EmblemHealth

**SailPoint Identity Management Project**

**Deployment Plan**



Version 1.0

Effective Date:

Prepared By: Cognizant Technology Solutions

*All information contained herein is proprietary and shall be kept confidential.*

Approvals

Approval denotes acceptance of the business requirements contained herein and serves as authorization to move forward with related documents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Role** | **Date** |
| Arjun Sengupta | Cognizant | Reviewer |  |
| Saleem AT | Cognizant | Reviewer |  |
| Sudhir Kumar Panda | Cognizant | Reviewer |  |
| Bhaskar Bhattacharya | Cognizant | Approver |  |
| Randall Dulin | Cognizant | Approver |  |
| Jim Altinay | Emblem Health | Approver |  |
| Tom McDermot | Emblem Health | Approver |  |

Revision History

| **Version** | **Version Date** | **Author** | **Reviewed by** | **Comments** |
| --- | --- | --- | --- | --- |
| 1.0 | 02/28/2018 | Debasmita/Archana/Sreejit |  | Initial draft |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Deployment Plan 1](#_Toc511926282)

[Revision History 3](#_Toc511926283)

[Table of Contents 4](#_Toc511926284)

[1.0 Project Purpose 5](#_Toc511926285)

[2.0 Document Purpose 5](#_Toc511926286)

[3.0 Scope 5](#_Toc511926287)

[3.1 In-Scope 5](#_Toc511926288)

[3.2 Out of Scope 6](#_Toc511926289)

[4.0 Roles & Responsibility 6](#_Toc511926290)

[5.0 Definition & Acronyms 6](#_Toc511926291)

[6.0 Release Process 7](#_Toc511926292)

[6.1 Backup 7](#_Toc511926293)

[6.2 Rollback 8](#_Toc511926294)

[6.3 Deployment Steps 8](#_Toc511926295)

[6.3.1 UI Branding 8](#_Toc511926296)

[6.3.2 File List 8](#_Toc511926297)

[6.3.3 Steps to Import using script 10](#_Toc511926298)

[6.3.4 Configuration 11](#_Toc511926299)

[6.3.4.1. Migration of Existing Active Directory groups 11](#_Toc511926300)

[6.3.4.2. Lifecycle Manager Configuration 13](#_Toc511926301)

[6.3.4.3. QuickLink Category 14](#_Toc511926302)

[6.3.4.4. Group Create 14](#_Toc511926303)

[6.3.4.5. Group Update 15](#_Toc511926304)

[6.3.4.6. Manage Access 17](#_Toc511926305)

[6.3.4.7. Audit Configuration 20](#_Toc511926306)

[6.3.4.8. InfoSec Team Workgroup 20](#_Toc511926307)

[6.4 Version Control 20](#_Toc511926308)

[6.5 Verification procedure: 20](#_Toc511926309)

[6.5.1 Migration of Existing Active Directory Groups 20](#_Toc511926310)

[6.5.2 Group Management QuickLink 21](#_Toc511926311)

[6.5.3 Group Create 22](#_Toc511926312)

[6.5.4 Group Update 22](#_Toc511926313)

# Project Purpose

Emblem Health (“EH” henceforth) is looking for services from Cognizant to implement Identity and Access Management (IAM) service/system to streamline the business processes currently followed in user identity management for Emblem users and contractors.

Below are the modules that will be addressed by automation and process improvement in this release of Phase2 implementation of the identity management project:-

* Migration of existing Active Directory groups
* Automation of ongoing Active Directory Group Management

The Cognizant Team envisions addressing these gaps by rolling out improved and efficient identity management business processes through market leading COTS vendor product SailPoint IIQ. This document summarizes the requirement of this release of Phase 2 implementation in SailPoint IIQ.

# Document Purpose

This Deployment Plan describes the approach and controls for Emblem Health to deploy SailPoint IdentityIQ identity management solution in Emblem Health infrastructure. This plan will:

* Describe the approach that will be used to deploy the system
* Define the activities and documentation that will be followed during system deployment
* Ensures that the deployment activities are in alignment with the overall project plan

# Scope

## In-Scope

The in-scope of the deployment includes below configuration items:

* Migration of existing Active Directory groups
  + *ou=Application, ou=Groups, ou=Accounts, ou=CORP*
  + *ou=Distribution, ou=Groups, ou=Accounts, ou=CORP*
  + *ou=Security, ou=Groups, ou=Accounts, ou=CORP*
  + *ou=Application, ou=Groups, ou=Accounts, ou=HIPA*
  + *ou=Distribution, ou=Groups, ou=Accounts, ou=HIPA*
  + *ou=Security, ou=Groups, ou=Accounts, ou=HIPA*
* Automation of ongoing Active Directory Group Management
  + Group Create
    - *ou=<SelectedApplication>,ou=Application, ou=Groups, ou=Accounts, ou=CORP*
    - *ou=Distribution, ou=Groups, ou=Accounts, ou=CORP*
  + Group Update - all existing groups which will be migrated from Active Directory and all new groups which will be created from IIQ
  + Group Manage Access - all existing groups which will be migrated from Active Directory and all new groups which will be created from IIQ

## Out of Scope

* Group Migration
  + *ou=isilon, ou=Application, ou=Groups, ou=Accounts, ou=CORP*
  + *Groups under Medicare groups are out of scope*
* Group Create
  + There will be no groups created in Security ou *(ou=Security, ou=Groups, ou=Accounts, ou=CORP)* going forward
  + There will be no groups created in HIPA ou and Medicare ou going forward

# Roles & Responsibility

|  |  |  |
| --- | --- | --- |
| **Serial Number** | **Team Name** | **Responsibility** |
| 1 | SailPoint Team | Responsible for configuring SailPoint IdentityIQ and infrastructure |
| 2 | InfoSec Team | Responsible for taking care of configuration pertaining to QAR and Microsoft FIM |

# Definition & Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| IDM | Identity Management |
| IAM | Identity and Access Management |
| FTE | Full Time Employees |
| Cognizant Associates | Contractors working in Emblem from Cognizant |
| Vendor | Contractors working in Emblem other than Cognizant |
| PeopleSoft | On-premise HR system. Authoritative source for FTEs |
| EH PMO | Authoritative source for Cognizant Emblem Health Project Management Office |
| AD | Active Directory |
| Exchange | Email server used in EH |
| LCM | Life Cycle Manager |
| LOA | Leave of Absence |
| OOTB | Out of the box |
| SailPoint | SailPoint provides identity governance solutions with on-premises and cloud based IAM software.  [https://www.SailPoint.com/](https://www.sailpoint.com/) |
| Identity IQ | Identity IQ is a premiere identity management software that provides identity and access management control to business  [https://www.SailPoint.com/products/identityiq](https://www.sailpoint.com/products/identityiq) |
| Identity Now | IdentityNow is a cloud based identity management solution which will be leveraged got password management and SSO by EH |
| Virtual Appliance | It is virtual machine deployed within EH network and all communications between Identity Now and EH internal systems (e.g. AD) will take place through Virtual appliance |
| Source System | Source of truth for Identity IQ to trigger life cycle events such as joiner, mover and leaver. E.g. of source system is Work Day. |
| Target System | Systems that are updated by Identity IQ based on data received from Source systems. E.g. of target system is Active Directory. |
| Group | **Active Directory Group** |
| OU | Organizational Unit |

# Release Process

Follow the steps in the sequence below during deployment.

## File List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Object Type** | **Object Name** | **Import / Manual** | **Type** |
| **Group Migration** | Application | AD | Manual | Existing |
| Rule | EH\_Group\_Aggregation\_Refresh\_Rule | Import | Existing |
| Rule | EH\_AD\_Customization\_Rule | Import | Existing |
| TaskDefinition | EH Account Group Aggregation Task | Import | Existing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Object Type** | **Object Name** | **Import / Manual** | **Type** |
| **Group Create** | QuickLink | Create Group | Import | New |
| Custom | EH\_Group\_DN | Import | New |
| Rule | EH\_Rule\_Library\_2 | Import | Existing |
| Workflow | EH\_GroupManagement\_CreateGroup\_Workflow | Import | New |
| EmailTemplate | EH\_Email\_Create\_Group\_GroupAlreadyExist\_Notification | Import | New |
| EH\_Email\_Create\_Group\_Failure\_Requestor\_Notification | Import | New |
| EH\_Email\_Create\_Group\_Approval | Import | New |
| EH\_Email\_Create\_Group\_Rejected\_Notification | Import | New |
| EH\_Email\_Create\_Group\_Inactive\_GOManager | Import | New |
| EH\_Email\_Create\_Group\_Approval\_Reminder | Import | New |
| EH\_Email\_Create\_Group\_Success\_Notification | Import | New |
| EH\_Email\_Create\_Group\_Monthly\_Report | Import | New |
| EH\_Email\_Create\_Group\_Expired\_Notification | Import | New |
| AuditConfig | AuditConfig | Manual | Existing |
| Form | EH\_GroupManagement\_CreateGroup\_Form | Import | New |
| EH\_GroupManagement\_CreateGroup\_Form\_Approval\_RO | Import | New |
| Task Definition | Groups Created Monthly Report | Import | New |
| EH\_Groups\_Created\_Report | Import | New |

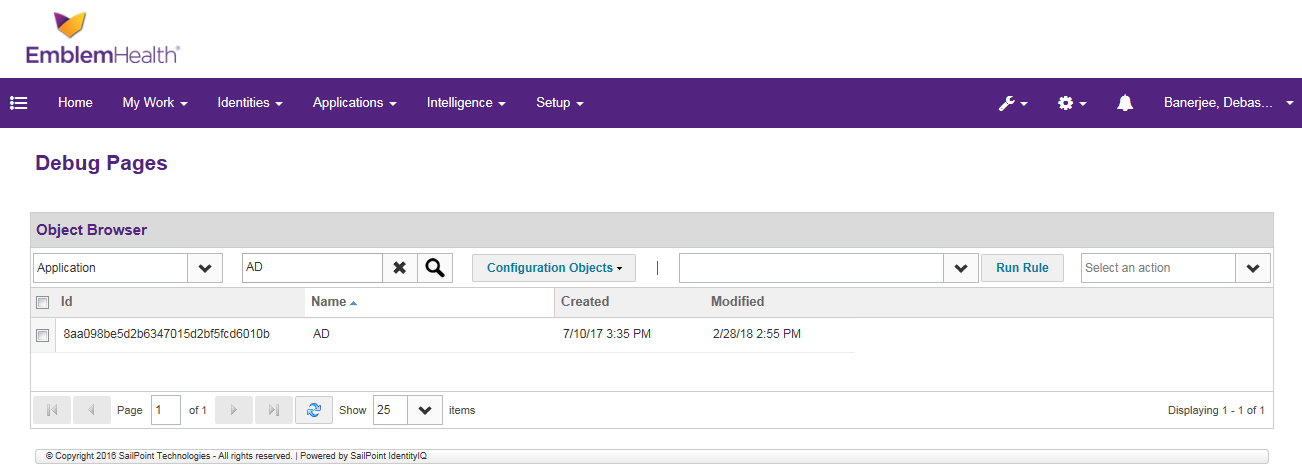
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Object Type** | **Object Name** | **Import / Manual** | **Type** |
| **Group Update** | Dynamic Scope | EH\_Group Update | Import | New |
| QuickLink | Update Group | Import | New |
|  | EH\_QuickLinkRestriction\_Groups | Import | New |
| Workflow | Entitlement Update | Import | Existing |
| EH - Update\_Group\_Workflow | Import | New |
| Email Template | EH\_Email\_Update\_Group\_Weekly\_Report | Import | New |
| EH\_Email\_Update\_Group\_Monthly\_Report | Import | New |
| EH\_Email\_Update\_Group\_Success\_Notification | Import | New |
| EH\_Email\_Update\_Group\_Failure\_Requestor\_Notification | Import | New |
| EH\_Email\_Update\_Group\_Generic\_Report | Import | New |
| AuditConfig | AuditConfig | Manual update | Existing |
| Form | EH - Update Groups Form | Import | New |
| EH - Update Group Report Form | Import | New |
| Task Definition | EH-Updated\_Groups\_Monthly\_Report | Import | New |
| EH-Update\_Groups | Import | New |
| EH-Updated\_Groups\_Weekly\_Report | Import | New |
| Groups Updated Monthly Report | Import | New |
| Groups Updated Generic Report | Import | New |
| Groups Updated Weekly Report | Import | New |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Object Type** | **Object Name** | **Import / Manual** | **Type** |
| **Group Manage Access** | QuickLink | Request Access | Manual | Existing |
| Dynamic Scope | Manager | Manual | Existing |
| Self Service | Manual | Existing |
| Rule | EH\_AD\_BeforeProvisioning\_Rule | Import | Existing |
| All Objects Roles | Import | New |
| Workflow | EH\_LCM\_Provisioning | Import | New |
| EH\_Provisioning\_Approval\_Subprocess | Import | New |
| EH\_Approve\_and\_Provision\_Subprocess | Import | New |
| EH\_Identity\_Request\_Notify | Import | New |
| EmailTemplate | EH\_LCM\_Requester\_Notification | Import | New |
| EH\_LCM\_Identity\_Update\_Approval | Import | New |
| EH\_Email\_ManageAccess\_Fail\_Notification | Import | New |
| EH\_LCM\_Reminder\_Notification | Import | New |
| UIConfig | UIConfig | Manual | Existing |
| Configuraion | Lifecycle Manager | Manual | Existing |
| Task Definition | EH - Access Request Status Report | Import | New |
| Full Text Index Refresh | Import | Existing |
| EH - Account Group Members Report | Import | New |
| Account Group Membership Generic Report | Import | New |
| Access Request Status Details Report | Import | New |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Object Type** | **Object Name** | **Import / manual** | **Type** |
| **DUO** | Application | DUO(email field should be "required" not "review required") | Import | New |
| Task-Account Aggregation | DUO Aggregation Task | Manual | New |
| Business Role | DUO\_Access | Manual(add DUO Application Provisioning Policy Form in the Role) | New |
| Rule | DUOSmsPassCodeIIQClient | Import | New |
| DUOEnrollmentIIQClient | Import | New |
| EH\_DUO\_RuleLibrary | Import | New |
| EH\_DUO\_Customization | Import | New |
| EH\_DUO\_BeforeProvisioning\_Rule | Import | New |
| EH\_DUO\_AfterProvisioning\_Rule | Import | New |
| DUOStatusIIQClient | Import | New |
| All Objects Roles | Import,add the role in Quicklink Populations-->Self Service | New |
| DynamicScope | Infosec Team | Import | New |
| CustomObject | EH\_Application\_Names | Modify | Modify |
| QuickLink | Manage Duo User | Import | New |
| QuickLinkCategory | DUO | append to SystemConfiguration.xml | Modify |
| Email Template | EH\_Email\_DUOEmailID\_Update | Import | New |
| EH\_Email\_DUO\_Activate\_Mobile | Import | New |
| EH\_Email\_DUO\_Mobile\_Update | Import | New |
| EH\_Email\_DUO\_Resend\_Enrollment\_Link | Import | New |
| EH\_Email\_DUO\_Provisioning | Import | New |
| EH\_Email\_DUO | Import | New |
| EH\_LCM\_Identity\_Update\_Approval | Import | New |
| EH\_Email\_DUO\_Unlock | Import | New |
| EH\_Email\_DUO\_Manage\_Failure\_Notification | Import | New |
| EH\_LCM\_Requester\_Notification | Import | New |
| Form | DUOManageForm | Import | New |
| DuoManageFormMessage | Import | New |
| DuoCheckStatusFrom | Import | New |
| Task Definition | EH\_DUO\_\_ManageAccess\_Report\_Weekly | Import | New |
| EH\_DUO\_\_ManageAccess\_Report\_Monthly | Import | New |
| EH\_DUO\_Request\_Access\_Report\_Monthly | Import | New |
| EH\_DUO\_Request\_Access\_Report\_Weekly | Import | New |
| Workflow | DUO Manage Access | Import | New |
| EH\_LCM\_Provisioning | Import | New |
| EH\_Approve\_and\_Provision\_Subprocess | Import | New |
| EH\_Provisioning\_Approval\_Subprocess | manual | Modify |
| EH\_Workflow\_Leaver\_Deprovisioin | manual | Modify |
|  | AuditConfig | AuditConfig | Manual | Modify |
|  | SystemConfiguration | SystemConfiguration | Manual | Modify |

## Backup

We need to take back-up of all the existing files that are going to be impacted. Please refer to file list for reference.

For example, below is the screenshot to take application **‘AD’** back-up from the debug page

1. **Workflow**

* EH - Create Service Account Workflow

1. **Form**

* EH - Service Account Report Form
* EH – ManageServiceAccountsReportForm
* EH - Ownership Transfer of Service Account On Termination Report Form

1. **TaskDefinition**

* EH - Service Account Created Generic Report
* EH - Service Account Created Report
* EH - Service Account Owner Reports
* EH - Service Account Owner Report
* EH - Manage Service Account
* EH - Manage Service Account Generic Report
* EH - Ownership Transfer On Termination
* EH - Ownership Transfer On Termination Generic Report

## Rollback

Revert back the changes in Identity IQ by re-importing the backed up files.

## Deployment Steps

### UI Branding - 4

Follow the below steps for branding in all four production server

* Take backup for the old css file.
* Stop the server to which changes are to be done.
* Copy the below iiq-custom.css file from ‘/apphome/sailpoint/apache-tomcat-8.5.12/webapps/identityiq/css’ of dev server and replace the file in the production server in the same location.
* In another way, open iiq-custom.css file in vi editor and make the change.



### Place END user guide – 2

In UI servers

### Proxy Configuration (ADDED in PROD, NEED TO RAISE FIREWALL REQUEST port 80, then revert)

* + 1. Login to Sailpoint server
    2. Go to below location /apphome/sailpoint/apache-tomcat-8.5.12/bin
    3. Open setenv.sh file and update the file with below lines:

***export JAVA\_OPTS="$JAVA\_OPTS -Dhttps.proxyHost=ehproxy.emblemhealth.com -Dhttps.proxyPort=8080"***

* + 1. Repeat steps 1 – 3 for all servers.

### Import Duo certificate - 4

* + - 1. Download Duo certificate from browser and store it in **/apphome/sailpoint/installers** location
      2. Login to the server using Putty and run this below command.

*keytool -import -v -alias DUO -file /apphome/sailpoint/installers/* *duouat.cer -keystore /apphome/sailpoint/SSL/tomcatca.jks*

* + - 1. Repeat steps 1 – 2 for all the servers.

### Update Audit Configuration

To update Audit Configuration, follow the below steps:

1. Login to IIQ web console using ‘spadmin’ privilege
2. Navigate to /debug page
3. Search and select ‘AuditConfig’ in object browser
4. Search
5. Open the AuditConfig XML
6. Search for ‘*AuditAction’* entry in the XML
7. Add below entry for the custom category

**Update Group**

*<AuditAction displayName="Group\_Management\_Update\_Group" enabled=”true” name=”UpdateGroup"/>*

**

**Create Group**

*<AuditAction displayName="* *Group\_Management\_Create\_Group" enabled=”true” name=”* *CreateGroup"/>*

**

***DUO***

|  |
| --- |
| <AuditAction displayName="DUO\_Manage\_Access" enabled="true" name="DUOManageAccess"/>  <AuditAction displayName="DUO\_Request\_Access" enabled="true" name="DUORequestAccess"/> |



1. Click on **“Save”** button to save changes.

### Restart Tomcat servers

Restart all servers. Hence test connection will be successful between DUO and IIQ.

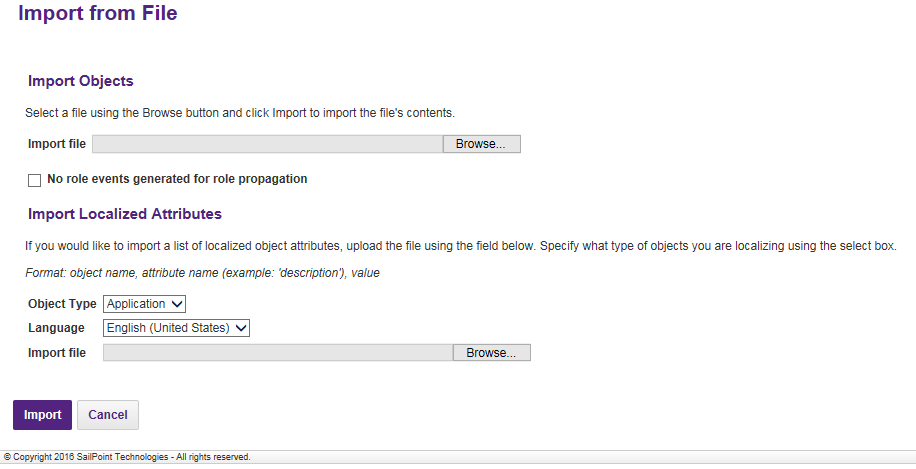
### Steps to Import using script

To import the components, please follow the below steps:

1. Navigate to **Global Settings 🡪 Import from Rules**. The following page will appear
2. **Browse** for the below attached import script



1. Click on **Import** button



### Configuration

Configure the below components in SailPoint production environment

### Request /Manage DUO access

Import/Modify the below components:

### Import Application

Import the below application object using the steps described under the section 6.3.2

1. DUO

We have to provide DUO api host name, Client ID and Secret Key which needs to be generated from DUO portal.

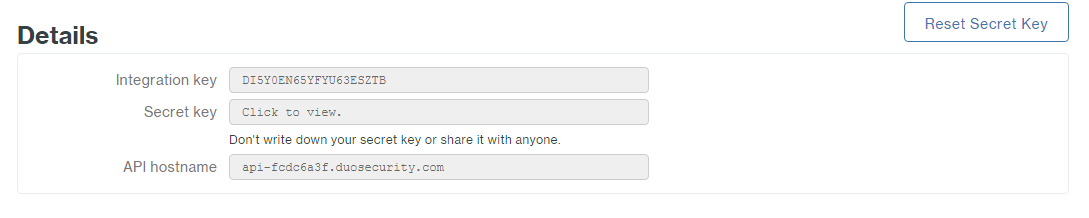
**In Duo**

* + - 1. Login as an administrator user and log into the **Duo Administrator Panel**.

Note:Ensure that the administrator creating the new Administrator API integration has the following permissions: - Grant Administrators- Grant Applications- Grant Read Resource

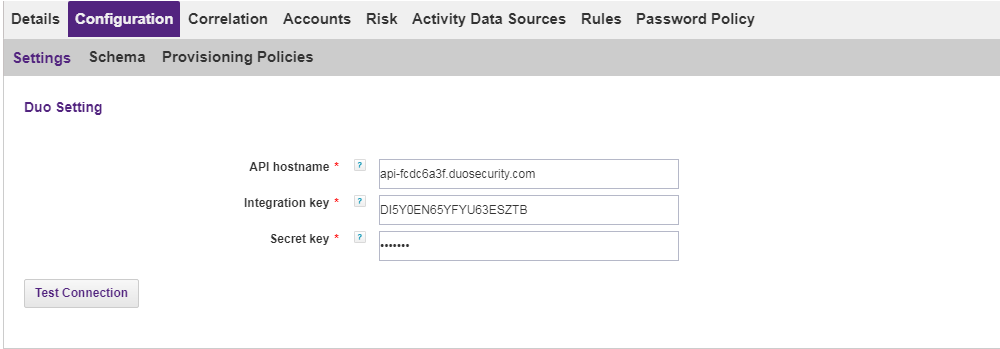
1. Create a new Admin API integration.

This will generate an integration key and secret key for you to use as mentioned in the following “Configuration parameters” section.



Now we have to provide below details in Sailpoint IIQ.

|  |  |
| --- | --- |
| API host name | api-fcdc6a3f.duosecurity.com |
| Integration Key | DI5Y0EN65YFYU63ESZTB |



After providing all details we have to configure proxy in tomcat server and import DUO certificate in Sailpoint server keystore using below commands.

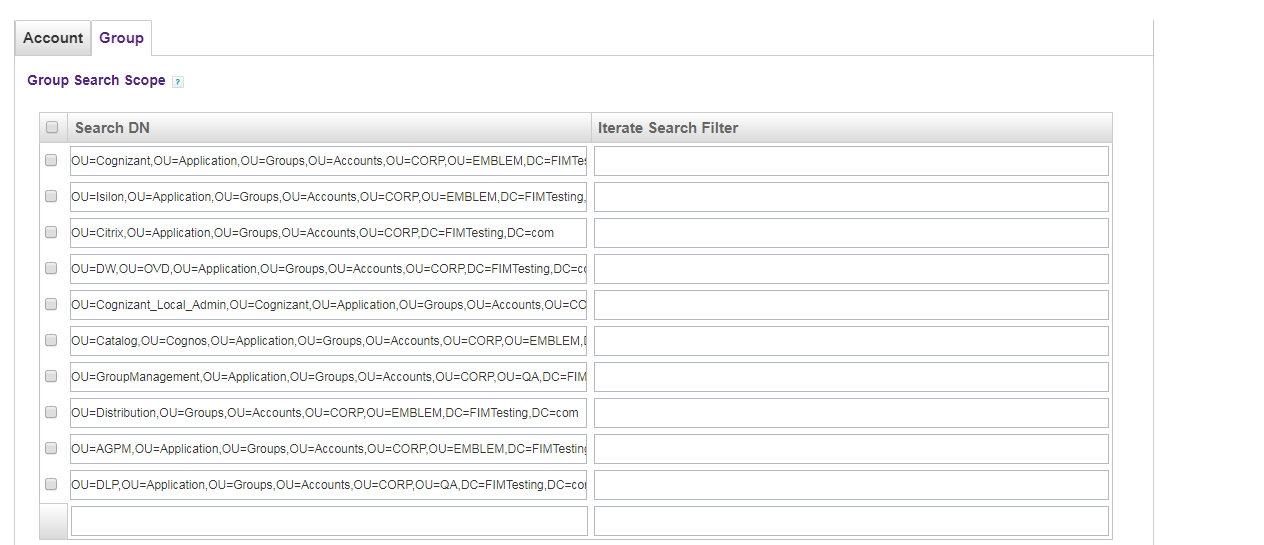
### Migration of Existing Active Directory groups

**Application**

Navigate to the below path in IIQ.

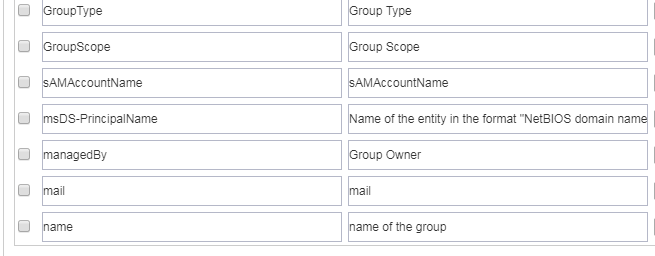
Applications->AD->Configuration->Settings->Group

1. Add the below group search DNs – one OU AGPM
   1. ou=Application,ou=Groups,ou=Accounts,ou=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM
   2. ou=Distribution,ou=Groups,ou=Accounts,ou=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM
   3. ou=Security,ou=Groups,ou=Accounts,ou=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM
   4. ou=Application,ou=Groups,ou=Accounts,ou=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM
   5. ou=Distribution,ou=Groups,ou=Accounts,ou=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM
   6. ou=Security,ou=Groups,ou=Accounts,ou=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM



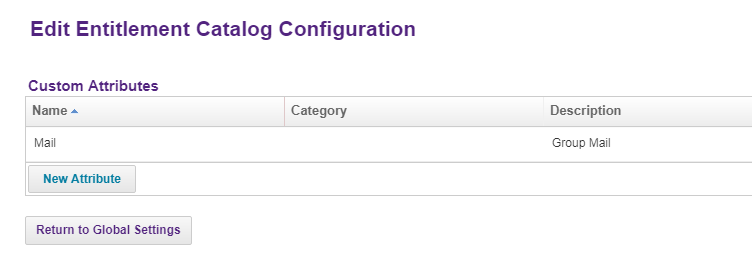
1. Add the attribute with below details in schema for object type ‘**group’**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl#** | **Name** | **Description** | **Type** | **Properties** |
| 1 | managedBy | Group Owner | string |  |
| 2 | mail | mail | string |  |
| 3 | name | name | string |  |



1. Add the below in Global Settings 🡪Entitlement Catalog Attributes 🡪 New Attribute

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sl#** | **Attribute Name** | **Display name** | **Type** | **Description** | **Searchable** | **Editable** |
| 1 | mail | Mail | String | Group Mail | TRUE | FALSE |

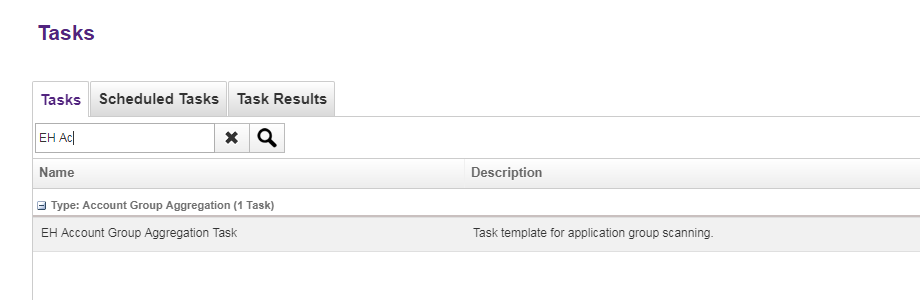


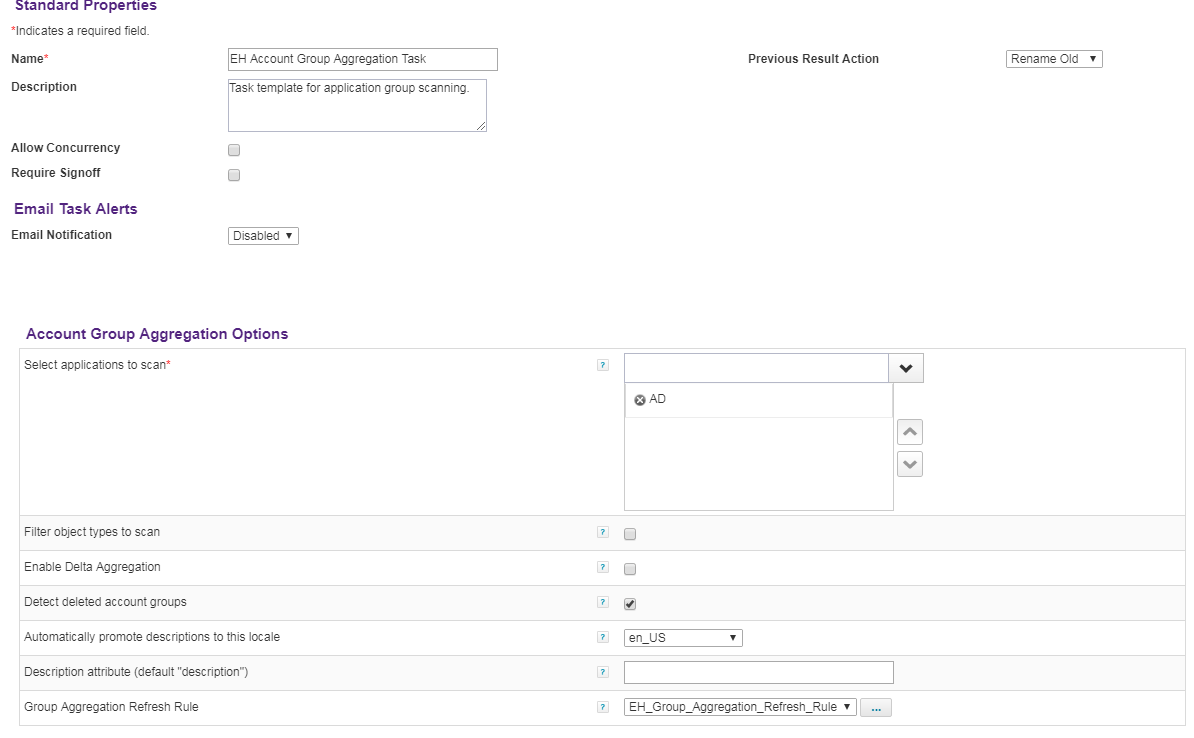
1. Update the below rules:

* EH\_Group\_Aggregation\_Refresh\_Rule
* EH\_AD\_Customization\_Rule

### Run AD Group Aggregation

Run the EH Account Group Aggregation Task to import the AD, DLP groups from AD to IIQ





### Run Full AD Account Aggregation

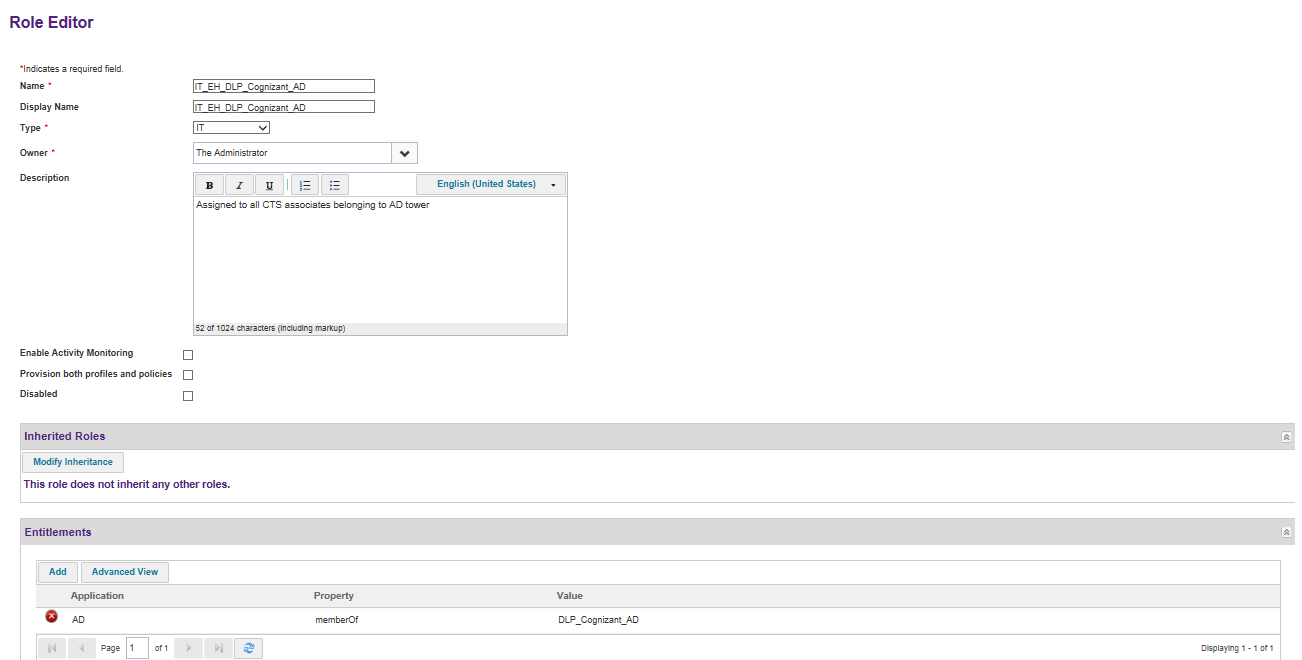
* + 1. Search for the task - “Full AD Account Aggregation” Task
    2. Right click on it and click on “**Execute”** button

### Creation of IT Role

Follow the below steps to create the IT Roles

1. Go to Set up🡪 Roles
2. Click on ADD new role and select IT from the “Type” drop down.
3. Add the name , the display name and description for the role
4. Add the entitlement to the role in the Entitlement Section.
5. Attach the AD rule and click on submit.

Repeat the above steps for all the 22 IT roles that need to be created.



### Creation of Business role

### DUO

**Steps:**

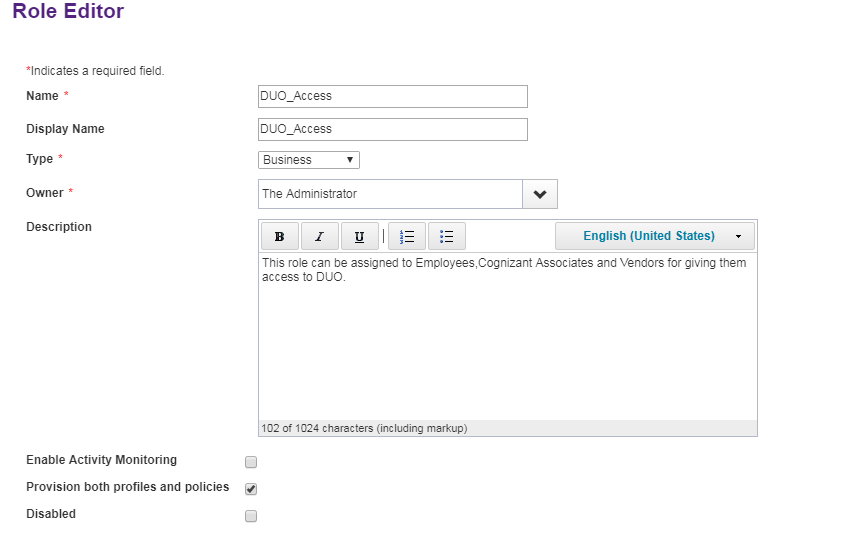
1. Navigate to Setup🡪Roles
2. Click on “**New Role**”
3. Provide the following details:

Name: “**DUO\_Access**”

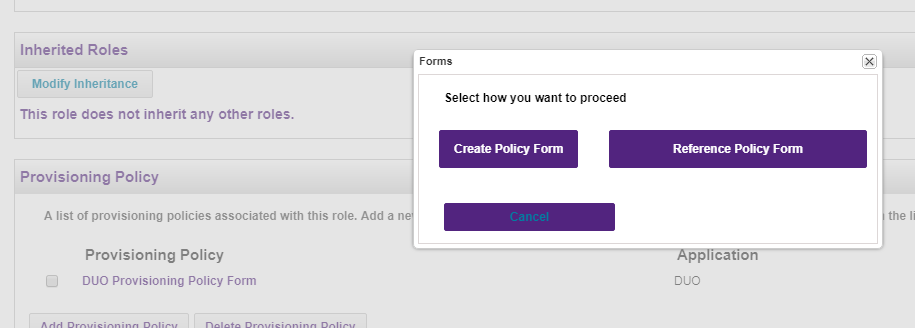
Display Name: **“DUO\_Access”**

Type: ”**Business**”

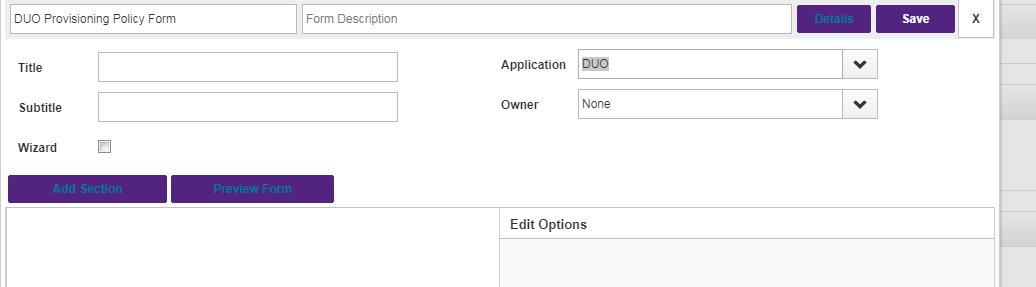
1. Provide a Role Description.
2. Select “**Provision both profile and policies**” checkbox.



1. Go to Provisioning Policy section.
   1. Click on Add Provisioning Policy
   2. Click on Create Policy Form.



1. Provide the below details:
   1. Form Name and Description.
   2. Select **DUO** from the Appilcation dropdown list.
   3. Click on Save button.

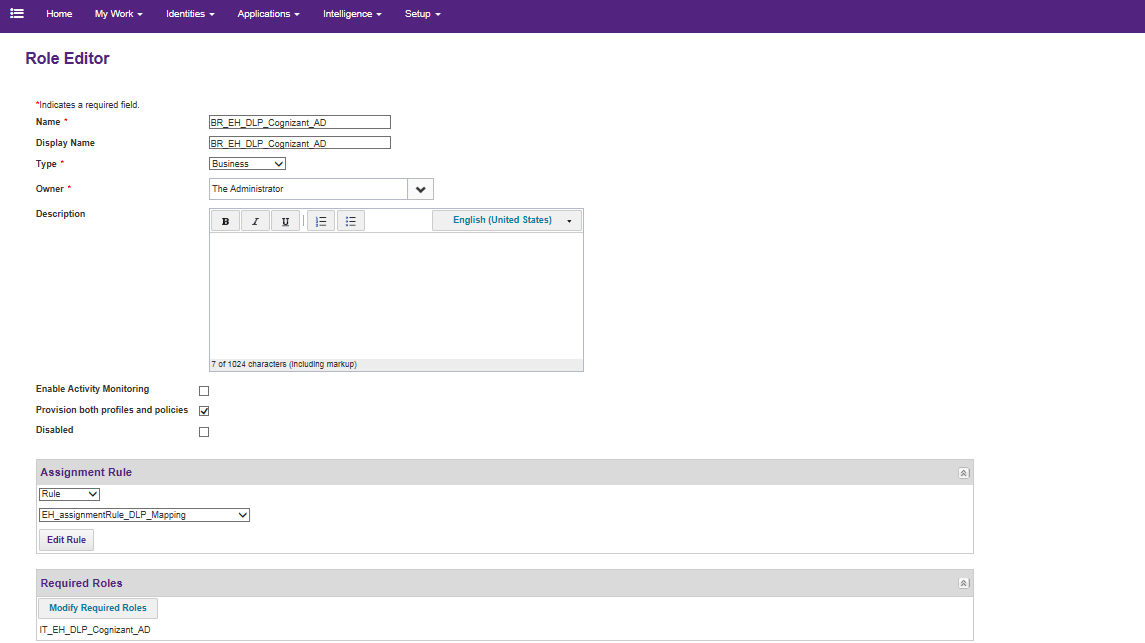


### DLP Roles

Follow the below steps to create the Business Roles

1. Go to Set up🡪 Roles
2. Click on ADD new role and select Business in the “Type” dropdown
3. Add the name , the display name and description for the role
4. Select Rule in the dropdown for Assignment Rule Section. Add the assignment rule “EH\_assignmentRule\_DLP\_Mapping” from the drop down
5. Attach the corresponding IT role in the Required Roles section and click on submit.

Repeat the above steps for all the 22 Business roles that need to be created.



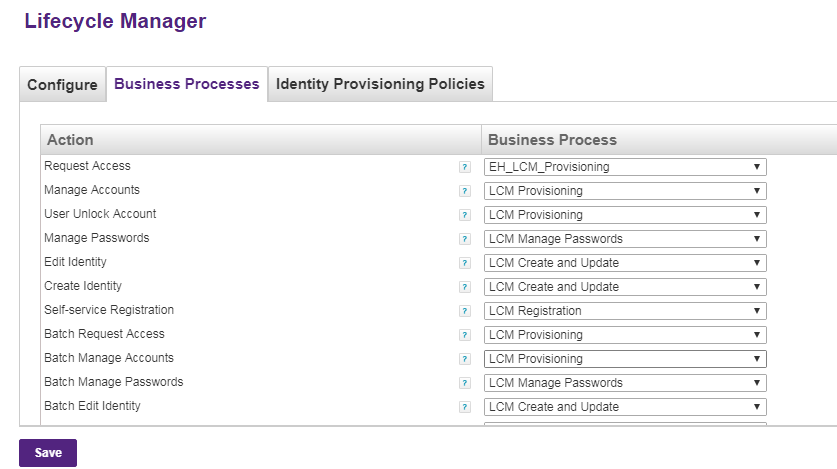
### Run Refresh task for EHPMO

* + 1. Search for the task – “Refresh Identity Cube – Provisioning EHPMO” and click on Edit button
    2. Execute the task

### Lifecycle Manager Configuration

Select the appropriate workflow for manage access

* Navigate to Lifecycle Manager
* Click on Business Processes
* Select workflow ‘EH\_LCM\_Provisioning’ for action ‘Request Access’
* Click on SAVE



### QuickLink Category

To add custom quick link categories, follow the below steps:

1. Login to IIQ web console using ‘spadmin’ privilege
2. Navigate to /debug page
3. Search and select ‘Configuration’ in object browser
4. Search ‘*System Configuration*’
5. Open the object XML
6. Search for ‘*quickLinkCategories*’ entry in the XML
7. Add below entry for the custom category:
   1. **AD Group Management**

|  |
| --- |
| <QuickLinkCategory cssClass="quickLinkCategoryEHGroupManagement" messageKey="Group Management" name="EHGroupManagement" ordering="9"/> |

******

* 1. ***DUO***

<QuickLinkCategory cssClass="quickLinkCategoryTasks" messageKey="Duo" name=”Duo" ordering="10"/>



1. Click on “**Save**” button to save changes.

### Quicklink Configuration

**QuickLink**

Add category=”Access” in Request Access

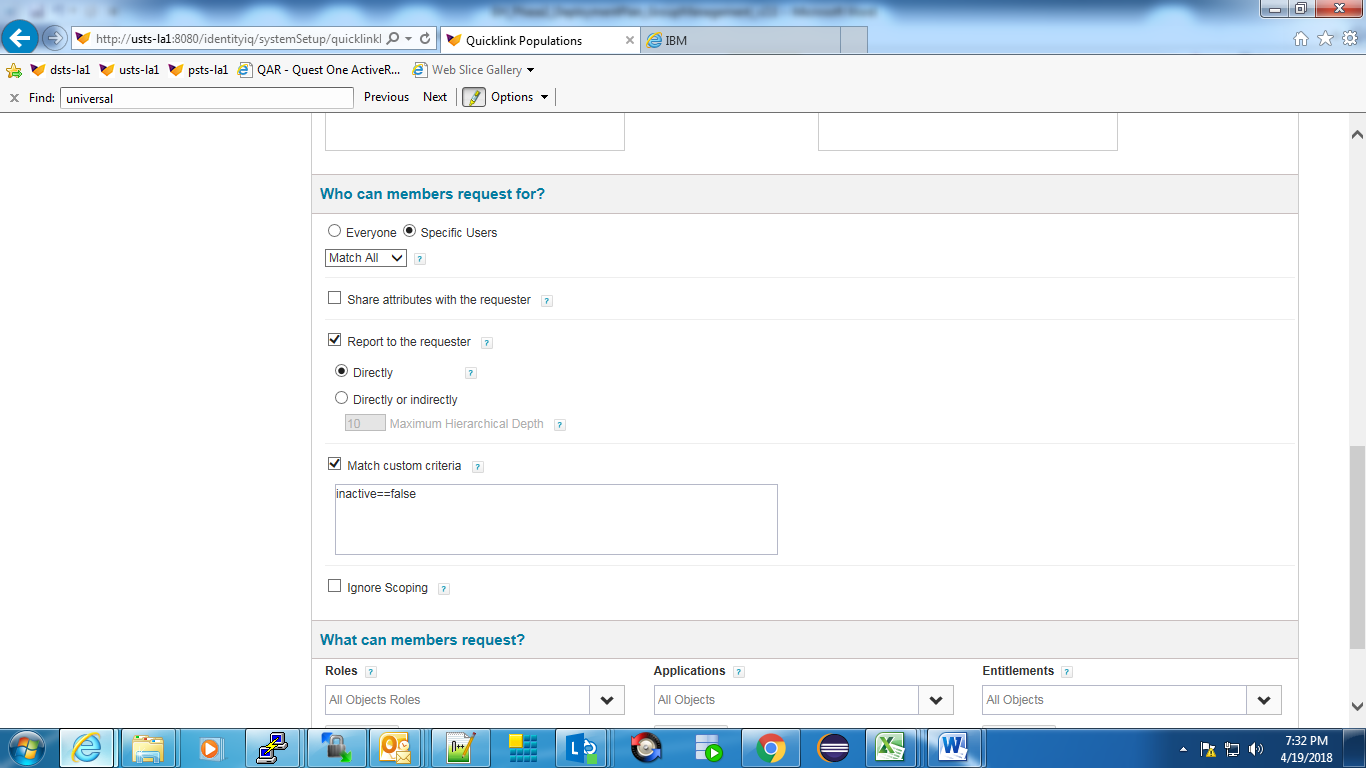
****

### Dynamic Scope Configuration

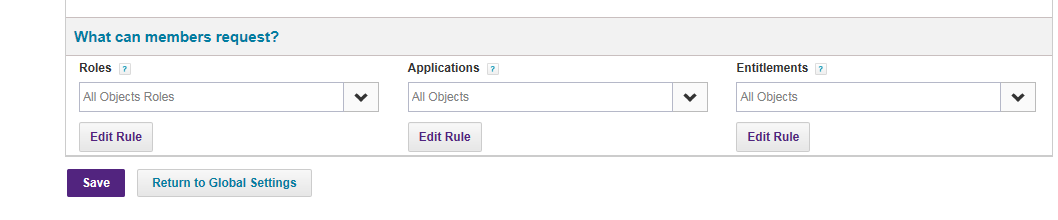
Navigate to Global Configuration 🡪 QuickLink Population. Update the below

***Manager***

1. Configuration - Who can member request for
   1. Select specific user
   2. Match All option
   3. Report to the requester – Directly
   4. Match custom criteria (inactive==false)

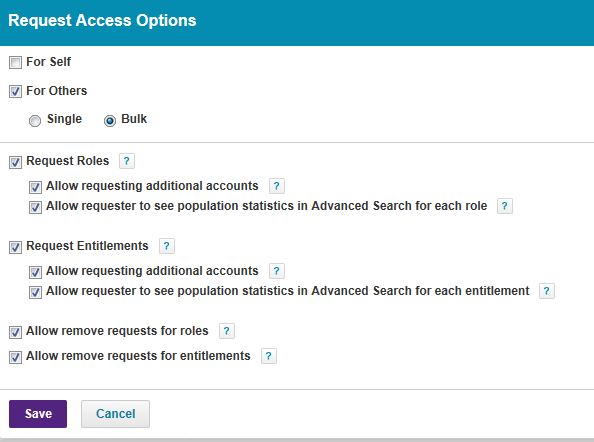


1. Configuration - What can members request
   1. Roles – All Objects Roles
   2. Applications – All Objects
   3. Entitlements – All Objects

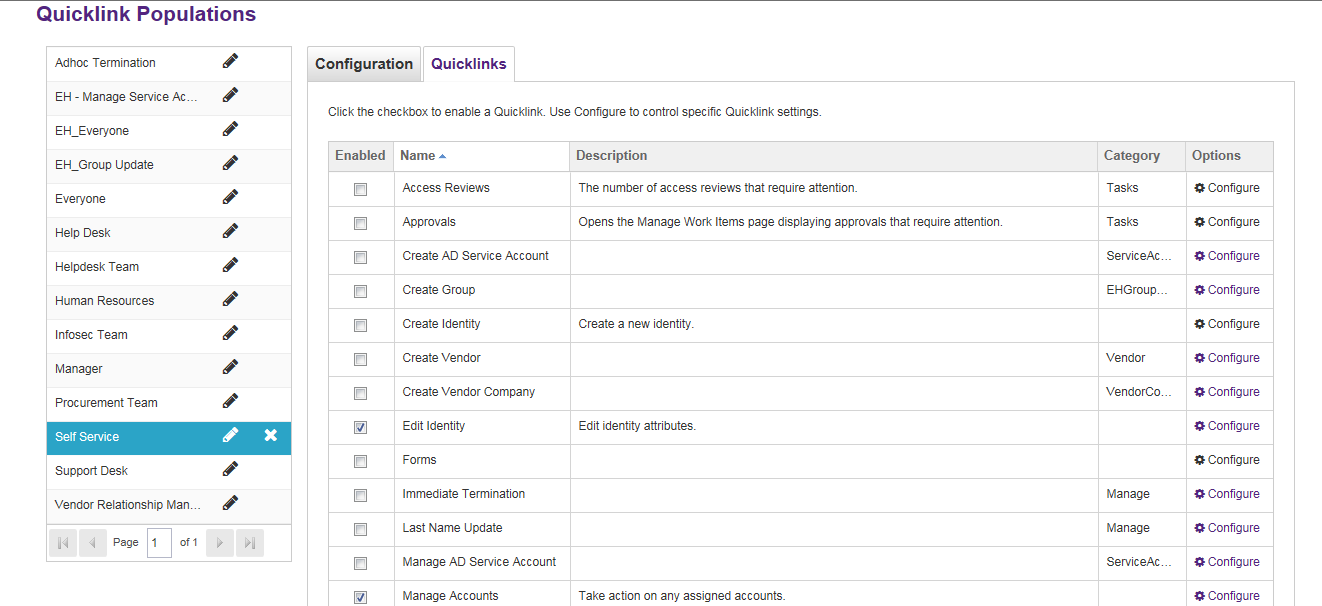


1. Quick Links
   1. Select Request Access
   2. Click on configure. Select the below
      1. For Others – Bulk
      2. Request Roles – Both Options
      3. Request Entitlements – Both Options
      4. Allow remove request for roles
      5. Allow remove request for entitlements

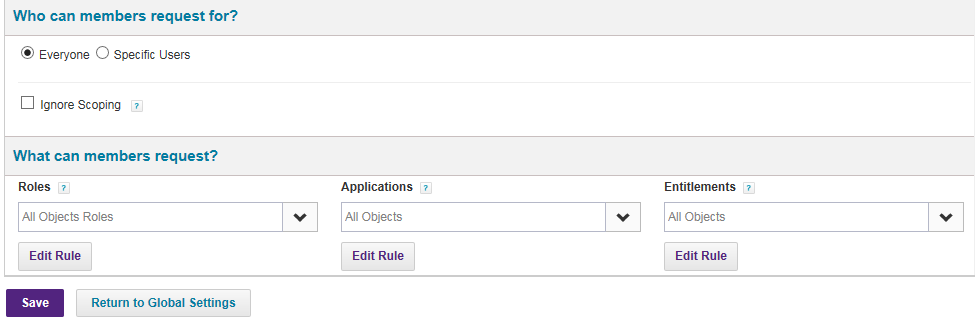




***Self Service***

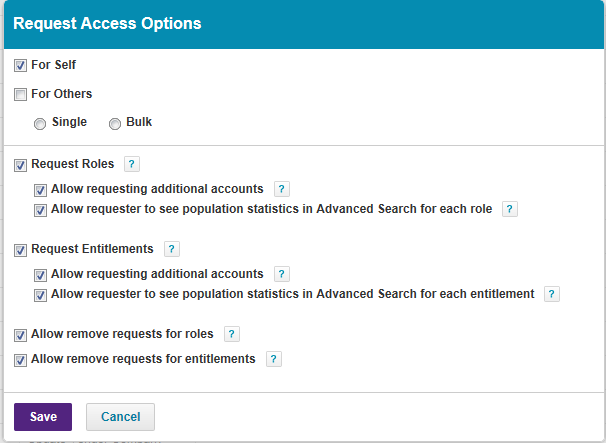


1. Configuration - Who can member request for
   1. Everyone
2. Configuration - What can members request
   1. Roles – All Objects Roles
   2. Applications – All Objects
   3. Entitlements – All Objects



1. Quick Links
   1. Select Request Access
   2. Click on configure. Select the below
      1. For Self
      2. Request Roles – Both Options
      3. Request Entitlements – Both Options
      4. Allow remove request for roles
      5. Allow remove request for entitlements





### Update UIConfig

Update the UIConfig as per below:

* IdentitySearchAttribute
  + displayName
  + name
  + firstname
  + lastname
  + networkID



<entry key="identitySearchAttributes" value="displayName,name,firstname,lastname,networkID"/>

* uiRequestAccessIdentityCard
  + networkID
  + email



<entry key="uiRequestAccessIdentityCard">

<value>

<List>

<ColumnConfig dataIndex="networkID" groupProperty="networkID" headerKey="Network ID" property="networkID" sortProperty="networkID" stateId="networkID"/>

<ColumnConfig dataIndex="email" groupProperty="email" headerKey="Email" property="email" sortProperty="email" stateId="email"/>

</List>

</value>

</entry>

* uiAccessItemsColumnsEntitlement
  + **Remove attribute:** memberOf from Add access page
* uiCurrentAccessItemsColumnsEntitlement
  + **Remove attribute:** memberOf from Remove access page

### Update Custom Object

Update the below Custom Object comparing with the production environment.

EH\_Application\_Names

<entry key="duo" value="DUO"/>



### Update Rule

Update the below rule:

* EH\_AD\_BeforeProvisioning\_Rule

### Update workflow

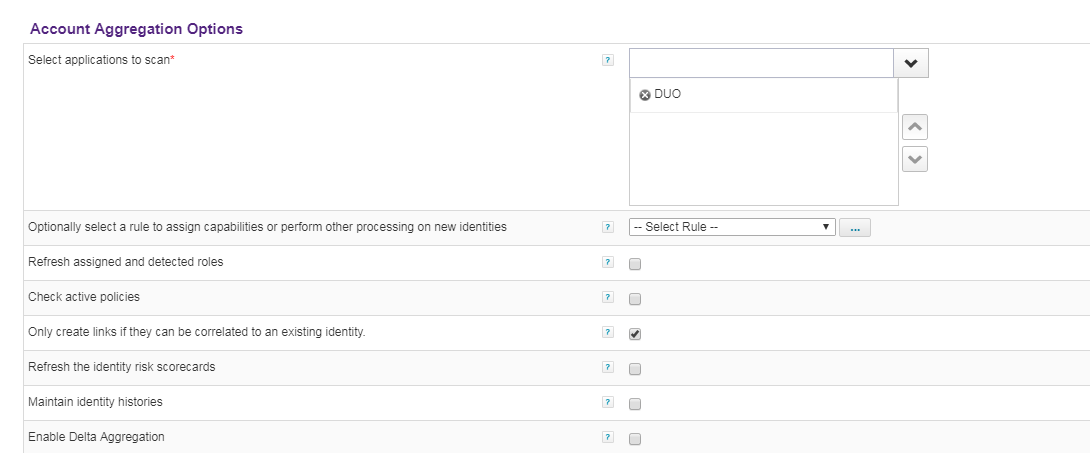
Update the below workflow comparing with the production environment (for DUO)

1. 1. EH\_Workflow\_Leaver\_Deprovision

### Create Aggregation Task (DUO)

**Steps:**

1. Navigate to Setup🡪Tasks
2. Create New Task🡪Account Aggregation
3. Name the task as “DUO Aggregation Task”
4. Select **DUO** application in the **“applications to scan”** section:
5. Check **“Only create links if they can be correlated to an existing identity”** checkbox.



5. Click on **Save** button.

### Add members to InfoSec Team Workgroup

To add an Identity as a member to InfoSec Team, follow the below steps:

1. Login to IIQ web console using ‘spadmin’ privilege
2. Navigate to Setup->Groups
3. Go to ‘Workgroup’ and search for ‘EH\_IDM\_ADMIN’ workgroup
4. Under Members section, search for the user and click on Add Members

## Version Control

Upload the xml files in respective folders using Microsoft Visual Studio 2010.

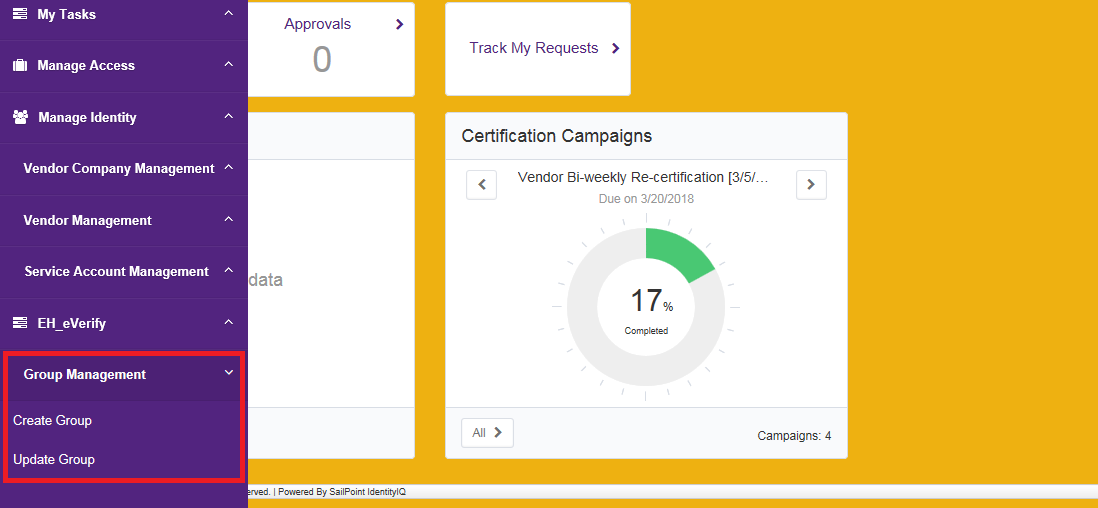
## Verification procedure:

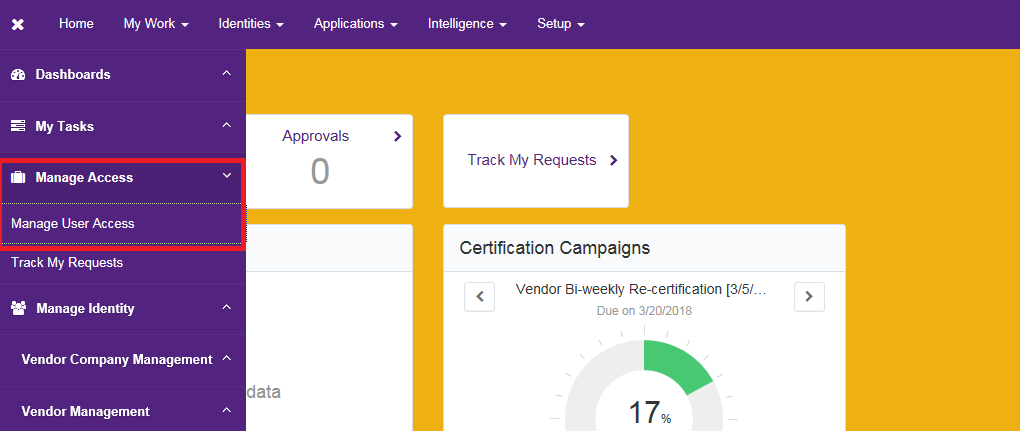
### Migration of Existing Active Directory Groups

Check the below

* Run EH Account Group Aggregation Task
* Compare the number of groups available in Active Directory and number of managed attribute objects available in the system post migration
* Verify if the below group details are updated correctly in the system
  + Group name
  + Group owner
  + Group description
  + Group Type
  + Group Scope
  + Group requestable
  + Group Members
  + Group Email
* Verify if the groups are available for Manage Access

### Group Management QuickLink

Check the below QuickLink are available under category ‘Group Management’ and are accessible

Check the below QuickLink is available under category ‘Manage Access’ and is accessible 

### Group Create

* Create a test group by launching the quick link Create Group and fill up the required details for group creation
* Verify if the below group details are updated correctly in IIQ and AD as provided during group creation process:
  + Group Name
  + Group Owner
  + Group Display Name
  + Group Description – Updated with the role and application name for Security Group provided while creation
  + Group Type
  + Group Scope
  + Group isrequestable
  + Group Members
  + Group Email

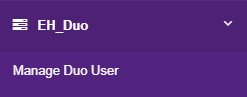
### Group Update

* Update a test group by launching the quick link Update Group and modify the required details for group updation
* Verify if all the below group details are updated correctly in IIQ and AD as provided during group updation process:
  + Group Display Name
  + Group owner
  + Group description
  + Group isrequestable

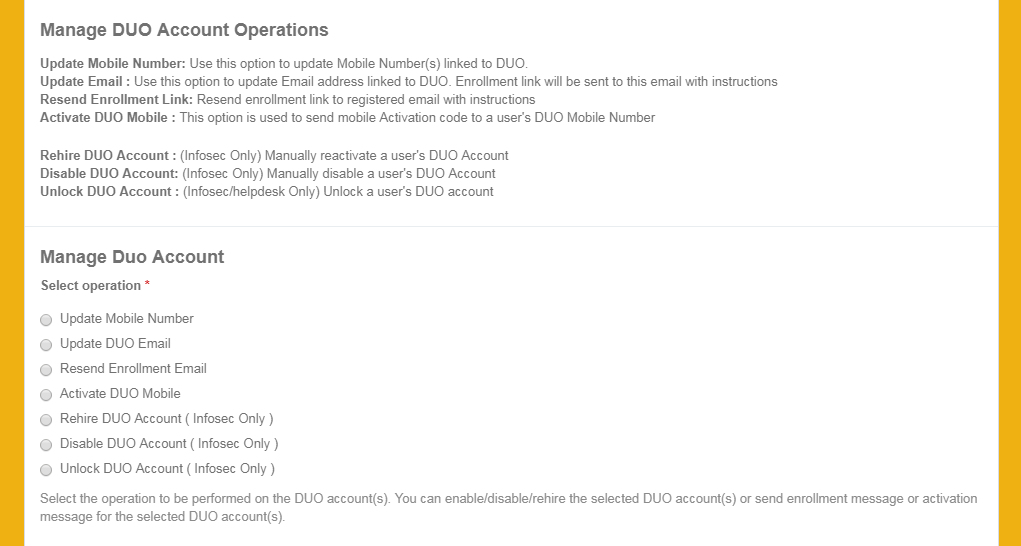
### Manage Access

### Manage Duo User

1. Check the below Quicklinks are accessible



1. Check whether form is getting generated

.

1. Check whether all test-cases are working successfully.

### Create Service Account:

1. Login to IDM
2. Open the Quicklink **Service Account Management -> Create AD Service Account**
3. Raise Service Account request through form as End User
4. Manager Approval should be generated.
5. Navigate to **MyWork -> Access Requests** the Access request should show the **Pending Interactions** as “Manager Approval”

### Reports

1. Login to IDM
2. Navigate to **Intelligence -> Reports**
3. Search for “**EH – Service Accounts Pending request Reports**” and **Right Click -> Edit**
4. Add Email Recipients and file format as **CSV** and Click **Save and Execute** button
5. Report should be generated with the pending request approval data

### Task to update description in AD:

1. Place feed file in the path **/apphome/sailpoint/CSVFILES/INPUT/SERVICE\_ACCOUNT**. Feed file should contain two columns: samaccountname and description.
2. Login to IDM
3. Navigate to **Setup -> Tasks**
4. Search for “**EH Service Accounts Description Update**” Task and **Right Click -> Edit**
5. Give the following input in the Rule Config

**fileSeparator,”,”,filePath,/apphome/sailpoint/CSVFILES/INPUT/SERVICE\_ACCOUNT/ServiceAccount- DescriptionUpdate.csv**

1. Click **Save and Execute**
2. Description should be updated in AD and IIQ.