*

*After providing all the required information, new file <CSR name>.cer and <CSR name>.key will be generated in the* ***/lib/*** *folder.*

1. Raise SR to get Internal PKI Certificate.
2. After getting certificate, raise SR for LB team to apply certificate at their end.
3. Upon receiving the certificate, download and place it into your home directory and execute below command to install the certificate.
   1. Shutdown the AGS TEST environment (SOA>OIM>Admin) server
   2. Copy the certificate file from your /home/<ckey>/<certificate file name> directory to /apps/Oracle/Test/Middleware/wlserver\_10.3/server/lib/DemoTrust.jks
   3. Navigate to the /apps/Oracle/Middleware/wlserver\_10.3/server/lib/ and take a backup of the existing **DemoTrust.jks** KeyStore.
   4. Remove the old certificate using the below command

**keytool -delete -alias <alias name> -keystore DemoTrust.jks -storepass** <password from the CyberArk>

* 1. Nowinstall the new certificate using the below command

**keytool -importkeystore -srckeystore <CertificateFileName>.pfx -srcstoretype pkcs12 -srcalias <Alias name mentioned in certificate File> -destkeystore DemoTrust\_071221.jks -deststoretype jks -destalias dev2ags -srcstorepass <certificate Password> -deststorepass <Password of DemoTrust>**

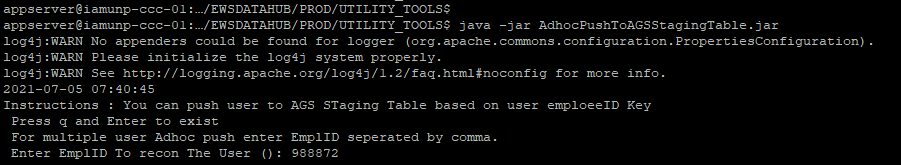
**\*\* Run this command to fetch alias in Certificate file**

**keytool -list -v -keystore <CertificateFileName>.pfx -storetype pkcs12 -storepass <Certificate Password>**

* 1. Validate the new certificate installed successfully by executing the below command.

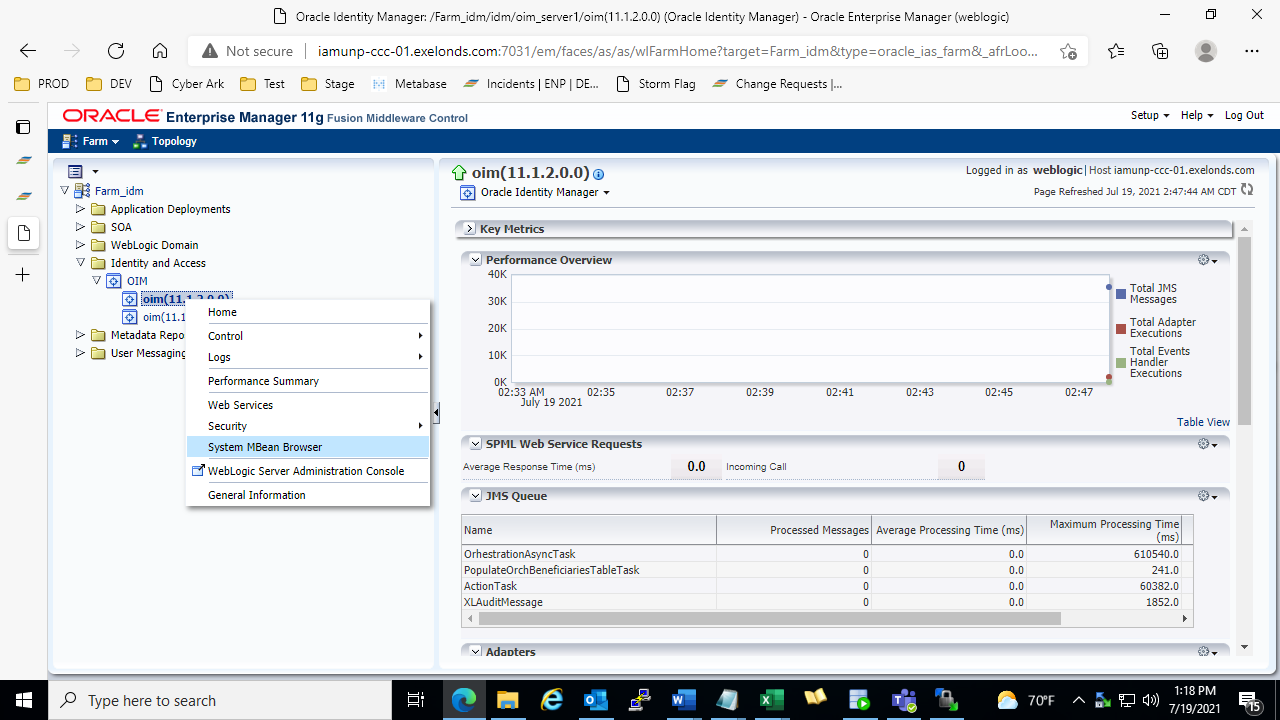
**keytool -list -v -alias dev2ags -keystore DemoTrust.jks -storepass <password from the CyberArk>**

1. Start the AGS application in this order (Admin > SOA > OIM)
2. Validate the <https://iamur2-test.exeloncorp.com/> and https://iamur2-test.exeloncorp.com/identity URI is accessible and contains the new certificate.
3. **Governance/management of service accounts**
4. **Performance improvement**
5. **Onboarding Steps for new team member**
6. **AGS Adhoc Jobs**
7. AdhocPushToAGSStagingTable.jar

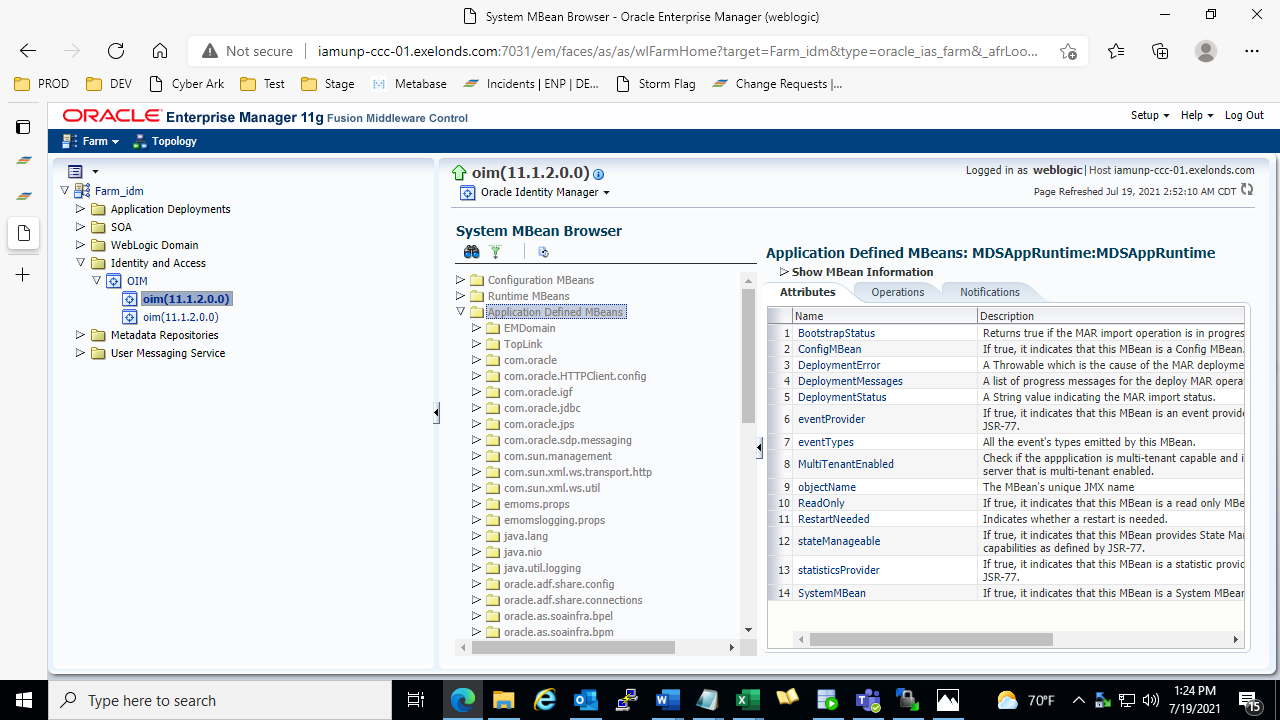




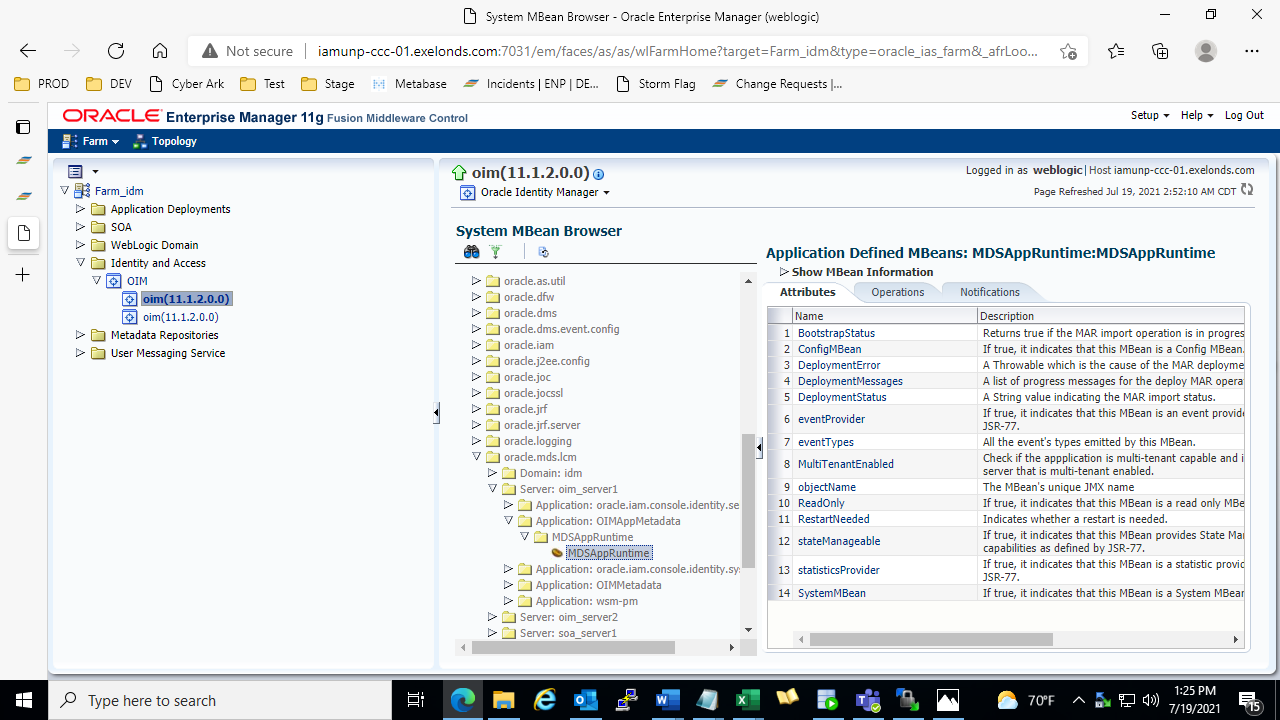
1. **Scheduled Jobs and their tasks**
2. **How to raise Oracle SR and Generate list of patches**
3. **How to take MDS Export**
4. Login on EM Console. Expand **Identity and Access à OIM à oim(11.2.0.0)**. Right click and click on System Mbean Browser



1. Expand **Application Defined Beans.**



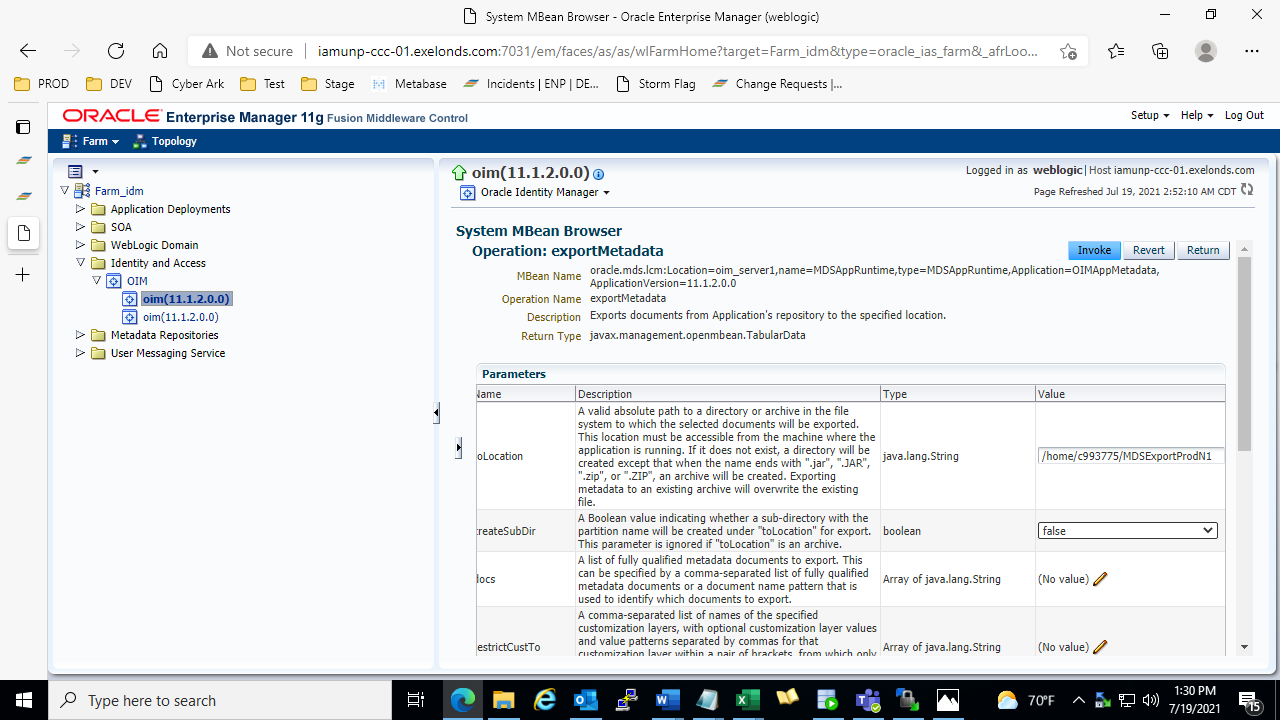
1. Expand **oracle.mds.lcm à Server à OIMAppMetaDAta à MDSAppRuntime**



1. Click on **Operations Tab.** Click on **exportMetadata.**



1. Enter directory location in **toLocation** field. Click on **Invoke.**



1. **REVOKE AGS ADMIN ACCESS**

Step 1 : login to the identity Console of Prod Environment(http://iamunp-ccc-01.exelonds.com:14021/identity).

Step 2: Now Click on Organization present in the identity console as shown below in the screenshot.

Step 3: After clicking on it you will get the screen present below in the screenshots.

Step 4: type **TOP** in Organisation Name and search for it as shown below in the screenshot.

Step 5: Now select TOP from below and goto Admin Roles ,you will find System Administration as shown in the screenshot below.

Step 6: Search for the AGSADMIN\_CXXXXXX , that you want to revoke.

Step 7: Now hit the revoke button. That got activated after selecting the AGSADMIN\_CXXXXXX.

Step 8 : Now After revoking it the user account can be used anymore.