Dynamic On-Premise Active Directory Group Management Requirements

## Overview

1. Create a csv file with the following columns

RuleName;GroupDn;Expression;AccountExpirationDate;

1. The dynamic expression for a group. For example:

'($\_.costCenter -eq "634" -and $\_.jobCode -like "\*US1\*")'

1. Based on the expression, users will be added to or removed from a group.

**Note :- AccountExpirationDate will be evaluated to verify it can be used**

## CSV Attribute Mappings

| **CSV Attributes** | **AD attributes** |
| --- | --- |
| GroupDn | groupDn |
| AccountExpirationDate | accountExpirationDate |

## Expression - AD Attribute Mappings

| **Expression** | **AD Attribute** |
| --- | --- |
| AccountEnabled | enabled |
| jobCode | extensionAttribute2 |
| CostCenter | extensionAttribute4 |
| EmployeeType | employeeType |
| OfficeLocation | physicalDeliveryOfficeName |
| JobTitle | title |
| buildingPrimaryState | state |
| legalEntityCode | extensionAttribute5 |

## Limitations:

1. Can we manually add or remove users from dynamic groups? Or can we have an exclusion list to manually manage specific users.
2. The rule being evaluated should be inverted to calculate users to be removed from the group.

## Prerequisites

Create a local AD with the following structure:

**Top Level**

DC = Com

DC = Local (This can be any name)

**Groups**

OU = CORPUSERS

OU = GROUPS

OU = IAM

CN = GroupName (this can be any name)

CN = GroupName2

CN = GroupName3

**Users**

OU = CORPUSERS

OU = Employees

OU = Contractors&Consultants

### 

### 