Active Directory Script User Guide

**INTRODUCTION**

This guide is meant to serve as an instruction manual for the ***CreateADComputer.ps1*** PowerShell script. This guide will refer to the script as ***CreateADComputer.ps1***. The purpose of this script is to assist with creating Computer Objects in Active Directory. If there are any questions, comments, bugs, or errors; then please email [SamuelFaulkner@MissouriState.edu](mailto:SamuelFaulkner@MissouriState.edu).

-----------------------------------------------------------------------------------------------------------------------------------------------------

**DEPENDENCIES**

This script was written and tested using PowerShell version 5.1 and heavily relies on the Active Directory Module for PowerShell. All Windows machines will have PowerShell natively installed but may not have Active Directory installed. To determine if a machine has the Active Directory Module for PowerShell, open a PowerShell window and run the command below:

Import-Module ActiveDirectory

If do not have the Active Directory Module for PowerShell, you will receive an error that says the following:

Import-Module : The specified module ‘ActiveDirectory’ was not loaded because no valid module file was found in any module directory.

If that is the case, you will need to install Active Directory Users and Computers from the Remote Server Administration Tools (RSAT). Instructions for completing this process can be found in the appendix at the end of this guide.

**IMPORTANT:** Do not continue until you can run the command above with no errors. The script will not work without Active Directory Users and Groups installed on your local machine.

**RUNNING THE SCRIPT**

If you are unfamiliar with running a PowerShell script, be sure to understand this section before continuing. There are two ways to run PowerShell scripts. Whichever method you wish to use will be up to personal preference.

Using Windows Explorer

* 1. Open *Windows Explorer*.
  2. Navigate to the directory containing the CreateADComputer.ps1 script.
  3. Right-Click the PowerShell script.
  4. Select “Run with PowerShell”.

Graphical user interface, text

Description automatically generatedGraphical user interface, text

Description automatically generated with medium confidence

Using PowerShell

1. Open *Windows PowerShell.*
2. Navigate to the directory containing the CreateADComputer.ps1 script by using either the CD or CHDIR command, followed by the full path of the directory.
3. Type .\CreateADComputer.ps1 and press *Enter.*

The script will have successfully started if you are met with the following screen.

Text

Description automatically generated

**USING THE SCRIPT**

The script currently, has three (3) different modes that it switches through. Mode 1 and Mode 2 function similarly to the other. They both allow you to create a single Computer Object by manually entering the object’s information. The difference between them lies in how they navigate to the desired OU. These are both recommended if you are creating a few Computer Objects.

Mode 3 is a little more intensive as it will attempt to import multiple machines’ information from a CSV file. There should be a CSV file called ***ADObject\_Template.csv***that came with the ***CreateADComputer.ps1*** script. I **highly** recommend taking that template and adding the machines you wish to add to it. This is important because the way the script reads the CSV file depends on how the first row is laid out and spelled. If there is a typo in the header at all, then the CSV import will fail.

To select your desired mode, just press *1*, *2*, or *3* and *Enter* to start it up.

-----------------------------------------------------------------------------------------------------------------------------------------------------

Mode 1: Manually Navigating to the Desired OU Path

In this mode, you will be navigating to the OU you wish to add a Computer Object to manually. This means going from one group into another repeatedly until you find the desired path. There are three (3) main sections to pay attention to.

Text

Description automatically generated

1. Locations

Near the top of the PowerShell window, you will see two or three lines. The script starts off in the SGF.EDUBEAR.NET/CUSTOM/COMPUTERS path by default. These color-coded lines tell you where you started in green, where you came from in magenta, and where you are currently in cyan.

**NOTE:** You will not see the magenta line until you start navigating through Active Directory.

1. Child Directories

Near the middle of the PowerShell window, you will see all the Child OUs of the Current OU directory. The left-hand column lists the numerical ID that represents the Child OU, and the right-hand column lists the name of the Child OU.

**NOTE:** If the Current OU path does not contain any Child OUs, then there will be no list. Instead, there will be a yellow line of text that reads “This OU does not contain any child OUs.”

1. List of Options

Near the end of the PowerShell window, you will see a list of available options you can choose from. The options available will depend on your current location, but they will be limited to the following:

* Enter ‘+’ to create a Computer Object at current location.
* Enter ‘^’ to return to Default OU location.
* Enter ‘<’ to return to Parent OU location.
* Enter the ID number to move to the respective OU location.

You will enter the numerical ID of the next path until you arrive at your desired location. Then, you will enter ‘+’ without the quotes to start creating a Computer Object. The other two options are there for you if you accidentally select the incorrect Child OU.

-----------------------------------------------------------------------------------------------------------------------------------------------------

Mode 2: Searching for the OU path using the Distinguished Name, Canonical Name, or with Keywords

This mode functions similarly to Mode 1. The main difference here is that instead of navigating from one path to another, this mode allows you to enter the full OU path or some select words to find the desired OU. I’ve listed the available formats all for the same OU path to give you a general idea of how this works. The main thing to know are the particular formats for each option.

Text

Description automatically generated with medium confidence

* Distinguished Name (DN): Highest level of the path is at the end and lowest level of the path is at the beginning. Each level starts with OU= and ends with a ‘,’. This does not include the top-most level of SGF.EDUBEAR.NET which is represented here as DC=SGF,DC=EDUBEAR,DC=NET.
* Canonical Name (CN): Highest level of the path is at the beginning and the lowest level of the path is at the end. Each level is separated by a ‘/’.
* Keywords (KW): This can really be any word that is in the path name of the OU. The main things to be cautious of here is using keywords that are words by themselves, but also exist in longer words (see Note 1 below); and using too many keywords as the returned listed will only pull paths that contain ALL the keywords entered (see Note 2 below).

**Note 1:** the keyword “OTHER” could reference “OTHER”, “mOTHER”, “brOTHER”, “hypOTHERmia”, “cryOTHERapy”, etc. This will not stop your OU from appearing on the list. It just might pull OUs you did not intend to search for.

**Note 2:** Entering the keywords CORE LIBR GLAS CHEK will not return an OU path as there is no OU path in our Active Directory that contains all four of those keywords.

To begin the search for the desired OU, type either full path of the desired OU in DN or CN format, or a few keywords that exist in the full OU path. Once you have done that and pressed *Enter*, the next screen will list all OU paths that match your query like the picture below after searching “CORE”.

Text

Description automatically generated

Your options here are limited to entering the numerical ID to select an OU path or pressing ‘^’ to try another search.

-----------------------------------------------------------------------------------------------------------------------------------------------------

Mode 1 and Mode 2: Entering Computer Object Information

After selecting an OU path to add a Computer Object to, the next screen should like the one below. This applies to BOTH Mode 1 and Mode 2. There are five (5) values the script is looking for and the beginning of Mode 1 and Mode 2 fill in the first value, “Computer OU”.

Text

Description automatically generated

The other fields required for the Computer Object are not as extensive as finding the Computer OU, but there are still some restrictions as to what is accepted for each field. These restrictions are listed below.

* Computer Name
  + The name must be between 1 and 15 characters.
  + The name cannot start with a . and/or contain the following characters: \ / : \* ? “ < > |
  + The name cannot be a Reserved Word. List of Reserved Words can be found in the appendix at the end of this guide.
  + The name cannot be used by a Computer Object that already exists in Active Directory.
* Computer MAC
  + The MAC Address must be 12 hexadecimal characters (0-9, A-F)
  + The MAC Address can only be delimited by the following characters: - . : Space
  + The MAC Address cannot be used by a Computer Object that already exists in Active Directory.
* Computer Description
  + No restrictions
* Computer Distribution Point
  + Only the Distribution Points in the list can be used. The list should be up-to-date provided the Configuration Manager console is installed on the local machine. If not, the script has a cached list of Distribution Points that was made on 3/9/2021.

After the last field is filled out, you will be met with a confirmation screen like the one below. This will list all the current values for each field you entered for the Computer Object and give you the opportunity to change the values, if need be. To change a value, enter the corresponding number in the options field below. If there are no changes to be made, press *Enter* to add the object to Active Directory.

Once the Computer Object has been added to Active Directory then you will be given the option to create another Computer Object in the same location, another Computer Object in a different location, or just close the script.

Text

Description automatically generated

The script creates a log file that details the operation. This file is created in the same directory that the script is in and called ***ADComputer\_Log.csv***. If the log file already exists from using it before, then instead of creating a new log file, the information from this session is appended to the end of the log file.

Mode 3: Importing Computer Objects via CSV file

This mode automates the steps above by entering all information needed into a CSV file. There is a file named ***ADObject\_Template.csv*** that comes with this script that is ready for you to add information in order to create a Computer Object. In the event that file gets deleted or lost, the only thing you need to make a new one is the header row. The script looks at the first row of a CSV file and looks for five (5) header names before importing any objects. The header row should look exactly like this:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COMPUTERNAME | COMPUTERMAC | COMPUTERDESC | COMPUTEROU | DEPLOYMENTSERVER |

**IMPORTANT:** The header must have each cell spelled exactly as it is above as well as having the same order as above. If a cell is in the wrong place or spelled incorrectly, then the import will fail every time.

The information for a single Computer Object should be contained in one row across these five columns. An example of a correct CSV file would look like this:

Application

Description automatically generated with medium confidence

You might notice that the Computer Objects I am attempting to import have different formats in the COMPUTERMAC, COMPUTEROU, and DEPLOYMENTSERVER fields. This is because the information in these fields can be entered just like it would in Modes 1 and 2 with the addition of using a shorter name for the DEPLOYMENTSERVER. All of the Deployment Servers that MEMCM uses follow the format of SCCM-DP-AREA-01.missouristate.edu where the AREA can be replaced with the area name that uses that Deployment Server. For example, you can use SCUF to represent SCCM-DP-SCUF-01.missouristate.edu, USIT to represent SCCM-DP-USIT-01.missouristate.edu, and COMN to represent SCCM-DP-COMN-01.missouristate.edu.

**NOTE:** I cannot tell you which Deployment Server you need to use. If you are unsure which one you are supposed to use, I would recommend contacting your MEMCM Site Administrator. They should be able to tell you which Deployment Server covers your area.

With all of that explained, you are now ready to tell the script which CSV file has the Computer Objects you wish to import. You should see a screen like the one below and you are prompted to enter the path of CSV file. This will be the full path of the file so make sure it looks similar to ***C:\Users\RM-CORE-SAM\Documents\Scripts\ADScript\CSVFILENAME.csv*** instead of something like ***.\CSVFILENAME.csv***

A picture containing timeline

Description automatically generated

While the import is happening, the script will tell you how many objects it found and the progress of the import. After every object has attempted to be created, the script will leave you with a screen telling you how many Computer Objects were successfully added to Active Directory and how many were unable to be added.

Text

Description automatically generated

The script creates a log file that details the operation. This file is created in the same directory that the script is in and called ***ADComputer\_Log.csv***. If the log file already exists from using it before, then instead of creating a new log file, the information from this session is appended to the end of the log file. The log file would look something like the table below.

A picture containing table

Description automatically generated

To tell if a computer was successfully added to Active Directory or not, you will look to the second-to-last column titled “SUCCESSFUL”. If the value is TRUE, then the machine should be on Active Directory. However, if the value is FALSE, then the Computer Object was NOT added to Active Directory. You can then look to the next column, titled “ERRORS”, and there should be a short description explaining why a Computer Object could not be created.

**NOTE:** The most common errors I have seen in testing are “COMPUTERNAME already exists in the AD”, “MAC Address is tied to COMPUTERNAME”, and “Could not find an OU you have access to matching these keywords”.

**APPENDIX**

-----------------------------------------------------------------------------------------------------------------------------------------------------

Installing Active Directory Users and Computers for Windows 10 Version 1809 and Above:

Starting with Windows 10 October 2018 Update, RSAT is included as a set of "Features on Demand" right from Windows 10. Do NOT download an RSAT package from <https://www.microsoft.com/en-us/download/details.aspx?id=45520>.

1. Go to ***Settings****.*
2. Select ***Apps***.
3. Click the link for “Optional Features”.
4. Select ***Add a Feature***to see the list of available RSAT tools.
5. Scroll down the list and select “RSAT: Active Directory Domain Services and Lightweight Directory Services Tools”
6. Select ***Install****.*

-----------------------------------------------------------------------------------------------------------------------------------------------------

Installing Active Directory Users and Computers for Windows 10 Version 1803 and Below:

**IMPORTANT:** You can install Remote Server Administration Tools for Windows 10 only on the full release of Windows 10 Professional or Windows 10 Enterprise.

1. Download and run the RSAT package that is appropriate for your computer’s architecture here: <https://www.microsoft.com/en-us/download/details.aspx?id=45520>.
2. When you are prompted by the Windows Update Standalone Installer dialog box to install the update, click ***Yes***.
3. Read and accept the license terms. Click ***I Accept***. Installation requires a few minutes to finish.

-----------------------------------------------------------------------------------------------------------------------------------------------------

List of Reserved Words

The following words can not be used as a computer name for an AD Computer Object:

ANONYMOUS, AUTHENTICATED USERS, BATCH, BUILTIN, CREATOR GROUP, CREATOR GROUP SERVER, CREATOR OWNER, CREATOR OWNER SERVER, DIALUP, DIGEST AUTH, INTERACTIVE, INTERNET, LOCAL, LOCAL SYSTEM, NETWORK, NETWORK SERVICE, NT AUTHORITY, NT DOMAIN, NTLM AUTH, NULL, PROXY, REMOTE INTERACTIVE, RESTRICTED, SCHANNEL AUTH, SELF, SERVER, SERVICE, SYSTEM, TERMINAL SERVER, THIS ORGANIZATION, USERS, WORLD.

-----------------------------------------------------------------------------------------------------------------------------------------------------