EmblemHealth

**Office 365 Provisioning**

**Design Document**



Version 1.0

Effective Date: 03/26/2018

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 |  |
| Manisha Roy | Cognizant | Approver |  |
| Randall Dulin | Cognizant | Approver |  |
| Jim Altinay | Emblem Health | Approver |  |
| Tom McDermott | Emblem Health | Approver |  |

Revision History

| **Version** | **Version Date** | **Author** | **Reviewed by** | **Comments** |
| --- | --- | --- | --- | --- |
| 1.0 | 3/26/2018 | Cognizant |  | Initial Version |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Design Document 2](#_Toc514867336)

[Revision History 4](#_Toc514867337)

[Table of Contents 5](#_Toc514867338)

[1.0 Introduction 7](#_Toc514867339)

[1.1 Document Purpose 7](#_Toc514867340)

[1.2 Project Purpose 7](#_Toc514867341)

[1.3 Design Scope 7](#_Toc514867342)

[1.3.1 In Scope 7](#_Toc514867343)

[1.3.2 Out of Scope 7](#_Toc514867344)

[1.4 Intended Audience 7](#_Toc514867345)

[1.5 Definition & Acronyms 7](#_Toc514867346)

[1.6 References 8](#_Toc514867347)

[2.0 Assumptions and Dependencies 8](#_Toc514867349)

[2.1 Design Considerations 8](#_Toc514867350)

[2.2 Assumptions 9](#_Toc514867351)

[2.3 Dependencies 9](#_Toc514867352)

[2.4 Constraints 9](#_Toc514867353)

[3.0 System Overview 9](#_Toc514867354)

[3.1 Description 9](#_Toc514867355)

[3.2 System Architecture 9](#_Toc514867356)

[3.2.1.1. TO-BE 9](#_Toc514867357)

[3.2.1.2. AS-IS 11](#_Toc514867358)

[4.0 Current State vs Future State – Requirements 12](#_Toc514867359)

[4.1 User Mailbox 12](#_Toc514867360)

[4.1.1 New Hires 12](#_Toc514867361)

[4.1.2 Termination of Employees 14](#_Toc514867362)

[4.1.3 Termination of Cognizant Associates and Vendors 16](#_Toc514867363)

[4.1.4 Termination of Users due to inactivity 18](#_Toc514867364)

[4.1.5 Rehire/Reactivation 19](#_Toc514867365)

[4.1.6 Rebadging or Employee to Vendor or Vendor to Employee Conversion 21](#_Toc514867366)

[4.1.7 Profile Updates sync from On Premise AD to Azure AD 23](#_Toc514867367)

[4.2 Distribution Lists 23](#_Toc514867368)

[4.2.1 Create Distribution List 23](#_Toc514867369)

[4.2.2 Edit DL Properties 23](#_Toc514867370)

[4.2.3 Add/remove Members in Group 24](#_Toc514867371)

[4.2.4 Rename DL 24](#_Toc514867372)

[4.3 Group Mailbox/Shared Mailbox 24](#_Toc514867373)

[4.3.1 Create Group mailbox 24](#_Toc514867374)

[4.3.2 Assign Permissions to Mailbox for users 25](#_Toc514867375)

[4.3.3 Edit Mailbox properties 25](#_Toc514867376)

[4.4 Define a way for co-existence of processes during migration activity 25](#_Toc514867377)

[4.5 Other Scenarios 25](#_Toc514867378)

[4.5.1 QAR provisioning of mailbox for Non Corp OU 25](#_Toc514867379)

[4.5.2 Mail enable a Security group 25](#_Toc514867380)

[5.0 System Design – IIQ 26](#_Toc514867381)

[5.1 AD Application 26](#_Toc514867382)

[5.1.1 Schema Attribute 26](#_Toc514867383)

[5.1.2 Provisioning Policy 26](#_Toc514867384)

[5.2 Workflows 26](#_Toc514867385)

[5.2.1 New Hire 26](#_Toc514867386)

[5.2.2 Termination 27](#_Toc514867387)

[5.2.3 Rehire 27](#_Toc514867388)

[5.2.4 AD Group Management 27](#_Toc514867389)

[5.3 Rules 28](#_Toc514867390)

[5.3.1 Rules 28](#_Toc514867391)

[5.3.2 Rule Library 28](#_Toc514867392)

[5.4 Custom 29](#_Toc514867393)

[5.5 Tasks 29](#_Toc514867394)

[5.6 Reports 29](#_Toc514867395)

[5.7 Email Templates 30](#_Toc514867396)

[6.0 System Design – Exchange/Office 365 30](#_Toc514867397)

[6.1 Placholder for Exchange and Office365 team 30](#_Toc514867398)

[7.0 Testing Approach 30](#_Toc514867399)

[8.0 Attributes and OU 31](#_Toc514867400)

[8.1 OU Synchronized 31](#_Toc514867401)

[8.2 Attributes Synchronized between On Premise AD and Office 365 32](#_Toc514867402)

[9.0 Appendix A - Naming Conventions / Business Logics 34](#_Toc514867403)

[9.1.1 AD Network id Naming convention 34](#_Toc514867404)

[9.1.2 AD – CN Naming convention 34](#_Toc514867405)

[9.1.3 Email Address Naming convention 34](#_Toc514867406)

[9.1.4 Active Directory Placement Policy 35](#_Toc514867407)

[10.0 Open Items 38](#_Toc514867408)

# Introduction

## Document Purpose

This document puts forth a technical design for Office 365 integration with SailPoint IIQ.

This document is for the technical audiences of this project comprising the developers working in this project, design engineers and architects along with different teams and stakeholders who will be part of the project. .

## Project Purpose

This document puts forth a technical design for Office 365 integration with SailPoint IIQ and IdentityNow

This document is for the technical audiences of this project comprising the developers working in this project, design engineers and architects along with different teams and stakeholders who will be part of the project. .

## Design Scope

### In Scope

* SailPoint IIQ
  + Replace the existing automated Direct provisioning in Exchange with office 365

### Out of Scope

* Direct Provisioning to Office 365
* License Management in Office 365
* Any users that are not in scope for SailPoint
* Internet access for Office 365
* Power BI users mailbox are created manually in office 365
* Archival/Retention/Legal hold process is out of scope of Infosec and is managed by Exchange team. Existing process should be followed in office 365
* Anything not explicitly called out as in-scope.

## Intended Audience

## 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 |
| EHPMO | Authoritative source for Cognizant Emblem Health Project Management Office |
| AD | Active Directory |
| Exchange | Email server used in EH |
| 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) |
| IdentityNow | IdentityNow is a cloud based identity management solution which will be leveraged got password management and SSO by EH |

## References

* + SailPoint product manuals



# Assumptions and Dependencies

## Design Considerations

***General***

* Office 365 environment will be deployed as a Hybrid solution
* There is only one environment of office 365
* DirSync is configured to run every 30 minutes to pull data from on-premise AD to Azure AD
* Only one directional data flow is configured in Office 365 (On-premise to Azure AD)
* Only Corp and HIPA OU data (Employees and Contractors) is synced in SailPoint
* The migration to office 365 from on premise Exchange will be done on a phased wise manner with mailboxes moving in batches from on premise exchange to Cloud office 365
* Commands for enabling mailbox and archiving mailbox are run by Exchange team.
* The OUs out of scope of Office 365 will continue to be provisioned in on –premise Exchange
* Licenses should be assigned by *Office 365* team

## Assumptions

* TBD

## Dependencies

* Product vendors for any product issues

## Constraints

* Unavailability of Office 365 test environment
* Testing needs to be done in PROD environment

# System Overview

## Description

This section gives the overall overview of the system architecture that this project is using to deploy the Identity Management solution in EmblemHealth.

## System Architecture

For Phase-1 implementation, Identity manager solution foundation will be established and integrated with a set of IT systems listed below by following the integration standards,

### TO-BE



**Note: The connection between IDM and Exchange will be removed once all mailboxes are migrated**

### AS-IS



# Current State vs Future State – Requirements

## User Mailbox

### New Hires

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| Step 1:  Create Identity  **(No Changes)** | Identity is created in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor Creation Screen | Identity is created in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor Creation Screen |
| Step 2:  Create AD Account  **(No Changes)** | AD account is created in On-premise Active Directory | AD account is created in On-premise Active Directory |
| Step 3:  Create Mailbox  (SailPoint)  **(Process Change)** | **Step i: Populate AD attributes**  Additional attributes are populated for in on premise AD for Office 365 mailbox creation   * proxyAddresses * mail * userprincipalname   Please refer to [Email Generation Logic](#_AD_Password_Policy) section for email logic  User is added to **“Vault\_Emblem”** AD group for now. | Provision the following attributes for Exchange from IIQ to create the email account using IIQ AD connector:-   * mailNickname * homeMDB   After provisioning, the following attributes are auto populated   * mail * proxyAddresses   **Note**: For Medicare Users, mailbox will not be created through SailPoint  User is added to **“Vault\_Emblem”** AD group so that mailbox is automatically archieved (Owner : Exchange Team) |
| Step 4;-  Add user to Office 365 AD group | **Add user to Office 365 AD group in on Premise**  **User will added to a Office 365 AD group in on premise. Azure AD will provide access to liceses based on this** |  |
| Step 5  Create Office 365 Account  **(new)**  (Exchange/  Office 365 Team) | **Step2 : Run Powershell Script (No delay required between I and ii – Factor in replication)**  **Enable-RemoteMailbox**   * Exchange team to provide the command   + Parameters to include archieval, remote mailbox,   + Enable-RemoteMailbox "Kim Akers" -RemoteRoutingAddress "kima@contoso.mail.onmicrosoft.com -Archive * A script needs to be developed to run in AD/exchange to call this command for every new ids that is created   **Note:**   * This attribute sets the proxyaddress and mail * We can use UPN for populating this command   **Step ii: DirSync (Automated =- Scheduled 30 mins)**  DIRSync will migrate the accounts in Office 365 after scheduled interval (30 mins)  This step is going to populate the [attributes](#_Attributes_Synchronized_between) from on-premise to Office 365  Azure AD account & Mailbox Created:-   * AD account gets created in Office 365 along with Mailbox. * The mail address will be same as the UPN/Proxyaddress * No License is assigned to the user and its default valid for 30 days * Please refer the [Attributes](#_Attributes_Synchronized_between) ... for the list of attributes synched to Azure AD from On premise AD   **Step (V) – License Assignment & Preservation & Retention policy**  A script needs to be run to take care of the below steps. This will add users part of AD group to the below  This needs to be run on a daily basis:-  **This needs to be run in Azure (Exchange Team) Exchange team to develop these scripts and run them**   * **Assign license through script** (Run in Azure)   Everyone get E3 license (Discussion is going on) – All users will get the same license   * **Preservation Policy and Retention Policy assignment** – (This needs to be run immediately after the mailbox is created for compliance) * **Retention policy archieves the mailbox after 90 days** |  |
| **Email Notifications**  **(SailPoint)** | **Email Scenarios**   * Emails sent to SCCD for ticket creation contain email address of the user. It will take some time for this email address to be visible in GAL **(AS-IS)** * New Hire email to manager (Employee and Vendor) has the email address of the user. It will take some time for this email address to be visible in GAL **(AS-IS)** * Welcome email for Employees: This email needs to be triggered at the end of day . (**Process change in SailPoint)** | **Email Scenarios**   * Emails sent to SCCD for ticket creation contain email address of the user. * New Hire email to manager (Employee and Vendor) has the email address of the user * Welcome email for Employees : get triggered to the user’s email mailbox at the time of email account creation **(Process change)** |

### Termination of Employees

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Update Identity**  **(No Changes)** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor update or Immediate Termination Screen and marked as terminated  **Note: Need to check if the termination through QAR is going to be affected due to this** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor update or Immediate Termination Screen and marked as terminated |
| **Step 2:**  **Terminate AD Account**  **(No changes)** | AD account is updated in On-premise Active Directory   * AD account is disabled * Cn is appended by zz, dn is changed accordingly * Description is updated (Disabled by IDM) * All existing groups are removed * User is added Vault\_Emblem\_Term\_Employees group * **Note**: Keep it as it is till the migration is done, after all mailboxes are migrated to office365, this process is not needed   Account is moved to Term OU | AD account is updated in On-premise Active Directory   * AD account is disabled * Cn is appended by zz, dn is changed accordingly   + V-asengupta becomes zzv-asengupta * Description is updated (Disabled by IDM) * Change the AD password * All existing groups are removed * User is added Vault\_Emblem\_Term\_Employees group * Account is moved to Term OU |
| **Step 3:**  **Disable/Rename Mailbox**  **No Process change** | **Step i: On premise mailbox rename and hide from GAL**  The below changes are done in Mailbox  Mail is appended by xxx by updating proxyaddress and mail attribute.   * [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [xxxjdoe@emblemhealth.com](mailto:xxxjdoe@emblemhealth.com)   Mail is hidden from GAL   * msexchangeHideFromAddressLists is set to true   UPN is unchanged  (Arjun to check the command to do this) | The below changes are done in Mailbox  Mail is appended by xxx by updating proxyaddress and mail attribute.   * [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [xxxjdoe@emblemhealth.com](mailto:xxxjdoe@emblemhealth.com)   Mail is hidden from GAL   * msexchangeHideFromAddressLists is set to true   UPN is unchanged |
| **Step 4:-**  **Terminate office /Remove License**  **Account (Office 365/Exchange Team)**  **(new )** | **Step ii: DirSync**  DirSync will Sync the accounts in Office 365 after scheduled interval  **Step iii: Azure AD updates**   * AD account profile gets updated in Office 365. * Email address should be updated in Office 365 * Email account should be hidden from GAL * License removal should be managed by Exchange Team.   **Action Item:- (Only license removal)**   1. Messaging team to remove licenses based on script or manual process – Messaging team (IF AD account is disabled, user is in termed ou and license is assigned). 2. Send a report back of failed ones |  |
| **Step 5:**  **Create Termination Work order (SailPoint)** | Email notification is sent to SCCD to generate termination work order | Email notification is sent to SCCD to generate termination work order |

### Termination of Cognizant Associates and Vendors

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Update Identity** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor update or Immediate Termination Screen and marked as terminated  **Note: Need to check if the termination through QAR is going to be affected due to this** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Vendor update or Immediate Termination Screen and marked as terminated |
| **Step 2:**  **Terminate AD Account**  **Day 0** | AD account is updated in On-premise Active Directory   * AD account is disabled * Description is updated (Disabled by IDM) * Account is moved to Term OU | AD account is updated in On-premise Active Directory   * AD account is disabled * Description is updated (Disabled by IDM) * Change the AD password * Account is moved to Term OU |
| **Step 3**  **Hide Mailbox Mailbox** | **Step i: On premise mailbox hide from GAL**  The below changes are done in Mailbox  Mail is hidden from GAL   * msexchangeHideFromAddressLists is set to true   UPN is unchanged  **Step ii: DirSync**  DirSync will Sync the accounts in Office 365 after scheduled interval  **Step iii: Azure AD updates**   * AD account profile gets updated in Office 365. * Email address should be updated in Office 365 * Email account should be hidden from GAL * License removal should be managed by Exchange Team. | The below changes are done in Mailbox   * msexchangeHideFromAddressLists is set to true   UPN is unchanged |
| **Step 4:**  **Termination Work order** | Email notification is sent to SCCD to generate termination work order | Email notification is sent to SCCD to generate termination work order |
| **Step 5:**  **Terminate AD Account**  **Day 15** | AD account is updated in On-premise Active Directory   * Cn is appended by zz, dn is changed accordingly * All existing groups are removed * User is added Vault\_Emblem\_Term\_Employees group | AD account is updated in On-premise Active Directory   * Cn is appended by zz, dn is changed accordingly * All existing groups are removed * User is added Vault\_Emblem\_Term\_Employees group |
| **Step 6:**  **Rename Mailbox**  **Day 15** | **Step i: On premise mailbox rename**  **The below changes are done in Mailbox**  Mail is appended by xxx by updating proxyaddress and mail attribute.   * [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [xxxjdoe@emblemhealth.com](mailto:xxxjdoe@emblemhealth.com)   Once the AD account is disabled, the Office365 account is disconnected. So this operation will not work.  **Discussion Points (Internal to Exchange Team):-**  Renaming the mailbox – Exchange team to chck with Hon on the existing process **(xxx rename)** and if this needs to be continued going forward | The below changes are done in Mailbox  Mail is appended by xxx by updating proxyaddress and mail attribute.   * [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [xxxjdoe@emblemhealth.com](mailto:xxxjdoe@emblemhealth.com) |
| **Step 7**  **Remove License**  **(office 365/Exchange Team)**  **(new)** | **Step ii: DirSync**  DirSync will Sync the accounts in Office 365 after scheduled interval  **Step iii: Azure AD updates**   * AD account profile gets updated in Office 365. * Email address should account should be renamed * Email account should be hidden from GAL * License removal should be managed by Exchange Team   Note: Some users have multiple email addresses  **Action Item:- (Only license removal)**   1. Messaging team to remove licenses based on script or manual process – Messaging team (IF AD account is disabled, user is in termed ou and license is assigned). 2. Send a report back of failed ones |  |

### Termination of Users due to inactivity

A script runs in QAR that scans all active users who have not logged in for 90 days and terminates the users. The steps followed are same as [Termination of Employees](#_Termination_of_Employees)

**Process Change:-**

**QAR may not support Office 365 Provisioning as we will need to see how to mitigate this**

|  |  |  |
| --- | --- | --- |
| **Action Items** | Need to automate in SailPoint to de- provision the user if they do not login for more than 90 days | Sailpoint Team  **Open item**   1. **Changes in QAR – Sudhir**   **If we need to remove the licenses, we can follow the same process for termination** |

### Rehire/Reactivation

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Update Identity** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Rehire Vendor and marked as Active  **Note: Need to check if the Undo Deprovisioning through QAR is going to be affected due to this** | Identity is updated in SailPoint IIQ from Authoritative source such as PeopleSoft HR/ EHPMO or Rehire Vendor and marked as Active |
| **Step 2:**  **Enable AD Account** | AD account is updated in On-premise Active Directory   * AD account is enabled * If Cn is appended by zz, then remove it * dn is changed according to cn * Description is updated to as per source value * All existing groups are reassigned * User is removed from Vault\_Emblem\_Term\_Employees group * Account is moved to appropriate OU based on placement policy | AD account is updated in On-premise Active Directory   * AD account is enabled * If Cn is appended by zz, then remove it * dn is changed according to cn * Description is updated to as per source value * All existing groups are reassigned * User is removed from Vault\_Emblem\_Term\_Employees group * Account is moved to appropriate OU based on placement policy |
| **Step 3:**  **Enable Mailbox if already present or create a new mailbox if not present** | **Step i: On Premise Mailbox Rename and unhide from GAL**  **If Present**  **(Note: mail is not going to be deleted going forward)**  Check Recipeint Type Details, if it is   * RemoteUserMailBox – the below process will be done on O365 account * UserMailBox – the below process will be done on Exchange account   If Mail is appended by xxx, then remove xxx by updating proxyaddress and mail attribute.   * xxx[jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com)   Mail is unhidden from GAL   * msexchangeHideFromAddressLists is set to false   UPN is unchanged | The below changes are done in Mailbox  **If Present**  If Mail is appended by xxx, then remove xxx by updating proxyaddress and mail attribute.   * xxx[jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com) will become [jdoe@emblemhealth.com](mailto:jdoe@emblemhealth.com)   Mail is unhidden from GAL   * **msexchangeHideFromAddressLists** is set to false   UPN is unchanged |
| **Step 4**  **Office 365 provisioning**  **(Office 365/exchange Team)** | **Step ii: DirSync**  DirSync will Sync the accounts in Office 365 after scheduled interval  **Step iii: Azure Updates**   * AD account profile gets updated in Office 365. * Email address should be updated in Office 365 and account should be hidden from GAL   **Step iv**   * Email address should be updated in Office 365 and account should be hidden from GAL   **Step (V) – License Assignment & Preservation & Retention policy**  **Part 1 – Generate list of impacted users**  List of users on which the script needs to be run needs to identified and sent to exchange team or the script needs to calculate  **Options:-**   * **Query in AD based on timestamp** * **Get a report (Not a good approach as this will cause delay)**   **Part 2 – Run script**  A script needs to be run to take care of the below steps.  This needs to be run on a daily basis:-  **This needs to be run in Azure (Exchange Team) Exchange team to develop these scripts and run them**   * **Assign license through script** (Run in Azure)   Everyone get E3 license (Discussion is going on) – All users will get the same license   * **Preservation Policy and Retention Policy assignment** – (This needs to be run immediately after the mailbox is created for compliance) * Retention policy archieves the mailbox after 90 days |  |
| **Create new Mailbox (new Users if mailbox is not present)** | **Refer onboarding process** |  |
| **Step 4:**  **Create New Hire Work order** | Email notification is sent to SCCD to generate new hire work order | Email notification is sent to SCCD to generate new hire work order |
| **Follow Ups** | Exchange Team and Hon | Same as Termination of Employees to discuss renaming the mail (appending xxx during termination and removing xxx during rehire) is required |

### Rebadging or Employee to Vendor or Vendor to Employee Conversion

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Rebadging**  **Or**  **Employee to vendor or vice versa conversion** | Rebadging is a process that is done when a user becomes from Employee of Vendor or vice versa  In this scenario, the below are done based on naming convention:-  AD Account rename and updates   * Samaccountname is changed based on the new convention * Display name is changed based on the new convention * User is moved to the new OU based on placement policy   Email Address changes/Addition   * New Email address and proxy address is updated based on the new convention and the old email address is added as secondary proxy address.   This information should flow to Office 365  **Mail Copy**  Note: Sometime, if a new account is created, then the mailbox needs to be migrated to the new account  ***The above is done manually by exchange team.*** | Rebadging is a process that is done when a user becomes from Employee of Vendor or vice versa  In this scenario, the below are done based on naming convention:-  AD Account rename and updates   * Samaccountname is changed based on the new convention * Display name is changed based on the new convention * User is moved to the new OU based on placement policy   **Employee**:  Login ID: asengupta  Email id : [asengupta@emblemhealth.com](mailto:asengupta@emblemhealth.com)  **Cognizant/Vendor**  Login ID: v-asengupta  Email id : [a\_sengupta@emblemhealth.com](mailto:a_sengupta@emblemhealth.com)  Adding additional email address to the user’s old mailbox  [**a\_sengupta@emblemhealth.com**](mailto:a_sengupta@emblemhealth.com)  Email Address changes/Addition   * Email address is updated based on the new convention or a new proxyaddress is created for the account   **Mail Copy**  Note: Sometime, if a new account is created, then the mailbox needs to be migrated to the new account  ***The above is done manually by exchange team.*** |
| **Open Items** | Exchange/Office365 Team | **Scenario 1: Adding a new email address**  Follow the same process to create mailbox as in new hire and this gets updated in the next dirSync  **Scenario 2: If we rename the email address**  If we update proxyaddress, then email address gets updated in Office365.  Do we need to update mail or UPN also  We need to check during the POC  We need to change case of SMTP for primary and secondary email addresses  Note: We need to keep mail and primary email address same for notification |
| **Follow Ups** | Exchange Team and Hon | Mail Copy  Note: Sometime, if a new account is created, then the mailbox needs to be migrated to the new account.  Confirm with Hon whether the existing process should remain same. |

### Profile Updates sync from On Premise AD to Azure AD

Profile updates (Any AD [attribute](#_Attributes_Synchronized_between) update) from on premise AD should flow to Azure AD using DirSync

## Distribution Lists

### Create Distribution List

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Create group marked as DL** | AD group is created in On-premise Active Directory | AD group is created in On-premise Active Directory |
| **Step 2:**  **Mail Enable the Group to make it a DL**  **(No Change in Overall process, need to check if things work as expected)** | Mail address for the DL is created in on premise Active Directory  **This is synced with office 365 using DirSync**  The DL is created in Office 365  The email address is added to the group in Office 365 | Mail address for the DL is created in on premise Active Directory  (There is not physical storage created) |

### Edit DL Properties

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Update group marked as DL** | AD group is updated in On-premise Active Directory such as owner, description, group name | AD group is updated in On-premise Active Directory such as owner, description, group name |
| **Step 2:**  **Mail Enable the Group to make it a DL**  **(No Change in Overall process, need to check if things work as expected)** | Mail address can be updated for the DL in On premise AD  This is synced with office 365 using DirSync  The DL is update in Office 365  The email address is updated to the group in Office 365 | Mail address can be updated for the DL in On premise AD |

### Add/remove Members in Group

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Group Membership update (Process Change)** | Modify group membership of users in directly in AD, this should update the group membership in Office 365. | A group owner can directly add or remove members to an owned through outlook |

### Rename DL

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Rename a DL name in AD through QAR or sailPoint** | Group name or email is updated in on premise AD  Note: Confirm during POC | Group name or email is updated in on premise AD |

## Group Mailbox/Shared Mailbox

### Create Group mailbox

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Create Group Mailbox**  **(This will be process change)** | Create an on-premises AD user object for shared mailbox.  **The below attributes need to be populated:-**  Run the New-RemoteMailbox cmdlet in the “Exchange Management Shell" to enable mailbox user.  Connect the O365 Exchange Online power shell and execute the Set-Mailbox <MailboxName> -Type Shared to convert remote mailbox type to Shared mailbox on the Cloud O365.  Assign the Preservation policy and retention policy for the shared mailbox in O365 Exchange Online (Note: License assignment is not require for the shared mailboxes) | Group Mailbox is created in On-premise Active Directory |
| **Open Items/Action Items** | BAU Team / Office 365 Team | Discuss with BAU team for the process change |

### Assign Permissions to Mailbox for users

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Assign Permission (No Changes)** | AD user object is assigned permission in On-premise Active Directory  This is synced with office 365 using DirSync. | AD user object is assigned permission in On-premise Active Directory  This is synced with office 365 using DirSync. |

### Edit Mailbox properties

|  |  |  |
| --- | --- | --- |
| **Step** | **TO-BE** | **AS-IS** |
| **Step 1:**  **Update Mailbox Property (No changes)** | AD user object is updated in On-premise Active Directory  This is synced with office 365 using DirSync. | AD group is updated in On-premise Active Directory |

## Define a way for co-existence of processes during migration activity

To be discussed

## Other Scenarios

### QAR provisioning of mailbox for Non Corp OU

This functionality should remain as-is

### Mail enable a Security group

This flow should be similar to DL email account creation flow

Note: Any other OU apart from the above is out-of-scope

# System Design – IIQ

## AD Application

### Schema Attribute

An attribute “proxyAddresses” should be added in the Account Schema. This is primarily used to set the email address to provision in O365.

### Provisioning Policy

The AD attributes, “homeMDB” and “mailNickname” should not set in Provisioning Policy to stop provisioning accounts in exchange.

The AD attributes, “mail”, “proxyAddresses” and “userPrincipalName” should set in Provisioning Policy to provision accounts in O365.

The uniqueness of mail attribute should be done using “proxyAddresses” attribute.

## Workflows

### New Hire

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Workflow Name** | **Applicable for** | **Description** |
| UC001 | EH\_Lifecycle\_Event\_Joiner\_Hybrid\_Design | All types of users | The purpose of this workflow is to assign EH Business roles to the users created in IDM, depending on the user type and provision the users in Active Directory, Office 365 and home drives for new joiners |

**Overview:**

The below changes are required:-

* + - 1. Restrict new hire welcome email to new Employees
      2. Restrict email creation for Medicare Users

### Termination

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Workflow Name** | **Applicable for** | **Description** |
| UC002 | EH\_Workflow\_Leaver\_Deprovision | All types of users | The purpose of this workflow is to disable the user in IDM and AD based on feed for EH and Cognizant associates and UI for vendors; also move the user in the corresponding AD OU (Termed) |
| UC002 | EH\_Workflow\_Leaver\_DeprovisionVendor | Cognizant Associate and Vendor | The purpose of this workflow is to remove the groups and rename the mail and display name in AD which is trigger after the 15th day of termination. |

**Overview:**

The below changes are required:-

* + - 1. Verify the commands that are being used for renaming the exchange users.
      2. Do not run any exchange commands any more
      3. Update mail and primary proxyAddress attribute by prefixing “xxx”.

### Rehire

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Workflow Name** | **Applicable for** | **Description** |
| UC003 | Lifecycle\_Event\_Rehire | All types of users | The purpose of this workflow is to re-enable the user in IDM and AD based on feed for EH and Cognizant associates and UI for vendors; also move the user in the corresponding AD OU. |

**Overview:**

The below changes are required:-

* + - 1. Verify the commands that are being used for renaming the exchange users.
      2. Do not run any exchange commands any more
      3. Remove “xxx” in mail and primary proxyAddress attributes
      4. Do not send new hire welcome email for Employees

### AD Group Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Workflow Name** | **Applicable for** | **Description** |
| UC004 | EH\_GroupManagement\_CreateGroup\_Workflow | AD Groups | The purpose of this workflow is to create a Security/Distribution group in IDM, as well as in AD |

**Overview:**

The below changes are required:-

* + - 1. Set mail attribute during provisoning
      2. Remove mailNickname attribute during ptovisoning

## Rules

### Rules

|  |  |  |
| --- | --- | --- |
| **Rule Name** | **Description** | **Logic** |
| EH\_Daily\_Welcome\_Mailer | This rule is used to send Welcome email to the Employees during new hire and rehire on the day. | 1. The rule is triggered using a task called “EH-DailyWelcomeMailerTask”. 2. The rule captures the new hire, rehire users from Audit events, which is captured during the execution of new hire, and rehire process. 3. The rule process each identity and send the welcome email. |
| EH\_FieldValue\_AD\_CreateProxyAddress | This rule is used to set proxy address during new hire | This rule uses the email generation logic to set primary proxy address for the user. Refer [Section 9.1.3](#_AD_Password_Policy) |
| EH\_FieldValue\_AD\_CreateHomeMDb | This rule is used to set HomeMDB if the user has to provision in exchange during new hire. | This rule set the homeMDB value from the custom object |
| EH\_FieldValue\_AD\_CreateMailNickName | This rule is used to set mailNickName if the user has to provision in exchange during new hire. | This rule generates unique mailNickName based on the email generation logic |
| EH\_FieldValue\_AD\_CreateMail | This rule is used to set mail during new hire. | This rule uses the email generation logic to set primary proxy address for the user. Refer [Section 9.1.3](#_AD_Password_Policy) |
| EH\_Enable\_Remote\_Mail\_Powershell | This powershell command is used to enable remote mailbox in office 365 after creating the account | This rule use the enable remote mailbox power shell command to create user in Office365 |

### Rule Library

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SL NO** | **Rule Name** | **Type** | **Method Name** | **Arguments** | **Return Type** | **Description** | **Logic** |
| 1 | EH\_Rule\_Library | Rule | getMail | Identity identity | String | This method is used to generate the mail based on the First Name and Last name of the user and check the uniqueness of mail attribute in AD | The mail is generated based on the logic in the [Appendix 9.1.3](#_AD_Password_Policy) |
| 2 | EH\_Rule\_Library\_2 | Rule | isOffice365 | Identity identity | Boolean | This method is used to check whether the user mailbox should be created in Ofiice365 and exchange | This rule returns true if user should provision in Office365. |

## Custom

|  |  |  |
| --- | --- | --- |
| **S No** | **Custom Object Name** | **Description** |
| 1 | EH\_AD\_Custom\_Objects | This custom object is used to set the Office365 AD group during new hire and rehire process. |

## Tasks

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case ID** | **Task Name** | **Description** | **Logic** |
| UC005 | EH-DailyWelcomeMailerTask | This task is used to send Welcome email to the Employees during new hire and rehire on the day. | * The task triggers a rule called “EH\_Daily\_Welcome\_Mailer”. * The rule captures the new hire and rehire users from Audit events, which is captured during the execution of new hire, and rehire process of the respective identity. * The rule process each identity and send the welcome email. |

## Reports

|  |  |  |
| --- | --- | --- |
| **Use Case ID** | **Report Name** | **Description** |
| UC001 | Weekly onboarding and offboarding report for Employee/vendor and Cognizant Associates | Add the messaging team DL in the weekly and monthly reports |

## Email Templates

The below email templates contain email address of the user. They will keep on using the existing logic:-

|  |  |  |
| --- | --- | --- |
| **SL** | **Scenario** | **Description** |
| 1 | New Hire/Rehire email for Employees |  |
| 2 | New Hire email for vendors |  |
| 3 | SCCD new Hire emails |  |
| 4 | Termintion Workorders |  |

# System Design – Exchange/Office 365

## Placholder for Exchange and Office365 team

# Testing Approach

Office 365 testing should done in UAT environment by pointing the existing AD application connector to PROD AD environment. User account should create in the Test OU.

The following lifecycle events should tested:

* + - 1. New Hire
* Execute Peoplesoft HR/EHPMO aggregation
* IDM process the user record from the feed file (Peoplesoft HR/EHPMO) for new hire process
* Create user in IDM
* Create AD Account in PROD Test OU
  + - 1. Termination
* Execute Peoplesoft HR/EHPMO aggregation
* IDM process the user record from the feed file (Peoplesoft HR/EHPMO) for termination process
* Disable user in IDM
* Disable AD Account in PROD Test OU
* Update the mail and proxyAddresses attribute values by prefixing “xxx”.
  + - 1. Rehire
* Execute Peoplesoft HR/EHPMO aggregation
* IDM process the user record from the feed file (Peoplesoft HR/EHPMO) for termination process
* Enable user in IDM
* Enable AD Account in PROD Test OU
* Remove “xxx” in mail and primary proxyAddress attributes

Employee/Cognizant Associate lifecycle events should tested through PeopleSoft HR/EHPMO feed file. Vendor Lifecycle events should be tested through Forms in IDM.

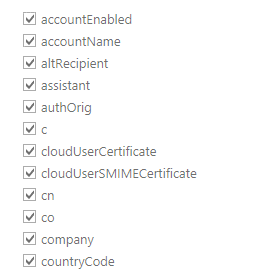
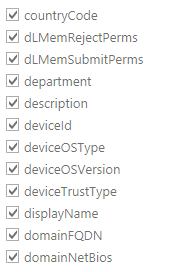
NOTE: No other task should executed during Office365 testing in UAT environment.

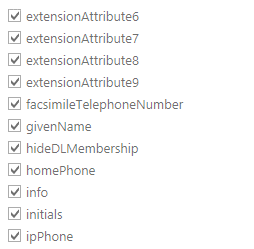
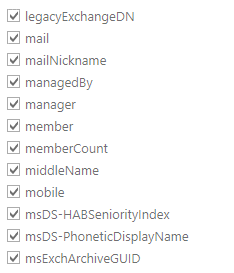
# Attributes and OU

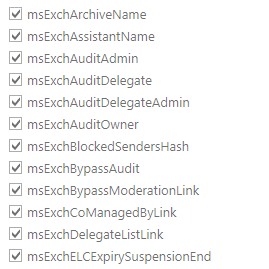
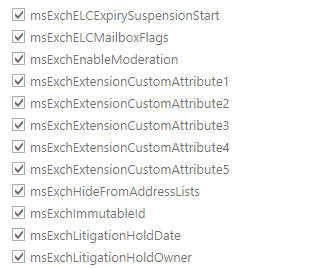
## OU Synchronized

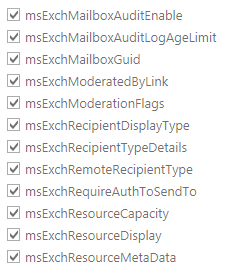
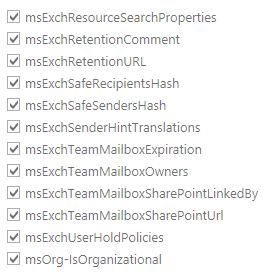
|  |  |
| --- | --- |
| CORP |  |
|  | Contacts |
|  | Contractors |
|  | Disabled |
|  | Employees |
|  | Groups |
|  | Kiosk Accounts |
|  | mailBoxes |
|  | O365 ( Under Service) |
|  | Training |
|  |  |
| HIPA |  |
|  | Contacts |
|  | Contractors |
|  | Disabled |
|  | Employees |
|  | Groups |
|  | mailboxes |
|  |  |
| Test |  |

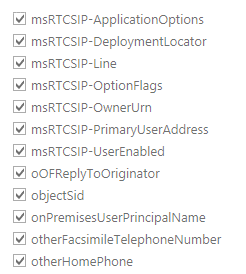
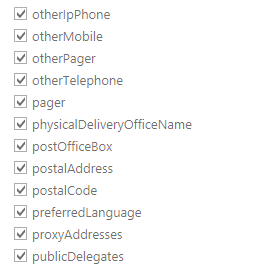
## Attributes Synchronized between On Premise AD and Office 365

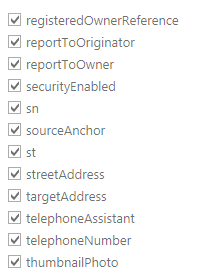
 



# Appendix A - Naming Conventions / Business Logics

### AD Network id Naming convention

**General Considerations**

* Remove any special characters from firstname and lastname
* Length – As per AD standard

**Logic:**

**Employee**: <First letter of first name><Last Name>

**Vendor**: V<-><First letter of first name><Last Name>

**Logic for Duplication:**

The below algorithm will be followed to generate and assign the networkID to the users:

**Step 1:** START

**Step 2:** Initialize flag = 0

**Step 3:** flag = flag + 1

**Step 4:** networkID = <flag number of letters of fist name> + <last name>

**Step 5:** Check in IDM, if the generated ‘networkID’ is already present in IDM or not

**Step 6:** If yes, go to **Step 3,** Else go to **Step 7**

**Step 7:** Assign the generated networkID to the user in IDM

**Step 8:** END

### AD – CN Naming convention

cn will be same as network id (samAccountName) of the user as per the new process

### Email Address Naming convention

**General Consideration**

* Remove any special characters from firstname and lastname
* On Termination - Append <xxx> in email

**Suffix :**

CORP users - @emblemhealth.com

**Name portion**

The below algorithm will be followed to generate and assign the Email Address to the users:

**Step 1:** START

**Step 2:** Initialize flag = 0

**Step 3:** flag = flag + 1

**Step 4:** emailAddress = <flag number of letters of fist name> + <last name> + <suffix>

**Step 5:** Check in AD, if the generated ‘emailAddress’ is already assigned to any user present in AD or not

**Step 6:** If yes, go to **Step 3,** else go to **Step 7**

**Step 7:** Assign the generated ‘emailAddress’ to the user

**Step 8:** END

**Note:** Logic for UPN is same as mail

Active Directory ExternsionAttribute12 logic:-

|  |  |  |  |
| --- | --- | --- | --- |
| **User Type** | **ExtensionAttribute12** | **Email Logic** | **Notes** |
| Corp/HIPA Employees | NA, This Policy applied to all the recipients in Exchange and will not refer the Attribute12. | [UserAlias@emblemhealth.com](mailto:UserAlias@ehmedicare.com) | In scope of IDM |
| Corp Contractors | CORP-Contractors | [UserAlias@emblemhealth.com](mailto:UserAlias@ehmedicare.com) | In scope of IDM |
| Cognizant Associates | CORP-Contractors | [UserAlias@emblemhealth.com](mailto:UserAlias@emblemhealth.com) | In scope of IDM |
| Medicare Employees | MEDICARE-Employees | [UserAlias@ehmedicare.com](mailto:UserAlias@ehmedicare.com) | Creation of Email ID is not in scope of IDM. |
| Medicare Vendors | MEDICARE-Contractors | [UserAlias@ehmedicare.com](mailto:UserAlias@ehmedicare.com) | Out of scope of IDM |
| ConnectiCare Employees | CCI-Employees | [UserAlias@connecticare.com](mailto:UserAlias@connecticare.com) | Out of scope of IDM |
| ConnectoCare HEP Employees | NA, This policy applied to users with company attribute value is equal to"HEP" | [UserAlias@connecticare.com](mailto:UserAlias@connecticare.com) | Out of scope of IDM |
| ConnectiCare Vendors | CCI-Contractors | [UserAlias@connecticare.com](mailto:UserAlias@connecticare.com) | Out of scope of IDM |

### Active Directory Placement Policy

Below are the placement rules in Active Directory:-

|  |  |  |  |
| --- | --- | --- | --- |
| **User Type** | **OU** | **Condition** | **Remarks** |
| CORP Employees | OU=<City>,OU=Employees,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM  <City> can be Albany/LakeKatrine/Melville/NYC/Syracuse | * Feed is PeopleSoft HR * User is active | In scope |
| OU=LOA,OU=Disabled,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User goes on leave | In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User is terminated | In scope |
| CORP Contractors | OU=ACP,OU=Contractors,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active * Vendor Name is ACP | In scope |
| OU=CognizantTemporary,OU=Contractors,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active * Feed is EHPMO * BGV is In-progress | In scope |
| OU=Cognizant,OU=Contractors,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active * Feed is EHPMO * BGV is Completed | In scope |
| OU=Contractors,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active * Vendor Name is neither ACP nor Cognizant | In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is terminated | In scope |
| CORP Admins | OU=Admin,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User/Contractor has an admin account and the In scope account is active | In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=CORP,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User/Contractor has an admin account and the account is in active | In scope |
| HIPA Employees | OU=Employees,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User is active | No Changes for existing users. Refer Corp for new users.  Existing users to move to HIPA ou on transfers, rehire.  In scope |
| OU=LOA,OU=Disabled,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User goes on leave | In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User is terminated | In scope |
| HIPA Contractors | OU=Contractors,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active | No Changes for existing contractors. Refer Corp for new contractors.  Existing contractors to move to HPA ou on transfers, rehire  In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is terminated | In scope |
| HIPA Admins | OU=Admin,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User has an admin account and the account is active | In scope |
| OU=Termed,OU=Disabled,OU=Accounts,OU=HIPA,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User/Contractor has an admin account and the account is in active | In scope |
| Medicare Employees | OU=<Location>,OU=Employees,OU=Accounts,OU=Medicare,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM  City> will be Florida/NYC/Syracuse | * Feed is PeopleSoft HR * User is active | In scope |
| OU=LOA,OU=Disabled,OU=Accounts,OU=Medicare,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Feed is PeopleSoft HR * User goes on leave | In scope |
| OU=Disabled,OU=Accounts,OU=Medicare,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User is terminated | In scope |
| Medicare Contractors | OU=Contractrors,OU=Accounts,OU=MEDICARE,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is active | Out of scope |
| OU=Calabrio,OU=Contractrors,OU=Accounts,OU=MEDICARE,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM |  | Out of scope |
| OU=Disabled,OU=Accounts,OU=Medicare,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * Contractor is terminated | In scope |
| Medicare Admins | OU=Admin,OU=Accounts,OU=MEDICARE,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User/Contractor has an admin account and the account is active | In scope |
| OU=Disabled,OU=Accounts,OU=Medicare,DC=EMBLEM,DC=EMBLEMHEALTH,DC=COM | * User/Contractor has an admin account and the account is in active | In scope |

# Open Items

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S No.** | **Question** | **Concerned Team** | **Priority** | **Open Date** | **Action Items** | **Comments, if any** | **Remarks** |
| 1 |  |  |  |  |  |  |  |