Domain User & Group Automator manual (DUGAM)

This is a powershell tool that is used to create AD user and mass adjust group membership on AD, Entra and exchanged by copying from an existing user.

Tool Functions

The two primary function you can select from. It will then follow the prompts for each respective function:

Create a New AD/Entra User Account:

- **Use Case:**

  Ideal for creating new AD user that will be synced up to Entra. It will create a password from the password.dict file and random amount of numbers, and special characters to reach the minimum length. If desired it will copy all AD and Entra groups via a schedule task from an existing user.

- **Prompts:**

  Will prompt for the following: First Name*, SurName*, Title, Department, Employee ID, Manager, Office Location, and Phone Extension. Fields with * are required. The Manager Prompt will ask for name, it will then search AD to find an user that matches. The Office locations will prompt you to select form the list built in config file. If one of the office location info is blank(City, Office name, State, postalCode) it will then prompt the user for it. If there is an typo or the OU in config file is not found it will error out and exit. Once the user is created it will prompt if you want to copy groups from an existing users.

- **Group Copying:**

  It will prompt if you want to copy group memberships from an existing user. if selected to copy, it will copy all group memberships from another user in AD, Entra, and Exchange. The user running the tool must have permission to adjust membership on the groups. Entra and Exchange groups are copied via a scheduled task to ensure the new account fully syncs.

- **Notification:**

  Once the setup is complete, the tool will notify the user's manager and blind carbon copy the IT team with the account details and password. This can be turn off via the config file setting, sendManagerEmail.

2. Mass Group Membership:

- **Use Case:** This tool is ideal for when a user switches departments, sites, or different positions and they no longer need to access items from their previous position. It will remove all existing groups and copy new group membership over from an existing user for AD, Exchange, and entra.

- **Prompts:** Will prompt for the Target User, Source User. It will search for those users in AD and have you select from the found result. It will prompt if you want to adjust AD or Entra, both can be selected on a single run of the tool. it will also prompt if you want to remove existing groups before coping over new groups.

- **Remove Existing Memberships:** Clears all current group memberships for AD or/and Entra depending on user selection.
- **Copy New Memberships:** Copies group memberships from another user for AD or/and Entra. User running the tool must have permission to adjust group membership.

Tool setup

1. It is recommended to user powershell 7 when running this tool. In testing I have found the Powershell module Graph runs smoother and errors out less on version 7 rather than version 5. The module needed are:
    - Microsoft.Graph
        - `Install-Module Microsoft.Graph -Scope AllUsers`
    - ExchangeOnlineManagement
        - `Install-Module -Name ExchangeOnlineManagement -Scope AllUsers`
    - PSFrameworks
        - `Install-Module PSFramework -Scope AllUsers`

    Currently you must install the modules manually. It is recommend to install for All Users.
2. One the modules are installed you will need to edit the `config.json` file to include your setting requirements. Detail information can be found in the 'Config File' section.
3. After `config.json` is has the field configured. Create a shortcut point to `"C:\Program Files\PowerShell\7\pwsh.exe" "C:\PATH\DUGAM\CustomNew-ADUser.ps1"` this will call the main tool menu.
4. Run though some tests (1. Create new user, group membership removal and copy on existing user, etc.) to verify `config.json` fields are correct.

Specific Function Information

Prompts

- **Office**:

  When creating a new user it will prompt for the office location. This prompt is built with option from the config file. `config.sitecode` array will be the choices. The site code will link to the `config.site.[SiteCode.code]` and use those fields when creating the AD user.

- **Company**

  This prompt will only show if you have multiple Company names listed under `config.settings.company`. If there is only one it will use that by default without a prompt. Having Multiple Company names is helpful when creating dynamic distribution list for example. You want a Distribution list that has all accounts that are in a region, Contoso NA, Contoso EU, etc.

User lookup

The user lookup function will search AD under the `config.settings.searchou` for matching Name, or SamAccountName. If no user is found with the name provide it will give an error. Certain lookup are mandatory(e.g. SourceUser for group copying) and will continue to prompt until an user is selected. If the user lookup is not mandatory it will let you exit the search by typing in `Exit`

Graph/Exchange Authentication

Authentication for Entra and Exchange is provided via entra app authentication using certificate. This is used by the schedule task so no login credentials need to be stored. The certificate need to be setup per computer that the script is running from. It is recommend to run on an server with Active Directory Remote Administration Server Tools(RAST) install for this reason.

⚠IT IS NOT RECOMMENDED TO RUN ON A DOMAIN CONTROLLER⚠

Logging

The script will generate a log file for each day(yyyy-mm-dd) & username running the script(e.g. `1600-01-31-JoeSmith.log`). The logs can be found under the `\Logs` folder.

Files

Within the tool folder you will find the following folder structure. The tools makes calls to other file via relative path. Some Specific file that will need editing.

- `config.json` house all the setting and configuration needed before running the tool. View the config section of the manual for additional information regarding the fields.
- `password.dic` contains the words used when creating the password. Each line is considered a word. It will pull two words.
- `MailTemplateUserCreated.html` This is the email body that will be sent to the manager/IT team with the user login information. you can view it in any browser. The image that is displayed in the email needs to be setup as an attachment under `config.smtp.attachments` with matching file name (e.g. logo.png). This should let the email load without having the need to allow it by the user. The file name can be found on line 305 `<img src="cid:logo.png"/>`

  if you do not want the email to have an image at top remove or comment out the following command block.

```
<!-- COMPANY LOGO-->
<table>
    <tr>
        <td class="logo" align="center" style="padding-bottom:10px;">
            <img src="cid:logo.png"/>
        </td>
    </tr>
</table>
```

```
DUGAM
├── ManualFiles
│   ├── Manual.md
│   └── Manual.pdf
├── Logs
│   └── 1600-01-31-JoeSmith.log
├── Resources
│   ├── config.json
│   ├── EntraUser.csv
│   ├── MailTemplateUserCreated.html
│   └── password.dict
├── CustomNew-ADUser.ps1
├── NDU-Functions.psm1
└── ScheduleEntraGroupCopy.ps1
```

Config File

This configuration file is in JSON format and is used to configure the tool. Below is a breakdown of the key sections and their meanings:

1. **SMTP Configuration**

The **SMTP** section provides settings related to email notifications and sending messages.

- `address`: Specifies the SMTP server domain to be used for sending emails (e.g., `smtp.domain.com`).
- `from`: Defines the "From" address and display name for outgoing emails (e.g., `Email Name <from@domain.com>`).
- `subject`: The subject line of the email. It includes a placeholder (`{{user.fullname}}`) that will dynamically insert the user's full name when the email is sent.
- `attachment`: The path to a file that will be attached to the email, e.g., a `.png` image located at `C:\Path\jpeg.png`.
- in progress ~~`ErrorTo`: Specifies the email address where errors will be sent~~.
- `ITEmail`: Defines an IT team's email address to be included in the BCC (blind carbon copy) field for emails containing user credentials.
- `sendManagerEmail`: Boolean field(`TRUE` or `FALSE`) indicating whether an email should be sent to the user's manager with account details once finished. It false is selected it will only sent to the `ITEmail`.

2. **Settings Configuration**

This section contains general settings related to the domain, email templates, and authentication.

- `mailTemplateManager`: Specifies the HTML template for the email sent to the manager after a user is created. The file is located in the application's directory `/Resources` (e.g., `MailTemplateUserCreated.html`).
- `mailTemplateServiceDesk`: Defines the HTML template for email notifications sent to the service desk (e.g., `MailTemplateServiceDesk.html`).
- `domain`: The name of the Active Directory domain (e.g., `contoso.local`).
- `maildomain`: The domain used for email addresses (e.g., `domain.com`).

- `Company`: Specifies the company name (e.g., `Contoso`).
- `SearchOU`: Defines the Organizational Unit (OU) in Active Directory to search for users. (e.g.`OU=Users,DC=Contoso,DC=com`)

Authentication Information:

- `Auth`: Authentication details for accessing services like Entra (Microsoft Entra, formerly Azure AD) via a deploy Application with cert authentication. ~~Setup Entra App Authentication~~
  - `tenant_id`: The ID of the Entra (Azure AD) tenant.
  - `certThumbprint`: The certificate thumbprint used for authentication.
  - `client_id`: The client ID of the application in Entra.
  - `Organization`: The name of the Entra organization.

3. **Site Codes and Locations**

The `SiteCode` and `site` sections define site-specific configurations for different locations, including city, office, and organizational unit (OU) in Active Directory.

- `SiteCode`: An array of site definitions, where each site has a code and name:
  - `Code`: A unique code for the site (e.g., `BER01`, `NYC`).
  - `Name`: The name of the site (e.g., `City Centre Alexanderplatz`, `New York City`).
- `site`: Defines detailed settings for each site based on its code. Each field is representative of the AD field. (e.g. `City` will display in AD City field):
  - For site `BER01`:
    - `City`: The city where the office is located (e.g., `Berlin`).
    - `office`: An name for the office. If there are multiple office in Berlin location this is a way to distinguish them. (e.g., `City Centre Alexanderplatz, East Side Galley`).
    - `OU`: The Organizational Unit in Active Directory where user accounts for this site will be stored (e.g., `OU=Users,OU=Site01,DC=Contoso,DC=com`).
    - `state`: The state\provence of the office location (e.g., `Minnesota`).
    - `PostalCode`: The postal code of the office location (e.g., `10001`).
  - For Additional sites add `,` after the closing `}` and follow the required formatting.

```
"BER01": {
  "City": "Berlin",
  "office": "City Centre Alexanderplatz",
  "OU": "OU=Users,OU=Berlin,DC=Contoso,DC=com",
  "state": "Brandenburg",
  "PostalCode": "10178"
    }
```

Summary of Key Components:

1. **SMTP Configuration**: Used to send emails with user account details, attachments, and notifications to managers and IT teams.

2. **Settings**: Contains email templates, domain, company information, and Entra authentication settings for interacting with cloud services.
3. **Site Configuration**: Specifies different office locations (sites), including details like city, office code, organizational units in Active Directory, state, and postal code.

Full Config file example:

```
{
    "SMTP": {
      "address": "smtp.domain.com",
      "from": "Email Name <from@domain.com>",
      "subject": "User Account details for {{user.fullname}}",
      "attachment": "C:\Path\jpeg.png",
      "ErrorTo": "error email address. [[IN PROGRESS]]",
      "ITEmail": "IT team email to be BCC for user creds",
      "sendManagerEmail": "TRUE\FALSE"
    },
    "Settings": {
      "mailTemplateManager": "MailTemplateUserCreated.html",
      "mailTemplateServiceDesk": "MailTemplateServiceDesk.html",
      "domain": "AD Domain",
      "maildomain": "Email Domain",
        "Company": "Contoso",
      "SearchOU": "DC=Contoso,DC=com",
      "Auth":{
        "tenant_id": "Entra App Tennant ID",
        "certThumbprint": "Entra App Cert thumbprint",
        "client_id": "App Client ID",
        "Organization": "Entra Domain name"
      }

    },
    "SiteCode":
        [
          {
            "Code": "BER01",
            "Name": "City Centre Alexanderplatz"
          },
          {
            "Code": "02",
            "Name": "Site02"
          }

        ]
      ,
    "site": {
      "BER01": {
        "City": "Berlin",
        "office": "City Centre Alexanderplatz",
        "OU": "OU=Users,OU=Berlin,DC=Contoso,DC=com",
        "state": "Brandenburg",
        "PostalCode": "10178"
```

```
    },
    "02": {
      "City": "Indianapolis",
      "office": "IND",
      "OU": "OU=Users,OU=Site02,DC=Contoso,DC=com",
      "state": "Texas",
      "PostalCode": "10002"
    }
  }
}
```

1. This document is created with markdown and convert to PDF. If there are format issue please view the markdown file.