Contents

Disclaimer

Objective of the script

This PowerShell scripts aims to collect Azure Active Directory user information and to synchronize these data with a SharePoint list. The SharePoint list is used as a source for our Active Directory Web Part. The SharePoint list structure is created from the web part in the management console.

The script should be executed once a day (scheduled as batch job) so that the changes in your Azure AD data are synchronized with the SharePoint list.

This script **SyncAAD.ps1** is provided for free (and 'as is') to the users of our Active Directory Web Part.

Script to store the encrypted password

Use the script file **CreateEncryptedPW.ps1** to securely store the password of the account that will perform the Azure Active Directory synchronization (encrypted password).

The script will create a file called "**AADS.txt**" which will contain the encrypted password. You will be prompted to provide a destination folder, the SharePoint login account and the associated password.

Script SyncAAD.ps1 parameters

All the parameters are located at the beginning of the script file, in the section #Config Variables.

$LimitUsers	Amount of users to import. Set to -1 for no limit.
$Username	SharePoint username allowed to access the SharePoint list (read/write/delete items)
$SecurePwPath	Path to the SharePoint encrypted password file to be used by the script (encrypted data)
$SiteURL	SharePoint site URL where the SharePoint list is maintained
$ListName	Name of the SharePoint list to be synchronized with the Azure Active Directory data
$ExcelFileName	Excel file name to generate (leave empty if no excel file is required)
$ExcelFolderPath	Path for the Excel file name to be generated (if any)
$FilterOnlyAccountEnabled	Set to true if you wish to synchronize enabled accounts only
$FilterExcludeGuest	Set to true if you don't want to synchronize guest accounts
$RemoveNotFoundADUsersFromSP	Set to true if you wish that script removes accounts that were not listed in your Active Directory (set to false if you wish to add and manual entries from the SharePoint list)
$FilterPhoneRequired	Set to true to only synchronize users having a phone number defined

Implementation Steps

1) Deploy the web part and create the SharePoint list with it, via the management console (name the list as you want).
2) On the machine from which you will run the script to feed your SharePoint list:
    a. Make sure to have at least PowerShell 5.1
    b. Create a folder where the script will be stored and executed
    c. Run the following commands to install required modules:

```
Install-Module SharePointPnPPowerShellOnline
Install-Module AzureAD -Force
```

    d. Login your windows session with the account that will run the scheduled script, and run the script "CreateEncryptedPW.ps1" When prompted, provide the path where the scripts are stored. Then provide the Office 365 account username and password that will be used to connect to the SharePoint list. An encrypted file called AADS.txt will be generated. This file will contain the encrypted password (you'll need to specify the username in the script parameters).
    e. Edit the script SyncAAD.ps1 and adjust the parameters. if Excel isn't installed on this machine then leave `$ExcelFileName =""`. Note that you need to **un-comment** the parameter $SiteURL and provide the correct SharePoint site URL where the SharePoint list has been created.
    f. Run the script SyncAAD.ps1 and verify if you list is filled-in.
    g. Schedule the script with the Windows tasks scheduler. Example of command:

```
Powershell.exe -file "C:\admin\ADUsersSynch\SyncAAD.ps1" -ExecutionPolicy ByPass
```

Note

It can be handy to disable the user account password expiry for the account running synchronization in batch. This can be done with the PowerShell command (replace the user address email accordingly):

```
Set-MsolUser -UserPrincipalName user@contoso.com -PasswordNeverExpires $true
```