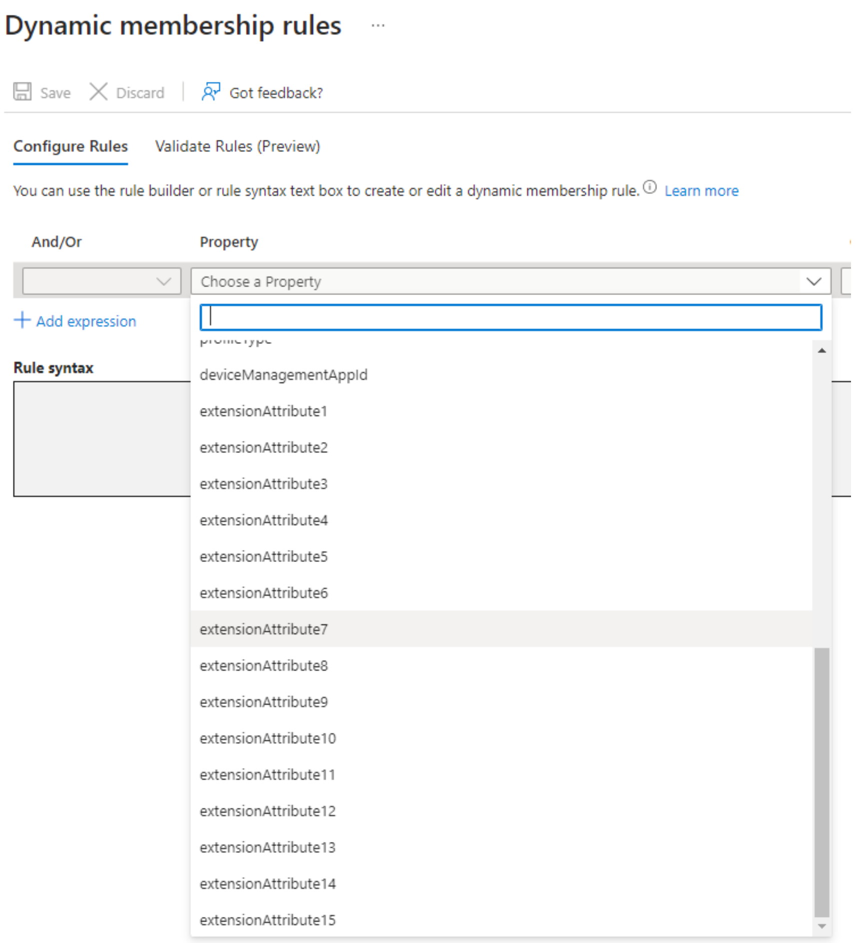
Create a Device Assigned Cloud-based security group from “*lastSyncedDate*” attribute.

If you know how to manage cloud-based sec. groups in Azure AD (AAD) you’re aware of some limitation around attributes/properties available to be used by dynamic rules



You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

If device is managed, we should know ***LastSyncDateTime*** from those devices.

Then I checked one of my posts from the other day

```
Install-Module Microsoft.Graph -Scope AllUsers
Connect-MSGraph
$Devices = Get-IntuneManagedDevice -Filter "contains(operatingsystem, 'Windows')" |
Get-MSGraphAllPages
foreach ($item in $Devices.devicename) { Get-IntuneManagedDevice -Filter
"contains(deviceName,'$($item)')" | Invoke-IntuneManagedDeviceSyncDevice }
```

Then I tweaked the code

```
#Connect to MSGraph and List all Windows Devices
Install-Module Microsoft.Graph -Scope AllUsers
Connect-MSGraph
$Devices = Get-IntuneManagedDevice -Filter "contains(operatingsystem, 'Windows')" | Get-MSGraphAllPages

#Define the amount of days to exclude from the search

$limit = (Get-Date).AddDays(-30) #older than 30 days
$olderthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -lt $limit} | select devicename,lastsyncdatetime #older than 30 days
#$olderthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -lt $limit} #all devices info
#$olderthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -lt $limit} | export-csv -NoTypeInformation -Encoding all-devices-older-than-limit.csv #all devices info to csv

#Badr eddine Zaki asked for only devices active in the last 30 days

$newwerthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -gt $limit} | select devicename,lastsyncdatetime #only devicename and lastsyncdatetime
#$newwerthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -gt $limit}  #all devices info
#$newwerthanlimit = $Devices | Where-Object {$_.lastsyncdatetime -gt $limit} | export-csv -NoTypeInformation -Encoding all-devices-greater-than-limit.csv

#add devices by name, object it to AAD sec. group
```

Right after I managed to have the main goal achieved, I realized some environments have the amazing Hybrid Azure AD joined devices in there, where all nightmares and headaches lie.

Main issues found.

- MsGraph Get-IntuneManagedDevice does not retrieve Azure AD ObjectID
    - Required to add devices to a cloud-based sec. group in AAD
- Then after I was able to retrieve all devices using MsGraph and extracted the device Name
- I used this device name to search for it in AAD (Azure AD), moment I got the duplicated device name, even retrieving **isManaged** and **isCompliant** I realized that I did miss the

Then I finally got what I wanted to accomplish working

Download the Script at my GitHub repository.

Thanks,

Thiago Beier
Toronto, ON