PowerShell workshop

Management of Active Directory content - graphical cmdlet help

Microsoft Premier Support

Author: Robert Novák

version 2.0c

Table of content

Terms of Use

How to use this help

-path <string[]>

- Specifies a path to one or more locations.
- When specifying multiple values for a parameter, use commas to separate the values:
  For example, "<parameter-name> <value1>, <value2>"
- Wildcards are permitted.
- The default location is the current directory (.).

Required?	false
Position?	1
Default value	Current location
Accept pipeline input?	true (ByValue, ByPropertyName)
Accept wildcard characters?	true

-include <string[]>

- **Retrieves only the specified items**.
- The value of this parameter qualifies the Path parameter.
- Enter a path element or pattern, such as "*.txt".
- Wildcards are permitted.
- is effective only when:
  - the command includes the Recurse parameter
  - the path leads to the contents of a directory, such as C:\Windows*, where the wildcard character specifies the contents of the C:\Windows directory.
- **is not efective when Path parameter contains only name of the folders**
- **When using the Include parameter without the Recurse parameter, the path must point to contents, not a container**

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	true

[] - empty brackets after data type name - the parameter accepts list of values of given data type

If you need specify multiple values for a parameter, use commas to separate particular values of given data type (i.e. string, integer, ...):
For example:

```
-include *.txt, *.log
```

Switch parameters

- **if ommited** on command line **false value is applied**
- **if included** on command line **true value is applied**

```
-recurse
```

This can be overriden by specifying value to swich parametr:

```
-recurse:$false
-recurse:$true
```

1 **Cmdlet name**

```
Get-Item [-path] <string[]>
Get-Item [-literalPath] <string[]>
```

```
[-include <string[]>] [-exclude <string[]>] [-filter <string>] [-force] [-credential <PSCredential>] [<CommonParameters>]
```

gi 2 **Alias**

3 **Mandatory parameters are always in bold red frame**

4 **[-parameter] - items in brackets are not required**

5

6

7 If the various **parameter sets** of given cmdlet have some **common set of parameters** these common parameters are included **only once**

-filter <string>

- Specifies a filter in the provider's format or language.
- The value of this parameter qualifies the Path parameter.
- The syntax of the filter, including the use of wildcards, depends on the provider.
- Filters are more efficient than other parameters, because **the provider applies them when retrieving the objects,** rather than having Windows PowerShell filter the objects after they are retrieved.

Required?	false
Position?	2
Default value	
Accept pipeline input?	false
Accept wildcard characters?	true

8

Information about the parameters

The help for particular cmdlets includes a table containing information for each of its parameters. This table includes the following fields:

Required: Indicates whether the **parameter is required** (true) or **optional** (false).

Position: Indicates whether the **parameter is named or positional** (i.e. **numbered**).
Positional parameters must appear in a specified place in the command.

Named **indicates that the parameter name is required**, but that the parameter can appear anywhere in the command.

<Number> indicates that the **parameter name is optional**, **but when the name is omitted, the parameter must be in the place specified by the number**.

For example, **"2" indicates** that when the parameter name is omitted, the parameter must be:
a) the second (2) in the command
b) the only unnamed parameter in the command.

When the parameter name is used, the parameter can appear anywhere in the command.

Default value: The **value** that Windows PowerShell uses **if you do not include the parameter in the command.**

Accepts pipeline input: Indicates **whether you can (true) or cannot (false) send objects to the parameter through a pipeline** "**By Property Name**" means that the **pipelined object must have a property with the same name as the parameter name.**

Accepts wildcard characters: Indicates whether the value of a parameter can include wildcard characters, such as * and ?.

Get-ADObject

```
Get-ADObject -Filter <string>
Get-ADObject -LDAPFilter <string>
Get-ADObject [-Identity] <ADObject> →
```

```
→ [-ResultPageSize <int>] [-ResultSetSize <int]>] [-SearchBase <string>] -SearchScope <value>]
```

```
→ [-AuthType <value>] [-Credential <PSCredential>] [-IncludeDeletedObjects <switch>]
[-Partition <string>] [-Properties <string[]>] [-Server <string>] [<CommonParameters>]
```

-Filter <string>

- **specifies a query string** that retrieves Active Directory objects.
- **uses the PowerShell Expression Language syntax**
- Note: To query using LDAP query strings, use the LDAPFilter parameter.

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-LDAPFilter <string>

- Specifies an LDAP query string that is used to filter Active Directory objects
- The Filter parameter syntax supports the same functionality as the LDAP syntax

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultSetSize <int32>

- specifies the **maximum number of objects to return**
- If you want to receive all of the objects, leaf this parameter at default value - $null (null value).
- You can use Ctrl+c to stop the query

Required?	false
Position?	named
Default value	$null
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchBase <string>

- Specifies an AD path to search under:

Default values:

- When you run a cmdlet from an AD provider drive - **current path of the drive**.
- When you run a cmdlet outside of an AD provider drive - **default naming context of the target domain**

Empty string as value:

- if you are connected to a GC port, all partitions will be searched.
- If you are not connected to a GC port, an error will be thrown.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultPageSize <int>

- Specifies the number of objects to include in one page of a query result
- the default is 256 objects per page.
- the following example shows how to set this parameter.
- -ResultPageSize 500

Required?	false
Position?	named
Default value	256
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchScope <ADSearchScope>

- Specifies the scope of an Active Directory search. Possible values for this parameter are:
  - **Base or 0** - searches only the specified path or object
  - **OneLevel or 1** - searches the specified path and the immediate children of that path or object
  - **Subtree or 2** - searches the specified path or object and all children of that path or object

Required?	false
Position?	named
Default value	Subtree
Accept pipeline input?	false
Accept wildcard characters?	false

-Identity <ADObject>

- Specifies an AD object by providing one of the following property values:
  - Distinguished Name:
    Example: CN=User1,CN=Users,DC=abcd,DC=int
  - GUID (objectGUID):
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - object received through pipeline
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-IncludeDeletedObjects <switch>

- Specifies to **retrieve deleted objects and the deactivated forward and backward links**.
- When this parameter is specified, the **cmdlet uses the following LDAP controls**:
  - **Show Deleted Objects** (1.2.840.113556.1.4.417)
  - **Show Deactivated Link**s (1.2.840.113556.1.4.2065)

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Properties <string[]>

- Specifies the **properties of the output object to retrieve from the server**
- Use this parameter to **retrieve properties that are not included in the default se**t.
- Specify properties for this parameter as a **comma-separated list of names**.
- To display all of the attributes that are set on the object, specify * (asterisk).

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Using filter parameter

- Most **get-AD*** Active Directory module cmdlets use the Filter parameter to search for objects
- This string uses the **PowerShell Expression Language syntax:**
  - provides rich type-conversion support for value types received by the Filter parameter.
  - uses an in-order representation, which means that the operator is placed between the operand and the value.
- The filter-driven search:
  - starts at container specified by the **-SearchBase** parameter of the cmdlet
  - required depth is specified by **-SearchScope** parameter of the cmdlet (default is **subtree**)

Syntax:

Filter syntax

{ [-not] **attribute operator value** [-and / -or] **attribute operator value** }

- PropertyName
- LDAPDisplayName

wildcards other than "*", such as "?" are not supported

Operator	Description	LDAP equivalent
-eq	Equal to. This will not support wild card search.	(attribute = value)
-like	Similar to -eq and supports wildcard comparison. The only wildcard character supported is: *	(attribute = value)
-ne	Not equal to. This will not support wild card search	!(attribute = value)
-notlike	Not like. Supports wild card comparison.	!(attribute = value)
-le	less than or equal to	(attribute <= value)
-lt	less than	!(attribute x >= value)
-ge	greater than or equal to	(attribute >= value)
-gt	greater than	!(attribute <= value)
-and	AND	&
-or	OR	|
-not	NOT	!
-bor	Bitwise OR	:1.2.840.113556.1.4.804:=
-band	Bitwise AND	:1.2.840.113556.1.4.803:=
-recursivematch	Use LDAP_MATCHING_RULE_IN_CHAIN (Note: This control only works with Windows 2008 and later.)	:1.2.840.113556.1.4.1941:=
-approx	Approximately equal to	~=

Examples

To get all objects of the type specified by the cmdlet, use the asterisk wildcard:

```
Get-ADUser -Filter *
```

To get all user objects that have an e-mail message attribute, use one of the following commands:

```
Get-ADUser -Filter {EmailAddress -like "*"}
Get-ADUser -Filter {mail -like "*"}
Get-ADObject -Filter {(mail -like "*") -and (ObjectClass -eq "user")}
```

To get all users objects that have surname of Smith and that have an e-mail attribute, use one of the following commands:

```
Get-ADUser -filter {(EmailAddress -like "*") -and (Surname  -eq "smith")}
```
-or-
```
Get-ADUser -filter {(mail -eq "*") -and (sn -eq "Smith")}
```

To get all user objects who have not logged on since January 1, 2007, use the following commands:

```
$logonDate = New-Object System.DateTime(2007, 1, 1)
Get-ADUser  -filter { lastLogon -le $logonDate  }
```

To get all groups that have a group category of Security and a group scope of Global, use one of the following commands:

```
Get-ADGroup -filter {GroupCategory -eq "Security" -and GroupScope -eq "Global"}
Get-ADGroup -filter {GroupType -band 0x80000000}
```

The Filter parameter has been implemented to

- replace the function of the LDAP Filter
- add support for:
- PowerShell variables
  - rich data types
  - improved error checking
  - Active Directory extended form of the PowerShell Expression Language

Missing SearchBase parameter

depends on the position from which the cmdlet is executed:
- within the AD provider drive - current path on the AD drive
- outside of any AD provider drive - server's DefaultNamingContext (see RootDSE)

-recursivematch (equivalent of LDAP_MATCHING_RULE_IN_CHAIN, i.e. 1.2.840.113556.1.4.1941)

- provides a method to look up whether an object is directly or indirectly included in other object by means of a linked attribute
- allows to **eliminate** resource intensive **recursive group membership expansion** to figure out group membership - usually applications make multiple round-trips to figure out whether an object fell "in the chain" of group memberships

Example - check if a user, "user1" is a **direct or indirect member of group** "group1".

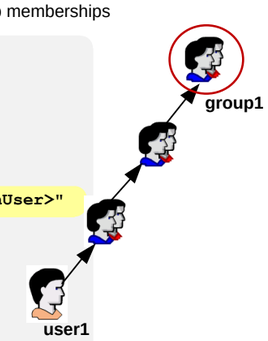
1. set the **base of query** to the distinguished name of the **user object** (dnUser)
2. set the **scope of the query** to **base**
3. execute following query using in filter parameter distinguished name of checked user group:

```
Get-ADUser -Filter {memberOf -RecursiveMatch "<dnGroup>"} -SearchBase "<dnUser>"
```

LDAP Filter Equivalent

```
(memberof:1.2.840.113556.1.4.1941:=(<dnGroup>))
```

4. This query returns the object of the user if it is the member of the group



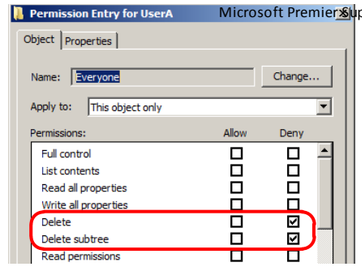
Optimizing Filters

- Avoid using:
  - -Recursive parameter as it intensifies resource usage of the search operation
  - bitwise AND operators and bitwise OR operators
  - logical NOT operator
- Break down your search into multiple queries with narrower conditions.

Set-ADObject

Set-ADObject cmdlet

- using this cmdlet you can modify values of:
  - **commonly used properties** (description, DisplayName, ProtectFromAccidentalDeletion) using the corresponding parameters
  - **other properties** by using the Add, Replace, Clear and Remove parameters.
- When you use the Add, Remove, Replace and Clear parameters together, the operations will be performed in the following order:
  1. Remove
  2. Add
  3. Replace
  4. Clear



-Identity <ADObject>

- Specifies an AD object by providing one of the following property values:
  - Distinguished Name
  - GUID (objectGUID)
  - object received through pipeline
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-Description <string>

- Specifies a description of the object.
- This parameter sets the value of the **Description attribute** for the AD object

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-DisplayName <string>

- Specifies the display name of the object
- This parameter sets the **displayName** attribute of the AD object

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ProtectedFromAccidentalDeletion [bool]

- when this property is set to **true**, you cannot delete the corresponding object without changing the value of the property - actually it adds Deny for Delete and Delete subtree ACE into the DACL of the AD object
- Possible values for this parameter include:
  $false or 0
  $true or 1 -

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Replace <hashtable>

Specifies values for an object properties that will replace the current values
You can modify more than one property by specifying a comma-separated list. The format for this parameter is

```
-Replace @{Attribute1LDAPDisplayName=value[],
          Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADObject [-Identity] <ADObject> [-Description <string>] [-DisplayName <string>] [-ProtectedFromAccidentalDeletion [bool]]
             [-Add <hashtable>] [-Clear <string[]>] [-Remove <hashtable>] [-Replace <hashtable>] →

Set-ADObject -Instance <ADObject> →
```

-Instance <ADObject>

- Specifies a **modified copy of an AD object to be saved in AD**
- The Instance parameter can only update Active Directory objects that have been retrieved by using the Get-ADObject cmdlet.
- **only properties that have changed are updated**
- When you specify the Instance parameter, you cannot specify other parameters that set properties on the object.

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Add <hashtable>

- Specifies values to add to an object properties specified by their LDAP display name
- You can specify multiple values to a property by specifying a comma-separated list of values and more than one property by separating them using a semicolon..
- The format forthis parameter is

```
-Add @{Attribute1LDAPDisplayName=value1, value2, ...;
       Attribute2LDAPDisplayName=value1, value2, ...;
       AttributeNLDAPDisplayName=value1, value2, ...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Clear <string[]>

- Specifies an array of object properties specified by their LDAP display name that will be cleared
- The format for this parameter is:

```
-Clear Attr1LDAPDisplayName,Attr2LDAPDisplayName
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false

-Remove <hashtable>

Specifies that the cmdlet remove values of an object properties specified by their LDAP display name
You can remove more than one property by specifying a semicolon-separated list.
The format for this parameter is:

```
-Remove @{Attribute1LDAPDisplayName=value[];
          Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-PassThru <switch>] [-Server <string>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an Active Directory provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

New-ADObject cmdlet

- creates a new AD object such as a new organizational unit or new user account
- use this cmdlet to create any type of AD object
- Properties that are not set by **Name**, **Type**, **Description** and **DisplayName** cmdlet parameters can be set by using the **OtherAttributes** parameter.
- The Path parameter specifies the container where the object will be created.. When you do not specify the Path parameter, the cmdlet creates an object in the default naming context container for AD objects in the domain.

New-ADObject

Three different ways to create an object by using this cmdlet:

Method 1: Use the New-ADObject cmdlet, specify the required parameters, and set any additional property values by using the cmdlet parameters.
Method 2: Use a template to create the new object:
1. retrieve an AD object that will serve as template:
   - create a new AD object
   - retrieve a copy of an existing AD object
2. set the property of this template object
3. specify the template AD object as the value to the Instance parameter of this cmdlet
4. You can override property values from the template by setting cmdlet parameters.

Method 3: Use the Import-CSV cmdlet with the Add-ADObject cmdlet to create multiple AD objects.
1. use the Import-CSV cmdlet to create the custom objects from a comma-separated value (CSV) file that contains a list of object properties
2. pass these objects through the pipeline to the New-ADObject cmdlet to create the AD objects.

-Name <string>

- This parameter sets the **name** attribute of the AD object

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Type <string>

specifies the type of object to create by the LDAP display name of the AD Schema Class that represents the object that you want to create.

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Path <string>

- Specifies the X.500 path of the Organizational Unit (OU) or container where the new object is created
- The rules for determining the default path (in the order of evaluation, first match wins):
  1. If the cmdlet is run from an AD PowerShell provider drive - **current path on the provider drive.**
  2. **default path of the cmdlet**. For example: in New-ADUser, the Path parameter would default to the Users container.
  3. **default naming context** of the target domain

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Description <string>

- Specifies a description of the object.
- This parameter sets the value of the **Description attribute** for the AD object

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-DisplayName <string>

- Specifies the display name of the object
- This parameter sets the **displayName** attribute of the AD object

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

```
New-ADObject [-Name] <string> [-Type] <string> [-Path <string>] [-Description <string>] [-DisplayName <string>]
             [-ProtectedFromAccidentalDeletion <bool>][-Instance <ADObject>] [-OtherAttributes <hashtable>]  →
```

-ProtectedFromAccidentalDeletion [bool]

- when this property is set to **true**, you cannot delete the corresponding object without changing the value of the property - actually it adds Deny for **Delete** and **Delete subtree** ACE into the DACL of the AD object
- Possible values for this parameter include:
  $false or 0
  $true or 1

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Instance <ADObject>

- Specifies an **instance of an AD object to be used as a template** for a new AD object.
- You can use an instance of an existing AD object as a template or you can construct a new AD object
- attributes of template object are not validated, so attempting to set attributes that do not exist or cannot be set will raise an error

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-OtherAttributes <hashtable>

Specifies values for new AD object attributes that are not represented by cmdlet parameters (Name, Description, DisplayName, ...)
You can set one or more attributes specified by their LDAP display name at the same time
If an attribute takes more than one value, you can assign multiple values as comma separated list
Syntax:

```
-OtherAttributes @{'Attribute1LDAPDisplayName'=value;
                   'Attribute2LDAPDisplayName'=value1,value2;...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-PassThru <switch>] [-Server <string>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Rename-ADObject

Rename-ADObject cmdlet

- renames an AD object by setting the **name** attribute of specified AD object
- To modify other naming attributes such as **given name**, **surname** and **sAMAccountName, ...** use the **Set-ADUser** cmdlet
- To modify the Security Accounts Manager (SAM) account name of a user, computer, or group, use the **Set-ADUser**, **Set-ADComputer** or **Set-ADGroup** cmdlet

-Identity <ADObject>

- Specifies an AD object by providing one of the following property values:
  - Distinguished Name
  - GUID (objectGUID)
  - object received through pipeline
- You can also use the **Get-ADGroup**, **Get-ADUser**, **Get-ADComputer**, **Get-ADServiceAccount**, **Get-ADOrganizationalUnit** and **Get-ADFineGrainedPasswordPolicy** cmdlets to get objects that you can pass through the pipeline to this cmdlet in order to rename them
- **If two or more objects are found when using dn or GUID as Identity**, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-NewName <string>

- This parameter sets the **name** attribute of the AD object

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

```
Rename-ADObject [-Identity] <ADObject> [-NewName] <string> →
→ [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-PassThru <switch>] [-Server <string>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Rename user account

Step 1. First we get in memory copy of user object

```
$UserToRename = Get-ADUser "TestUser01"
```

Step 2. Change all naming attributes to new values

```
Set-ADUser -Identity $UserToRename -Replace @{SAMAccountName="TestUser02"; `
           GivenName="Test"; sn="User02"; displayName="Test User02"; `
           userprincipalName="testuser02@abcd.int"} -Server DC1
```

Step 3. Rename user account using the Rename-ADObject cmdlet (note that this cmdlet requires to identify AD object to be renamed by its distinguishedName, objectGUID or pass the object to be renamed through pipeline)

```
#Step 3. Alternative 1
$UserToRename | Rename-ADObject -NewName "Test User02" -Server DC1

#Step 3. Alternative 2
Rename-ADObject -Identity "cn=TestUser01,cn=Users,dc=abcd,dc=int" `
                -NewName "Test User02" -Server DC1 -Server DC1
```

Move-ADObject

Move-ADObject cmdlet

- **moves an object or a container of objects from one container to another or from one domain to another**
- The Identity parameter specifies the Active Directory object or container to move.
- The TargetPath parameter must be specified. This parameter identifies the new location for the object or container.

-Identity <ADObject>

- Specifies an AD object by providing one of the following property values:
  - Distinguished Name
  - GUID (objectGUID)
  - object received through pipeline
- You can also use the **Get-ADGroup**, **Get-ADUser**, **Get-ADComputer**, **Get-ADServiceAccount**, **Get-ADOrganizationalUnit** and **Get-ADFineGrainedPasswordPolicy** cmdlets to get objects that you can pass through the pipeline to this cmdlet in order to move them
- **If two or more objects are found when using dn or GUID as Identity**, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-TargetPath <string>

- Specifies the new location for the object
- This location must be the path to a **container** or **organizational unit**.

Required?	true
Position?	2
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-TargetServer <string>

- **specifies the AD instance to be used if cross-domain move is performed**
- Note: A cross domain move requires a FQDN server name

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Move-ADObject [-Identity] <ADObject> [-TargetPath] <string> [-Server <string>] [-TargetServer <string>] →
→ [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-PassThru <switch>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADObject

Remove-ADObject cmdlet

- removes any type of AD object specified by Identity parameter
- If the object you specify to remove has child objects, you must specify the Recursive parameter.

-Identity <ADObject>

- Specifies an AD object by providing one of the following property values:
  - Distinguished Name
  - GUID (objectGUID)
  - object received through pipeline
- You can also use the **Get-ADGroup**, **Get-ADUser**, **Get-ADComputer**, **Get-ADServiceAccount**, **Get-ADOrganizationalUnit** and **Get-ADFineGrainedPasswordPolicy** cmdlets to get objects that you can pass through the pipeline to this cmdlet in order to remove them
- **If two or more objects are found when using dn or GUID as Identity**, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-IncludeDeletedObjects <switch>

- Specifies to **include deleted objects and the deactivated forward and backward links**.
- When this parameter is specified, the cmdlet uses the following LDAP controls:
  - Show Deleted Objects (1.2.840.113556.1.4.417)
  - Show Deactivated Links (1.2.840.113556.1.4.2065)

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Recursive <switch>

- Specifies that the cmdlet should remove the object and any children it contains.
- **Important**: if this parameter is used **all child objects even if they are marked with ProtectedFromAccidentalDeletion will be deleted**

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Remove-ADObject [-Identity] <ADObject> [-IncludeDeletedObjects <switch>][-Recursive <switch>]
→
[-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Restore-ADObject

Restore-ADObject cmdlet

- restores a deleted Active Directory object.
- **NewName parameter**
  - specifies the new name for the restored object
  - If not specified, the value of the AD attribute with an LDAP display name of "**msDS-lastKnownRDN**" is used.
- **TargetPath parameter**
  - specifies the new location for the restored object.
  - if not specified, the value of the Active Directory attribute with an LDAP display name of "**lastKnownParent**" is used.
- **Identity parameter** specifies the Active Directory object to restore

Returns the restored object when the PassThru parameter is specified. By default, this cmdlet does not generate any output.

-Identity <ADObject>

- Specifies an AD object to be restored by providing one of the following property values:
  - Distinguished Name
  - GUID (objectGUID)
  - object received through pipeline
- You can also use the **Get-ADObject** cmdlet with -**IncludeDeletedObjects** to retrieve a deleted objects that you can pass through the pipeline to this cmdlet in order to restore them
- **If two or more objects are found when using dn or GUID as Identity**, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-NewName <string>

- This parameter sets the **name** attribute of the restored AD object
- If not specified, the value of the "**msDS-lastKnownRDN**" attribute is used

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-TargetPath <string>

- Specifies the new location for the restored object
- This location must be the path to a **container** or **organizational unit**.
- if not specified, the value of the "**lastKnownParent**" attribute is used

Required?	true
Position?	2
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Rename-ADObject [-Identity] <ADObject> [-NewName <string>][-TargetPath <string>]
→ [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>]  [-PassThru <switch>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
C:\PS>Restore-ADObject -Identity "613dc90a-2afd-49fb-8bd8-eac48c6ab59f" -NewName "Kim Abercrombie" -TargetPath "OU=Finance,OU=UserAccoun
ts,DC=FABRIKAM,DC=COM"
```

Restores the ADObject while setting the 'msDS-LastKnownRDN' attribute of the deleted object to -NewName parameter and setting the 'lastK
nownRDN' to the -TargetPath parameter.

```
C:\PS>Get-ADObject -Filter 'samaccountname -eq "kimabercrombie"' -IncludeDeletedObjects | Restore-ADObject
```

Find a deleted user whose samaccountname is kimabercrombie, and restore it.

```
C:\PS>Restore-ADObject -Identity "CN=Kim Abercrombie\0ADEL:613dc90a-2afd-49fb-8bd8-eac48c6ab59f,CN=Deleted Objects,DC=FABRIKAM,DC=COM" -
NewName "Kim Abercrombie" -TargetPath "OU=Finance,OU=UserAccounts,DC=FABRIKAM,DC=COM"
```

Restores the ADObject while setting the 'msDS-LastKnownRDN' attribute of the deleted object to -NewName parameter and setting the 'lastK
nownRDN' to the -TargetPath parameter.

```
C:\PS>Get-ADObject -Filter 'msds-lastknownrdn -eq "user1"'  -Server server1:50000 -IncludeDeletedObjects -SearchBase "o=app1,c=us" | Restore-ADObject
```

Restore an AD-LDS object using msds-LastKnownRDN.

Get-ADUser

-Filter <string>

- **specifies a query string** that retrieves Active Directory objects.
- **uses the PowerShell Expression Language syntax**
- The Filter parameter syntax supports the same functionality as the LDAPFilter
- Note: To query using LDAP query strings, use the LDAPFilter parameter.

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-LDAPFilter <string>

- Specifies an LDAP query string that is used to filter Active Directory objects

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultSetSize <int32>

- specifies the **maximum number of objects to return**
- If you want to receive all of the objects, leaf this parameter at default value - $null (null value).
- You can use Ctrl+c to stop the query

Required?	false
Position?	named
Default value	$null
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchBase <string>

- Specifies an AD path to search under:

Default values:

- When you run a cmdlet from an AD provider drive - **current path of the drive**.
- When you run a cmdlet outside of an AD provider drive - **default naming context of the target domain**

Empty string as value:

- if you are connected to a GC port, all partitions will be searched.
- If you are not connected to a GC port, an error will be thrown.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Get-ADUser -Filter <string>
Get-ADUser -LDAPFilter <string>
Get-ADUser [-Identity] <ADUser> ...
```

```
[-ResultPageSize <int>] [-ResultSetSize <int]>] [-SearchBase <string>] -SearchScope <value>]
```

-ResultPageSize <int>

- Specifies the number of objects to include in one page of a query result
- the default is 256 objects per page.

Required?	false
Position?	named
Default value	256
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchScope <ADSearchScope>

- Specifies the scope of an Active Directory search. Possible values for this parameter are:
  - **Base or 0** - searches only the specified path or object
  - **OneLevel or 1** - searches the specified path and the immediate children of that path or object
  - **Subtree or 2** - searches the specified path or object and all children of that path or object

Required?	false
Position?	named
Default value	Subtree
Accept pipeline input?	false
Accept wildcard characters?	false

-Identity <ADUser>

- Specifies an AD object by providing one of the following property values:
  - **Distinguished Name (distinguishedName):**
    Example: CN=User1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: User1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

```
[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>]
[-Properties <string[]>] [-Server <string>] [<CommonParameters>]
```

-Properties <string[]>

- Specifies the **properties of the output object to retrieve from the server**
- Use this parameter to **retrieve properties that are not included in the default se**t.
- Specify properties for this parameter as a **comma-separated list of names**.
- To display all of the attributes that are set on the object, specify * (asterisk).

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADUser cmdlet

- gets a user object or performs a search to retrieve multiple user objects
- This cmdlet retrieves a default set of user object properties
- To retrieve additional properties use the Properties parameter

Usage:

- **Identity parameter**
  - specifies the AD user to get by its:
    - distinguished name (DN)
    - GUID
    - security identifier (SID)
    - SAM account name
    - name
  - You can also pass a user object through the pipeline to the Identity parameter.
- **Filter parameter**
  - uses the PowerShell Expression Language to write query strings for Active Directory
- **LDAPFilter parameter**
  - uses LDAP query syntax

New-ADUser,Set-ADUser supported properties

-ServicePrincipalNames <string[]>

- Specifies the service principal names for the account.
- This parameter sets the ServicePrincipalNames property of the account.
- Syntax:

To add values:

```
-ServicePrincipalNames @{Add=value1,value2,...}
```

To remove values:

```
-ServicePrincipalNames @{Remove=value3,value4,...}
```

To replace values:

```
-ServicePrincipalNames @{Replace=value1,value2,...}
```

To clear all values:

```
-ServicePrincipalNames $null
```

You can specify more than one change by using a list separated by semicolons. For example, use the following syntax to add and remo
ve service principal names.

```
@{Add=value1,value2,...};@{Remove=value3,value4,...}
```

The operators will be applied in the following sequence:
..Remove
..Add
..Replace

-AccountPassword <SecureString>

- Specifies a new password value for an account
- User accounts, by default, are created without a password.
- In order to ensure that accounts remain secure, user accounts will never be enabled unless a valid password is set or PasswordNotRequired is set to true.

-Certificates <X509Certificate[]>

- Modifies the DER-encoded X.509v3 certificates of the account.
- These certificates include the public key certificates issued to this account by the Microsoft Certificate Service.
- This parameter sets the Certificates property of the account object.
- Syntax:

To add values:

```
-Certificates @{Add=value1,value2,...}
```

To remove values:

```
-Certificates @{Remove=value3,value4,...}
```

To replace values:

```
-Certificates @{Replace=value1,value2,...}
```

To clear all values:

```
-Certificates $null
```

You can specify more than one operation by using a list separated by semicolons. For example, use the following syntax to add and remove Certificate values

```
-Certificates
@{Add=value1,value2,...};@{Remove=value3,value4,...}
```

The operators will be applied in the following sequence:
..Remove
..Add
..Replace

Naming and identification attributes

[-GivenName <string>]	givenName
[-Surname <string>]	sn
[-OtherName <string>]	middleName
[-Title <string>]	title
[-Description <string>]	description
[-DisplayName <string>]	displayName
[-Initials <string>]	initials
[-SamAccountName <string>]	sAMAccountName max 256 chars
[-UserPrincipalName <string>]	
[-ServicePrincipalNames <string[]>]	servicePrincipalName
[-EmployeeID <string>]	employeeID
[-EmployeeNumber <string>]	employeeNumber

Company and address attributes

[-StreetAddress <string>]	streetAddress
[-City <string>]	l
[-POBox <string>]	postOfficeBox
[-PostalCode <string>]	postalCode
[-State <string>]	st
[-Country <string>]	c
[-Company <string>]	company
[-Division <string>]	division
[-Department <string>]	department
[-Office <string>]	office
[-Organization <string>]	o
[-Manager <ADUser>]	manager distinguishedName, GUID, SID, SAMAccountname

Account properies attributes

[-Enabled <bool]>]	userAccountControl:ADS_UF_ACCOUNTDISABLE
[-AccountExpirationDate <DateTime>]	accountExpires 0 - never expires
[-AccountNotDelegated <bool>]	userAccountControl:ADS_UF_NOT_DELEGATED
[-SmartcardLogonRequired <bool>]	userAccountControl:ADS_UF_SMARTCARD_REQUIRED
[-TrustedForDelegation <bool>]	userAccountControl:ADS_UF_TRUSTED_FOR_DELEGATION

Contact attributes

[-EmailAddress <string>]	mail
[-HomePhone <string>]	homePhone
[-MobilePhone <string>]	mobile
[-OfficePhone <string>]	telephoneNumber
[-Fax <string>]	facsimileTelephoneNumber

Logon environment attributes

[-HomeDirectory <string>]	homeDirectory
[-HomeDrive <string>]	homeDrive
[-HomePage <string>]	wWWHomePage
[-ProfilePath <string>]	profilePath folder containing user profile
[-ScriptPath <string>]	scriptPath logon script path
[-LogonWorkstations <string>]	userWorkStations comma-separated list of SAMAccountNames or DNS names

Password properties attributes

[-AccountPassword <SecureString>]	
[-CannotChangePassword <bool>]	
[-AllowReversiblePasswordEncryption <bool>]	userAccountControl:ADS_UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED
[-ChangePasswordAtLogon <bool>]	
[-PasswordNeverExpires <bool>]	userAccountControl:ADS_UF_DONT_EXPIRE_PASSWD
[-PasswordNotRequired <bool>]	

Certificates attributes

[-Certificates <X509Certificate[]>]	userCertificate

New-ADUser

New-ADUser cmdlet

- creates a new Active Directory user
- it is able to create different types of user accounts such as iNetOrgPerson accounts by including the **Type** parameter and specifying any class in the AD schema that is a subclass of user and that has an object category of person.
- You can set commonly used user property values by using the cmdlet parameters
- Property values that are not associated with cmdlet parameters can be set by using the **OtherAttributes** parameter
- **Mandatory properties** for new user**:**
- SAMAccountName parameter

Three different ways to create an AD user by using this cmdlet:

Method 1: Use the New-ADUser cmdlet, specify the required parameters, and set any additional property values by using the cmdlet parameters.
Method 2: Use a template to create the new object:
1. retrieve an AD user object that will serve as template:
   - create a new AD user
   - retrieve a copy of an existing AD user
2. set the properties of this template user object
3. specify the template user object as the value to the **Instance** parameter of this cmdlet
4. You can override property values from the template by setting cmdlet parameters.

Method 3: Use the Import-CSV cmdlet with the Add-ADUser cmdlet to create multiple AD user objects.
1. use the Import-CSV cmdlet to create the custom objects from a comma-separated value (CSV) file that contains a list of object properties
2. pass these objects through the pipeline to the New-ADUser cmdlet to create the AD user objects.

-Name <string>

- Specifies the name of the user object
- This parameter sets the value of **name** attribute

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Path <string>

- Specifies the X.500 path of the Organizational Unit (OU) or container where the new object is created
- The rules for determining the default path (in the order of evaluation, first match wins):
  1. If the cmdlet is run from an AD PowerShell provider drive - **current path on the provider drive.**
  2. **default path of the cmdlet**. For example: in New-ADUser, the Path parameter would default to the Users container.
  3. **default naming context** of the target domain

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Type <string>

- Specifies the type of object to create.
- The selected type must be a subclass of the User schema class:
  - if this parameter is not specified it will default to "User".
  - use -Type "InetOrgPerson" to create a new Active Directory InetOrgPerson object.

Required?	false
Position?	named
Default value	user
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

```
New-ADUser [-Name] <string> PROPERTIES  [-Path <string>]  [-Instance <ADUser>]  [-OtherAttributes <hashtable>]  [-Type <string>]  →
```

See page **'New-ADUser,Set-ADUser supported properties'** for the list of supported properties

-Instance <ADObject>

- Specifies an **instance of an AD user object to be used as a template** for a new user objects.
- You can use an instance of an existing AD user object as a template or you can construct a new AD user object
- attributes of template object are not validated, so attempting to set attributes that do not exist or cannot be set will raise an error

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-OtherAttributes <hashtable>

Specifies user attributes and their values for attributes that are not represented by any cmdlet parameter
Syntax that shows how to set values for multiple attributes:

```
-OtherAttributes @{'Attribute1LDAPDisplayName'=value;
                   'Attribute2LDAPDisplayName'=value1,value2;...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADUser

Set-ADUser cmdlet

- modifies the attributes of an AD user account:
  - values of commonly used attributes by using the cmdlet parameters
  - values of attributes not represented by any cmdlet parameter can be modified by using the **Add**, **Replace**, **Clear** and **Remove** parameters
- can be used to manage content of both single and multi-valued attributes

-Identity <ADUser>

- specifies the AD user to modify by its:
  - distinguished name (DN)
  - GUID
  - security identifier (SID)
  - SAM account name
  - you can pass an object through the pipeline to the Identity parameter
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

See page **'New-ADUser,Set-ADUser supported properties'** for the list of supported properties

-Add <hashtable>

- Specifies values to add to an object properties specified by their LDAP display name
- You can specify multiple values to a property by specifying a comma-separated list of values and more than one property by separating them using a semicolon..
- The format forthis parameter is

```
-Add @{Attribute1LDAPDisplayName=value1, value2, ...;
       Attribute2LDAPDisplayName=value1, value2, ...;
       AttributeNLDAPDisplayName=value1, value2, ...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Replace <hashtable>

- Specifies values for properties that will replace their current values
- You can modify more than one property by specifying a comma-separated list.
- The format for this parameter is

```
-Replace @{Attribute1LDAPDisplayName=value[],
          Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADUser [-Identity] <ADUser> PROPERTIES [-Add <hashtable>] [-Clear <string[]>][-Remove <hashtable>] [-Replace <hashtable>] →

Set-ADUser -Instance <ADUser> [-SamAccountName <string>] →
```

-Instance <ADUser>

- provides a way to update a user object by **applying the changes made to a in-memory copy of the object**
- When you set the Instance parameter to a copy of an AD user object that has been modified, the Set-ADUser cmdlet makes the same changes to the original user object
- can only update AD objects that have been retrieved by using the Get-ADUser cmdlet
- **only properties that have changed are updated**

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Clear <string[]>

- Specifies an array of object properties specified by their LDAP display name that will be cleared
- The format for this parameter is:

```
-Clear Attribute1LDAPDisplayName,Attribute2LDAPDisplayName
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false

-Remove <hashtable>

- Specifies that the cmdlet **remove values** of an object properties specified by their LDAP display name
- You can remove more than one property by specifying a semicolon-separated list.
- The format for this parameter is:

```
-Remove @{Attribute1LDAPDisplayName=value1,value2;
          Attribute2LDAPDisplayName=value3,value4}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADUser

Remove-ADUser cmdlet

- removes an Active Directory user.
- The Identity parameter specifies the Active Directory user to remove.
- If the ADUser to be removed is identified by its DN, the Partition parameter will be automatically determined.

-Identity <ADUser>

- specifies the AD user to remove by its:
  - distinguished name (DN)
  - GUID
  - security identifier (SID)
  - SAM account name
  - you can pass an object through the pipeline to the Identity parameter
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Remove-ADUser [-Identity] <ADUser> [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADComputer

-Filter <string>

- **specifies a query string** that retrieves Active Directory objects.
- **uses the PowerShell Expression Language syntax**
- The Filter parameter syntax supports the same functionality as the LDAPFilter
- Note: To query using LDAP query strings, use the LDAPFilter parameter.

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-LDAPFilter <string>

- Specifies an LDAP query string that is used to filter Active Directory objects

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultSetSize <int32>

- specifies the **maximum number of objects to return**
- If you want to receive all of the objects, leaf this parameter at default value - $null (null value).
- You can use Ctrl+c to stop the query

Required?	false
Position?	named
Default value	$null
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchBase <string>

- Specifies an AD path to search under:

Default values:

- When you run a cmdlet from an AD provider drive - **current path of the drive**.
- When you run a cmdlet outside of an AD provider drive - **default naming context of the target domain**

Empty string as value:

- if you are connected to a GC port, all partitions will be searched.
- If you are not connected to a GC port, an error will be thrown.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Get-ADComputer -Filter <string>
Get-ADComputer -LDAPFilter <string>
Get-ADComputer [-Identity] <ADComputer>
```

```
[-ResultPageSize <int>] [-ResultSetSize <int]>] [-SearchBase <string>] -SearchScope <value>][-Properties <string[]>]
```

-Identity <ADComputer>

- Specifies an AD computer object by providing one of the following property values:
  - **Distinguished Name (distinguishedName):** Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):** Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-ResultPageSize <int>

- Specifies the number of objects to include in one page of a query result
- the default is 256 objects per page.

Required?	false
Position?	named
Default value	256
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchScope <ADSearchScope>

- Specifies the scope of an Active Directory search. Possible values for this parameter are:
  - **Base or 0** - searches only the specified path or object
  - **OneLevel or 1** - searches the specified path and the immediate children of that path or object
  - **Subtree or 2** - searches the specified path or object and all children of that path or object

Required?	false
Position?	named
Default value	Subtree
Accept pipeline input?	false
Accept wildcard characters?	false

-Properties <string[]>

- Specifies the **properties of the output object to retrieve from the server**
- Use this parameter to **retrieve properties that are not included in the default set**.
- Specify properties for this parameter as a **comma-separated list of names**.
- To display all of the attributes that are set on the object, specify * (asterisk).

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADComputer cmdlet

- gets a computer or performs a search to retrieve multiple computers
- This cmdlet retrieves a default set of computer object properties.
- To retrieve additional properties use the Properties parameter

```
.[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>] [-Server <string>] [<CommonParameters>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

New-ADComputer,Set-ADComputer supported properties

-ServicePrincipalNames <string[]>

- Specifies the service principal names for the account.
- This parameter sets the ServicePrincipalNames property of the account.
- Syntax:

To add values:

```
-ServicePrincipalNames @{Add=value1,value2,...}
```

To remove values:

```
-ServicePrincipalNames @{Remove=value3,value4,...}
```

To replace values:

```
-ServicePrincipalNames @{Replace=value1,value2,...}
```

To clear all values:

```
-ServicePrincipalNames $null
```

You can specify more than one change by using a list separated by semicolons. For example, use the following syntax to add and remo
ve service principal names.

```
@{Add=value1,value2,...};@{Remove=value3,value4,...}
```

The operators will be applied in the following sequence:
..Remove
..Add
..Replace

-AccountPassword <SecureString>

- Specifies a new password value for an account
- User accounts, by default, are created without a password.
- In order to ensure that accounts remain secure, user accounts will never be enabled unless a valid password is set or PasswordNotRequired is set to true.

-Certificates <X509Certificate[]>

- Modifies the DER-encoded X.509v3 certificates of the account.
- These certificates include the public key certificates issued to this account by the Microsoft Certificate Service.
- This parameter sets the Certificates property of the account object.
- Syntax:

To add values:

```
-Certificates @{Add=value1,value2,...}
```

To remove values:

```
-Certificates @{Remove=value3,value4,...}
```

To replace values:

```
-Certificates @{Replace=value1,value2,...}
```

To clear all values:

```
-Certificates $null
```

You can specify more than one operation by using a list separated by semicolons. For example, use the following syntax to add and remove Certificate values

```
-Certificates
@{Add=value1,value2,...};@{Remove=value3,value4,...}
```

The operators will be applied in the following sequence:
..Remove
..Add
..Replace

Naming and identification attributes

[-DNSHostName <string>]	
[-Description <string>]	description
[-DisplayName <string>]	displayName
[-SamAccountName <string>]	sAMAccountName max 256 chars
[-UserPrincipalName <string>]	
[-ServicePrincipalNames <string[]>]	servicePrincipalName
[-OperatingSystem <string>]	operatingSystem
[-OperatingSystemHotfix <string>]	operatingSystemHotfix
[-OperatingSystemServicePack <string>]	operatingSystemServicePack
[-OperatingSystemVersion <string>]	operatingSystemVersion
[-Location <string>]	location
[-HomePage <string>]	wWWHomePage
[-ManagedBy <ADPrincipal>]	managedBy

Account properies attributes

[-Enabled <bool]>]	userAccountControl:ADS_UF_ACCOUNTDISABLE
[-AccountExpirationDate <DateTime>]	accountExpires 0 - never expires
[-AccountNotDelegated <bool>]	userAccountControl:ADS_UF_NOT_DELEGATED
[-TrustedForDelegation <bool>]	userAccountControl:ADS_UF_TRUSTED_FOR_DELEGATION

Password properties attributes

[-CannotChangePassword <bool>]	
[-AllowReversiblePasswordEncryption <bool>]	userAccountControl:ADS_UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED
[-ChangePasswordAtLogon <bool>]	
[-PasswordNeverExpires <bool>]	userAccountControl:ADS_UF_DONT_EXPIRE_PASSWD
[-PasswordNotRequired <bool>]	

Certificates attributes

[-Certificates <X509Certificate[]>]	userCertificate

New-ADComputer

New-ADComputer

- cmdlet creates a new Active Directory computer object but does not join a computer to a domain
- **Providing values for attributes:**
  - values of commonly used computer attributes can be set using the cmdlet parameters.
  - values of attributes that are not represented by any cmdlet parameter can be modified by using the **OtherAttributes** parameter

Usage scenarios:
- You can use this cmdlet to provision a computer account before the computer is added to the domain.
- These pre-created computer objects can be used with:
  - offline domain join
  - unsecure domain Join
  - RODC domain join scenarios

Three different ways to create an AD computer by using this cmdlet:

Method 1: Use the New-ADComputer cmdlet, specify the required parameters, and set any additional property values by using the cmdlet parameters.
Method 2: Use a template to create the new object:
1. retrieve an AD computer object that will serve as template:
   - create a new AD computer
   - retrieve a copy of an existing AD computer
2. set the properties of this template computer object
3. specify the template computer object as the value to the **Instance** parameter of this cmdlet
4. You can override property values from the template by setting cmdlet parameters.

Method 3: Use the Import-CSV cmdlet with the New-ADComputer cmdlet to create multiple AD computer objects.
1. use the Import-CSV cmdlet to create the custom objects from a comma-separated value (CSV) file that contains a list of object properties
2. pass these objects through the pipeline to the New-ADComputer cmdlet to create the AD computer objects.

-Name <string>

- Specifies the name of the computer object
- This parameter sets the value of **name** attribute

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Path <string>

- Specifies the X.500 path of the Organizational Unit (OU) or container where the new computer object will be created
- The rules for determining the default path (in the order of evaluation, first match wins):
  1. If the cmdlet is run from an AD PowerShell provider drive - **current path on the provider drive.**
  2. **default path of the cmdlet**. For example: in New-ADComputer, the Parameter would default to the **Computers** container.
  3. **default naming context** of the target domain

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

```
New-ADUser [-Name] <string> PROPERTIES   [-Path <string>]  [-Instance <ADUser>]  [-OtherAttributes <hashtable>]  →
```

See page **'New-ADComputer,Set-ADCopmuter supported properties'** for the list of supported properties

-Instance <ADObject>

- Specifies an **instance of an AD computer object to be used as a template** for a new computer objects.
- You can use an instance of an existing AD computer object as a template or you can construct a new AD computer object
- attributes of template object are not validated, so attempting to set attributes that do not exist or cannot be set will raise an error

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-OtherAttributes <hashtable>

- Specifies user attributes and their values for attributes that are not represented by any cmdlet parameter
- Syntax that shows how to set values for multiple attributes:

```
-OtherAttributes @{'Attribute1LDAPDisplayName'=value;
                   'Attribute2LDAPDisplayName'=value1,value2;...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADComputer

Set-ADComputer cmdlet

- modifies the properties of an AD computer:
  - **values of commonly used attributes** by using the cmdlet parameters
  - **values of attributes not represented by any cmdlet parameter** can be modified by using the **Add**, **Replace**, **Clear** and **Remove** parameters
- When you use the Add, Remove, Replace and Clear parameters together, the operations will be performed in the following order:
  1.Remove
  2.Add
  3.Replace
  4.Clear

-Identity <ADComputer>

- Specifies an AD computer object to modify by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

See page **'New-ADComputer, Set-ADComputer supported properties'** for the list of supported properties

-Add <hashtable>

- Specifies values to add to an object properties specified by their LDAP display name
- You can specify multiple values to a property by specifying a comma-separated list of values and more than one property by separating them using a semicolon..
- The format forthis parameter is

```
-Add @{Attribute1LDAPDisplayName=value1, value2, ...;
       Attribute2LDAPDisplayName=value1, value2, ...;
       AttributeNLDAPDisplayName=value1, value2, ...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Replace <hashtable>

- Specifies values for properties that will replace their current values
- You can modify more than one property by specifying a comma-separated list.
- The format for this parameter is

```
-Replace @{Attribute1LDAPDisplayName=value[],
          Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADComputer [-Identity] <ADComputer> PROPERTIES [-Add <hashtable>] [-Clear <string[]>][-Remove <hashtable>] [-Replace <hashtable> →
Set-ADComputer -Instance <ADComputer> →
```

-Instance <ADComputer>

- provides a way to update a computer object by **applying the changes made to a in-memory copy of the object**
- When you set the Instance parameter to a copy of an AD computer object that has been modified, the Set-ADComputer cmdlet makes the same changes to the original computer object
- can only update AD objects that have been retrieved by using the Get-ADCOmputer cmdlet
- **only properties that have changed are updated**

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Clear <string[]>

- Specifies an array of object properties specified by their LDAP display name that will be cleared
- The format for this parameter is:

```
-Clear Attr1LDAPDisplayName,Attr2LDAPDisplayName
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false

-Remove <hashtable>

Specifies that the cmdlet remove values of an object properties specified by their LDAP display name
You can remove more than one property by specifying a semicolon-separated list.
The format for this parameter is:

```
-Remove @{Attribute1LDAPDisplayName=value[];
         Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADComputer

Remove-ADUser cmdlet

- removes an Active Directory Computer.
- The Identity parameter specifies the Active Directory computer to remove.
- If the AD computer is being identified by its DN, the Partition parameter will be automatically determined.

-Identity <ADComputer>

- Specifies an AD computer object to remove by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Remove-ADComputer [-Identity] <ADComputer> [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

```
C:\PS>Get-ADComputer -Filter 'Location -eq "NA/HQ/Building A"' | Remove-ADComputer

Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=LabServer-01,CN=Computers,DC=Fabrikam,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): a

Description
-----------
Remove all computers in a given location.
```

```
C:\PS>Get-ADComputer -Filter 'Location -eq "NA/HQ/Building A"' | Remove-ADComputer -confirm:$false

Remove all computers from a given location and disables the confirm prompt.
```

```
C:\PS>Remove-ADComputer -Identity "FABRIKAM-SRV4

Remove one particular computer.
```

Get-ADComputerServiceAccount

Get-ADComputerServiceAccount cmdlet

- **gets all of the service accounts that are hosted by the specified computer**
- managed service account is object of **msDS-ManagedServiceAccount** class

-Identity <ADComputer>

- Specifies an AD computer object that hosts the service accounts by providing one of the following values:
  - **Distinguished Name (distinguishedName):**
    Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Get-ADComputerServiceAccount [-Identity] <ADComputer>
```

```
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Add-ADComputerServiceAccount

Add-ADComputerServiceAccount cmdlet

- adds one or more computer service accounts to an Active Directory computer

Note: Adding a service account is a different operation than installing the service account locally.

- The **Identity** parameter specifies the Active Directory computer that will host the new service accounts.
- The **ServiceAccount** parameter specifies the service accounts to add.
  - If you are specifying more than one account, use a comma-separated list.

-Identity <ADComputer>

- Specifies an AD computer object that will host the service accounts by providing one of the following values:
  - **Distinguished Name (distinguishedName):** Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):** Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-ServiceAccount <ADServiceAccount>

- Specifies one or more AD service accounts by providing value for one of the following property:
  - **Distinguished Name (distinguishedName):** Example: CN=SQLSvc,OU=ServiceAccounts,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):** Example: SQLSvc
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Add-ADComputerServiceAccount [-Identity] <ADComputer> [-ServiceAccount] <ADServiceAccount[]> →
→ ..[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>][-PassThru <switch>][-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADComputerServiceAccount

Remove-ADComputerServiceAccount cmdlet

- removes service accounts from an Active Directory computer.
- The **Identity** parameter specifies the AD computer that contains the service accounts to remove
- The **ServiceAccount** parameter specifies the service accounts to remove
  - If you are specifying more than one service account, use a comma-separated list.

-Identity <ADComputer>

- Specifies an AD computer object that hosts the service accounts to be removed by providing one of the following values:
  - **Distinguished Name (distinguishedName):**
    Example: CN=CompA,CN=Computers,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: CompA$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-ServiceAccount <ADServiceAccount>

- Specifies one or more AD service accounts to be removed by providing value for one of the following property:
  - **Distinguished Name (distinguishedName):**
    Example: CN=SQLSvc,OU=ServiceAccounts,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-1103
  - **SAMAcccountName (sAMAccountName):**
    Example: SQLSvc
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Remove-ADComputerServiceAccount [-Identity] <ADComputer> [-ServiceAccount] <ADServiceAccount[]> →
→ ..[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>][-PassThru <switch>][-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADGroup

```
Get-ADGroup -Filter <string>
Get-ADGroup -LDAPFilter <string>
Get-ADGroup [-Identity] <ADGroup>
```

```
[-ResultPageSize <int>] [-ResultSetSize <int]>] [-SearchBase <string>] -SearchScope <value>][-Properties <string[]>]
```

```
.[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>] [-Server <string>] [<CommonParameters>]
```

-Filter <string>

- **specifies a query string** that retrieves Active Directory objects.
- **uses the PowerShell Expression Language syntax**
- The Filter parameter syntax supports the same functionality as the LDAPFilter
- Note: To query using LDAP query strings, use the LDAPFilter parameter.

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-LDAPFilter <string>

- Specifies an LDAP query string that is used to filter Active Directory objects

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultSetSize <int32>

- specifies the **maximum number of objects to return**
- If you want to receive all of the objects, leaf this parameter at default value - $null (null value).
- You can use Ctrl+c to stop the query

Required?	false
Position?	named
Default value	$null
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchBase <string>

- Specifies an AD path to search under:

Default values:

- When you run a cmdlet from an AD provider drive - **current path of the drive**.
- When you run a cmdlet outside of an AD provider drive - **default naming context of the target domain**

Empty string as value:

- if you are connected to a GC port, all partitions will be searched.
- If you are not connected to a GC port, an error will be thrown.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Identity <ADGroup>

- Specifies an AD computer object by providing one of the following property values:
  - **Distinguished Name (distinguishedName):** Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):** Example: Group1
  - **canonical name**
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-ResultPageSize <int>

- Specifies the number of objects to include in one page of a query result
- the default is 256 objects per page.

Required?	false
Position?	named
Default value	256
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchScope <ADSearchScope>

- Specifies the scope of an Active Directory search. Possible values for this parameter are:
  - **Base or 0** - searches only the specified path or object
  - **OneLevel or 1** - searches the specified path and the immediate children of that path or object
  - **Subtree or 2** - searches the specified path or object and all children of that path or object

Required?	false
Position?	named
Default value	Subtree
Accept pipeline input?	false
Accept wildcard characters?	false

-Properties <string[]>

- Specifies the **properties of the output object to retrieve from the server**
- Use this parameter to **retrieve properties that are not included in the default se**t.
- Specify properties for this parameter as a **comma-separated list of names**.
- To display all of the attributes that are set on the object, specify * (asterisk).

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADGroup cmdlet

- gets a group or performs a search to retrieve multiple groups
- gets a default set of group object properties
- To get additional properties use the **Properties** parameter

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

New-ADGroup,Set-ADGroup supported properties

-GroupCategory <ADGroupCategory>

- Specifies the category of the group that is stored in the **groupType** bitmask attributes
- Possible values of this parameter are defined in enumeration class **Microsoft.ActiveDirectory.Management.ADGroupCategory**
  - Distribution or 0
  - Security or 1

Required?	false
Position?	named
Default value	Security
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-GroupScope <ADGroupScope>

- Specifies the group scope of the group that is stored in the **groupType** bitmask attributes
- Possible values of this parameter are defined in enumeration class **Microsoft.ActiveDirectory.Management.ADGroupScope**:
  - DomainLocal or 0
  - Global or 1
  - Universal or 2

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

Naming and identification attributes

`[-Description <string>]`	`description`
`[-DisplayName <string>]`	`displayName`
`[-SamAccountName <string>]`	`sAMAccountName` max 256 chars
`[-HomePage <string>]`	`wWWHomePage`
`[-ManagedBy <ADPrincipal>]`	`managedBy`

Group object properies attributes

`[-GroupCategory <ADGroupCategory>]`	`groupType`
`[-GroupScope] <ADGroupScope]>`	`groupType`

New-ADGroup

New-ADGroup

- cmdlet creates a new Active Directory group object
- **Providing values for group object attributes:**
  - values of commonly used computer attributes can be set using the cmdlet parameters.
  - values of attributes that are not represented by any cmdlet parameter can be modified by using the **OtherAttributes** parameter

Usage scenarios:
- You can use this cmdlet to provision a computer account before the computer is added to the domain.
- These pre-created computer objects can be used with:
  - offline domain join
  - unsecure domain Join
  - RODC domain join scenarios

Three different ways to create an AD group object by using this cmdlet:

Method 1: Use the New-ADGroup cmdlet, specify the required parameters, and set any additional property values by using the cmdlet parameters.
Method 2: Use a template to create the new object:
1. retrieve an AD Group object that will serve as **template**:
   - create a new AD Group
   - retrieve a copy of an existing AD Group
2. **set the properties of this template** Group object
3. specify the **template Group object** as the value to the **Instance** parameter of this cmdlet
4. **You can override property values from the template** by setting cmdlet parameters.

Method 3: Use the Import-CSV cmdlet with the **New-ADGroup** cmdlet to create multiple AD Group objects.
1. use the **Import-CSV** cmdlet to create the custom group objects from a comma-separated value (CSV) file that contains a list of group objects properties
2. pass these objects through the pipeline to the **New-ADGroup** cmdlet to create the AD Group objects.

-Name <string>

- Specifies the name of the group object
- This parameter sets the value of **name** attribute

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

-Path <string>

- Specifies the X.500 path of the Organizational Unit (OU) or container where the new group object will be created
- The rules for determining the default path (in the order of evaluation, first match wins):
  1. If the cmdlet is run from an AD PowerShell provider drive - **current path on the provider drive.**
  2. **default path of the cmdlet**. For example: in New-ADGroup, the Path parameter would default to the **Computers** container.
  3. **default naming context** of the target domain

Required?	false
Position?	named
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

```
New-ADGroup [-Name] <string> [-GroupScope] <ADGroupScope> PROPERTIES [-Path <string>] [-Instance <ADGroup>] [-OtherAttributes <hashtable>]  →
```

-GroupScope <ADGroupScope>

- Specifies the group scope of the group that is stored in the **groupType** bitmask attributes
- Possible values of this parameter are defined in enumeration class **Microsoft.ActiveDirectory.Management.ADGroupScope**:
  - DomainLocal or 0
  - Global or 1
  - Universal or 2

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByPropertyName)
Accept wildcard characters?	false

See page **'New-ADGroup, Set-ADGroup supported properties'** for the list of supported properties

-Instance <ADObject>

- Specifies an **instance of an AD group object to be used as a template** for a new group objects.
- You can use an instance of an existing AD group object as a template or you can construct a new AD group object
- attributes of template object are not validated, so attempting to set attributes that do not exist or cannot be set will raise an error

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-OtherAttributes <hashtable>

- Specifies user attributes and their values for attributes that are not represented by any cmdlet parameter
- Syntax that shows how to set values for multiple attributes:

```
-OtherAttributes @{'Attribute1LDAPDisplayName'=value;
                   'Attribute2LDAPDisplayName'=value1,value2;...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADGroup

Set-ADGroup cmdlet

- modifies the properties of an AD grouip:
  - **values of commonly used attributes** by using the cmdlet parameters
  - **values of attributes not represented by any cmdlet parameter** can be modified by using the **Add**, **Replace**, **Clear** and **Remove** parameters
- When you use the Add, Remove, Replace and Clear parameters together, the operations will be performed in the following order:
  1.Remove
  2.Add
  3.Replace
  4.Clear

-Identity <ADGroup>

- Specifies an AD group object to modify by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

See page **'New-ADGroup, Set-ADGroup supported properties'** for the list of supported properties

-Add <hashtable>

- Specifies values to add to an object properties specified by their LDAP display name
- You can specify multiple values to a property by specifying a comma-separated list of values and more than one property by separating them using a semicolon..
- The format forthis parameter is

```
-Add @{Attribute1LDAPDisplayName=value1, value2, ...;
       Attribute2LDAPDisplayName=value1, value2, ...;
       AttributeNLDAPDisplayName=value1, value2, ...}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Replace <hashtable>

- Specifies values for properties that will replace their current values
- You can modify more than one property by specifying a comma-separated list.
- The format for this parameter is

```
-Replace @{Attribute1LDAPDisplayName=value[],
          Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADGroup [-Identity] <ADGroup> PROPERTIES [-Add <hashtable>] [-Clear <string[]>][-Remove <hashtable>] [-Replace <hashtable>]
Set-ADGroup -Instance <ADGroup>
```

-Instance <ADComputer>

- provides a way to update a group object by **applying the changes made to a in-memory copy of the object**
- When you set the Instance parameter to a copy of an AD group object that has been modified, the Set-ADGroup cmdlet makes the same changes to the original group object
- can only update AD objects that have been retrieved by using the Get-ADGroup cmdlet
- **only properties that have changed are updated**

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Clear <string[]>

- Specifies an array of object properties specified by their LDAP display name that will be cleared
- The format for this parameter is:

```
-Clear Attr1LDAPDisplayName,Attr2LDAPDisplayName
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false

-Remove <hashtable>

Specifies that the cmdlet remove values of an object properties specified by their LDAP display name
You can remove more than one property by specifying a semicolon-separated list.
The format for this parameter is:

```
-Remove @{Attribute1LDAPDisplayName=value[];
         Attribute2LDAPDisplayName=value[]}
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADGroup

Remove-ADUser cmdlet

- removes a security or distribution group
- The **Identity** parameter specifies the Active Directory group to remove.
- If the AD group is identified by its DN, the value of the **Partition** parameter will be automatically determined.

-Identity <ADGroup>

- Specifies an AD group object to remove by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Remove-ADGroup [-Identity] <ADGroup> [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

```
C:\PS>remove-adgroup SanjaysReports


Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=SanjayReports,DC=Fabrikam,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):


Description
-----------
Remove the group that has samAccountName 'SanjaysReports'.
```

```
C:\PS>get-adgroup -filter 'Name -like "Sanjay*"" | remove-adgroup


Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=SanjaysReports,DC=Fabrikam,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):


Description
-----------
Get all groups whose name starts with 'Sanjay' and then remove them.
```

```
C:\PS>Get-ADComputer -Filter 'Location -eq "NA/HQ/Building A"' | Remove-ADComputer -confirm:$false


Remove all computers from a given location and disables the confirm prompt.
```

Get-ADGroupMember

Get-ADGroupMember cmdlet

gets the members of an AD group
Members can be users, groups, and computers

-Identity <ADGroup>

- Specifies an AD group object whose members should be enlisted by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-Recursive <switch>

- Specifies that the cmdlet get all members including the members of nested groups
- If the specified group does not have any members, then nothing is returned.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Get-ADGroupMember [-Identity] <ADGroup> [-AuthType <value>] [-Credential <PSCredential>] [-Partition <string>] [-Server <string>] [-Recursive <switch>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an AD partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the **Identity parameter is set to a distinguished name**, the Partition is automatically generated from this distinguished name.
  - If **running cmdlets from an AD provider drive**, the Partition is automatically generated from the current path in the drive.
  - **default naming context** of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADGroupMember

Remove-ADGroupMember

- **removes one or more users, groups, service accounts, or computers from an Active Directory group**
- You cannot pass user, computer, or group objects through the pipeline to this cmdlet.
- To remove user, computer, or group objects from a group by using the pipeline, use the **Remove-ADPrincipalGroupMembership** cmdlet

-Identity <ADGroup>

- Specifies an AD group object from which specified members should be removed by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-Members <ADPrincipal[]>

- specifies a set of users, groups, and computers to be removed from a group by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=User1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Srv101$
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	2
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Remove-ADGroupMember [-Identity] <ADGroup> [-Members] <ADPrincipal[]> ... →
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Search-ADAccount

Search-ADAccount cmdlet

- **retrieves one or more user, computer, or service accounts that meet the criteria specified by the parameters**
- Search criteria include account and password status
- You can limit the search to user or computer accounts by specifying the UsersOnly or ComputersOnly parameter.
- Some search parameters, such as **AccountExpiring** and **AccountInactive** use a default time that you can change by specifying the DateTime or TimeSpan parameter. The DateTime parameter specifies a distinct time. The TimeSpan parameter specifies a time range from the current time.

-AccountDisabled <switch>

- Specifies a search for accounts that are disabled

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-AccountExpired <switch>

- Specifies a search for accounts that are expired
- An account is expired when the ADAccount **accountExpires** attribute is set to a time in the past

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-AccountExpiring <switch>

- search for accounts that are expiring:
  - **in a given time period** - use **TimeSpan** parameter
  - **by a specified time** - use **DateTime** parameter

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-TimeSpan <TimeSpan>

- Sets a time interval in the following format:
  [-]D.H:M:S.F
  where:
  D = Days (0 to 10675199)
  H = Hours (0 to 23)
  M = Minutes (0 to 59)
  S = Seconds (0 to 59)
  F= Fractions of a second (0 to 9999999)

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Search-ADAccount -AccountDisabled
Search-ADAccount -AccountExpired
Search-ADAccount -AccountExpiring [-DateTime <DateTime>] [-TimeSpan <TimeSpan>]
Search-ADAccount -AccountInactive [-DateTime <DateTime>] [-TimeSpan <TimeSpan>]
Search-ADAccount -LockedOut
Search-ADAccount -PasswordExpired
Search-ADAccount -PasswordNeverExpires
```

-AccountInactive <switch>

- Specifies to search for accounts that have not logged in within a given time period or since a specified time

-ComputersOnly <switch>

Specifies a search of only computer accounts.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-UsersOnly <switch>

Specifies a search of only user accounts.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultPageSize <int>

- Specifies the number of objects to include in one page of a query result
- the default is 256 objects per page.

Required?	false
Position?	named
Default value	256
Accept pipeline input?	false
Accept wildcard characters?	false

```
[-ComputersOnly <switch>][-UsersOnly <switch>] [-ResultPageSize <int>]
[-ResultSetSize <int>][-SearchBase <string>] [-SearchScope <value>] ... →
```

-PasswordExpired <switch>

- Specifies a search for accounts that have an expired password

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-PasswordNeverExpires <switch>

- Specifies a search for accounts that have a password that does not expire

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-LockedOut <switch>

- Specifies a search for accounts that are locked out

Required?	true
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-DateTime <DateTime>

- Specifies a distinct time value for **Search-ADAccount** cmdlet
- Time is assumed to be local time unless otherwise specified.
- When a time portion is not specified, the time is assumed to midnight local time
- When a date portion is not specified, the date is assumed to be the current date.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResultSetSize <int32>

- specifies the **maximum number of objects to return**
- If you want to receive all of the objects, leaf this parameter at default value - $null (null value).
- You can use Ctrl+c to stop the query

Required?	false
Position?	named
Default value	$null
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchBase <string>

- Specifies an AD path to search under:

Default values:

- When you run a cmdlet from an AD provider drive - **current path of the drive**.
- When you run a cmdlet outside of an AD provider drive - **default naming context of the target domain**

Empty string as value:

- if you are connected to a GC port, all partitions will be searched.
- If you are not connected to a GC port, an error will be thrown.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-SearchScope <ADSearchScope>

- Specifies the scope of an Active Directory search. Possible values for this parameter are:
  - **Base or 0** - searches only the specified path or object
  - **OneLevel or 1** - searches the specified path and the immediate children of that path or object
  - **Subtree or 2** - searches the specified path or object and all children of that path or object

Required?	false
Position?	named
Default value	Subtree
Accept pipeline input?	false
Accept wildcard characters?	false

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Server <string>]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, AD PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Note: this cmdlet doesn't work with the RODC

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

Various simple ADAccount operations

-Identity <ADAccount>

- specifies the Active Directory user, computer or service account that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

Enable-ADAccount cmdlet

enables an Active Directory user, computer or service account

```
Enable-ADAccount [-Identity] <ADAccount> ... →
```

Disable-ADAccount cmdlet

disables an Active Directory user, computer or service account

```
Disable-ADAccount [-Identity] <ADAccount> ... →
```

Unlock-ADAccount cmdlet

- restores domain access for an account that is locked
- domain access is suspended or locked for an account when the number of incorrect password entries exceeds the maximum number allowed by the account password policy.

```
Unlock-ADAccount [-Identity] <ADAccount> ... →
```

Clear-ADAccountExpiration cmdlet

- clears the expiration date for an AD user or computer account
- When you clear the expiration date for an account, the account does not expire.

```
Clear-ADAccountExpiration [-Identity] <ADAccount> ... →
```

```
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADAccountExpiration

Set-ADAccountExpiration cmdlet

- sets the expiration time for a user, computer or service account
- To **specify an exact time**, use the **DateTime** parameter
- To **specify a time period from the current time**, use the **TimeSpan** parameter
- you can use the **Search-ADAccount**, **Get-ADUser**, **Get-ADComputer** or **Get-ADServiceAccount** cmdlets to retrieve account objects that you can pass through the pipeline to this cmdlet

-Identity <ADAccount>

- specifies the Active Directory user, computer or service account that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-TimeSpan <TimeSpan>

- Sets a time interval in the following format:
  [-]D.H:M:S.F
  where:
  D = Days (0 to 10675199)
  H = Hours (0 to 23)
  M = Minutes (0 to 59)
  S = Seconds (0 to 59)
  F= Fractions of a second (0 to 9999999)

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-DateTime <DateTime>

- Specifies a distinct time value
- Time is assumed to be local time unless otherwise specified.
- When **a time portion is not specified**, the time is assumed to midnight local time
- When **a date portion is not specified**, the date is assumed to be the current date.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADAccountExpiration [-Identity] <ADAccount> [-TimeSpan] <TimeSpan> [-DateTime] <DateTime> ...
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**.
  Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADAccountPassword

Set-ADAccountPassword cmdlet

- sets the password for a user, computer or service account
- You must set the **OldPassword** and the **NewPassword** parameters to set the password unless you specify the **Reset** parameter.
- When you specify the **Reset** parameter, the password is set to the **NewPassword** value that you provide and the **OldPassword** parameter is not required.

-Identity <ADAccount>

- specifies the Active Directory user, computer or service account that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-NewPassword <SecureString>

- Specifies a new password value.
- This value is stored as an encrypted string.
- The following example shows how to set this parameter
  This command will prompt you and wait for a password:

```
-NewPassword (Read-Host -AsSecureString "New Password")
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-OldPassword <SecureString>

- Specifies a old password value.
- This value is stored as an encrypted string.
- The following example shows how to set this parameter
  This command will prompt you and wait for a password:

```
-OldPassword (Read-Host -AsSecureString "Old Password")
```

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Reset <switch>

- Specifies to reset the password on an account.
- When you use this parameter, you must set the **NewPassword** parameter only You do not need to specify the OldPassword parameter.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Set-ADAccountPassword [-Identity] <ADAccount> [-NewPassword <SecureString>][-OldPassword <SecureString>] [-Reset <switch>]...
```

```
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**.
  Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

C:\PS>Set-ADAccountPassword 'CN=Jeremy Los,OU=Accounts,DC=Fabrikam,DC=com' -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "p@ssw0rd" -Force)

Description

Sets the password of the user account with DistinguishedName: 'CN=Jeremy Los,OU=Accounts,DC=Fabrikam,DC=com' to 'p@ssw0rd'.

C:\PS>Set-ADAccountPassword -Identity tmakovec -OldPassword (ConvertTo-SecureString -AsPlainText "p@ssw0rd" -Force) -NewPassword (ConvertTo-SecureString -AsPlainText "qwert@12345" -Force)

Description

Sets the password of the user account with SamAccountName: tmakovec to 'qwert@12345'.

C:\PS>Set-ADAccountPassword -Identity saradavi

Please enter the current password for 'CN=Sara Davis,CN=Users,DC=Fabrikam,DC=com'
Password:**********
Please enter the desired password for 'CN=Sara Davis,CN=Users,DC=Fabrikam,DC=com'
Password:**********
Repeat Password:**********

Description

Sets the password of the user account with DistinguishedName: 'CN=Sara Davis,CN=Users,DC=Fabrikam,DC=com' (user is prompted for old and new password).

C:\PS>$newPassword = (Read-Host -Prompt "Provide New Password" -AsSecureString);
Set-ADAccountPassword -Identity mollyd -NewPassword $newPassword -Reset

Provide New Password: **********

Description

Prompts the user for a new password that is stored in a temporary variable named $newPassword, then uses it to reset the password for the user account with SamAccountName: mollyd.

Get-ADAccountAuthorizationGroup

Get-ADAuthorizationGroup cmdlet

- gets the security groups from the specified user, computer or service accounts token
- This cmdlet **requires a global catalo**g to perform the group search
- If the forest that contains the account does not have a global catalog, the cmdlet returns a non-terminating error.

-Identity <ADAccount>

- specifies the Active Directory user, computer or service account that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

```
Get-ADAccountAuthorizationGroup [-Identity] <ADAccount>
```

```
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Set-ADAccountControl

Set-ADAccountControl cmdlet

- modifies the user account control (UAC) values for an AD user or computer account
- various UAC values are represented by cmdlet parameters

-Identity <ADAccount>

- specifies the Active Directory user, computer or service account that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

All UAC based account properties have following characteristcs:

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

Parameter	Bit set in UAC mask	Description
AccountNotDelegated	ADS_UF_NOT_DELEGATED	the security context of the user is delegated to a service. When this parameter is set to true, the security context of the account is not delegated to a service even when the service account is set as trusted for Kerberos delegation
AllowReversiblePasswordEncryption	ADS_UF_ENCRYPTED_TEXT_ PASSWORD_ALLOWED	reversible password encryption is allowed for the account
CannotChangePassword		Modifies the ability of an account to change its password
DoesNotRequirePreAuth	ADS_ UF_DONT_REQUIRE_PREAUTH	Specifies whether Kerberos pre-authentication is required to logon using the user or computer account.
Enabled	ADS_UF_ACCOUNTDISABLE	Specifies if an account is enabled. An enabled account requires a password
HomedirRequired	ADS_UF_HOMEDIR_REQUIRED	Specifies whether a home directory is required for the account
MNSLogonAccount	ADS_UF_MNS_LOGON_ACCOUNT	• the account is a Majority Node Set (MNS) logon account • used to configure a multi-node cluster without using a shared disk drive
PasswordNeverExpires	ADS_UF_DONT_EXPIRE_PASSWD	the password of an account can expire
PasswordNotRequired	ADS_UF_PASSWD_NOTREQD	the account requires a password
TrustedForDelegation	ADS_UF_TRUSTED_FOR_DELEGATION	an account is trusted for Kerberos delegation. a service that runs under an account that is trusted for Kerberos delegation can assume the identity of a client requesting the service.
TrustedToAuthForDelegation	ADS_UF_TRUSTED_TO_ AUTHENTICATE_FOR_DELEGA TION	an account is enabled for delegation. When this parameter is set to true, a service running under such an account can impersonate a client on other remote servers on the network
UseDESKeyOnly	ADS_UF_USE_DES_KEY_ONLY	an account is restricted to use only Data Encryption Standard (DES) encryption types for keys

```
Set-ADAccountControl [-Identity] <ADAccount> [-AccountNotDelegated <bool>] [AllowReversiblePasswordEncryption <bool>] [-CannotChangePassword <bool>]
                     [-DoesNotRequirePreAuth <bool>] [-Enabled <bool>] [-HomedirRequired <bool>] [-MNSLogonAccount <bool>]
                    [-PasswordNeverExpires <bool>] [-PasswordNotRequired <bool>]  [-TrustedForDelegation <bool>]
                     [-TrustedToAuthForDelegation <bool>] [-UseDESKeyOnly <bool>] ...
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Get-ADPrincipalGroupMembership

Get-ADPrincipalGroupMembership cmdlet

- **gets the AD groups that is specified user, computer, group, or service account member**
- **requires a global catalog** to perform the group search
- if the forest that contains the user, computer or group does not have a global catalog, the cmdlet returns a non-terminating error
- If you want to search for local groups in another domain, use the ResourceContextServer parameter to specify the alternate server in the other domain.

```
Get-ADPrincipalGroupMembership [-Identity] <ADPrincipal> [-ResourceContextPartition <string>] [-ResourceContextServer <string>]
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-Identity <ADPrincipal>

- Specifies an AD principal object that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):** Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):** Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-ResourceContextPartition <string>

- distinguished name of the partition of an AD or AD LDS instance to search
- Use this parameter with the ResourceContextServer parameter to specify a partition hosted by the specified server
- If the ResourceContextPartition parameter is not specified, the default partition of the ResourceContextServer is searched.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-ResourceContextServer <string>

- cmdlet will return a list of groups that the user is a member of in the specified domain.
- **Use this parameter to search for groups in a domain that is not the domain where the user's account resides**.
- To search a partition other than the default partition in this domain, also specify the ResourceContextPartition parameter.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Add-ADPrincipalGroupMembership

Add-ADPrincipalGroupMembership cmdlet

- adds a user, group, service account, or computer as a new member to one or more AD groups
- This cmdlet is able to collect all of the user, computer and group objects from the pipeline, and then adds these objects to the specified group by using one AD operation
- You cannot pass group objects through the pipeline to the **MemberOf** parameter.
  - to add to a group by passing the group through the pipeline, use the **Add-ADGroupMember** cmdlet

-Identity <ADPrincipal>

- Specifies an AD principal object that you want to perform the operation with by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-MemberOf <ADGroup>

- Specifies one or more AD group objects into which AD principal objects will be added by providing one of the following value:
  - **Distinguished Name (distinguishedName):**
    Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):**
    Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):**
    Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):**
    Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	2
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Add-ADPrincipalGroupMembership [-Identity] <ADPrincipal> [-MemberOf] <ADGroup[]>
...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

Remove-ADPrincipalGroupMembership

Remove-ADPrincipalGroupMembership cmdlet

- removes a user, group, computer, service account, or any other account object from one or more AD groups
- This cmdlet is able to collect all of the user, computer and group objects from the pipeline, and then remove these objects from the specified group by using one AD operation

-Identity <ADPrincipal>

- Specifies an AD principal object that you want to remove from a group by providing one of the following value:
  - **Distinguished Name (distinguishedName):** Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):** Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	1
Default value	
Accept pipeline input?	true (ByValue)
Accept wildcard characters?	false

-MemberOf <ADGroup>

- Specifies one or more AD group objects from which AD principal objects will be removed by providing one of the following value:
  - **Distinguished Name (distinguishedName):** Example: CN=Group1,CN=Users,DC=abcd,DC=int
  - **GUID (objectGUID):** Example: 599c3d2e-f72d-4d20-8a88-030d99495f20
  - **SID (objectSID):** Example: S-1-5-21-3165297888-301567370-576410423-52123
  - **SAMAcccountName (sAMAccountName):** Example: Group1
  - **object received through pipeline**
- The cmdlet **searches the default naming context to find the object**.
- If two or more objects are found, the cmdlet returns a non-terminating error.

Required?	true
Position?	2
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

```
Remove-ADPrincipalGroupMembership [-Identity] <ADPrincipal> [-MemberOf] <ADGroup[]> →
→ ...[-AuthType <value>] [-Credential <PSCredential>][-Partition <string>][-Server <string>] [-PassThru <switch>] [-Confirm] [-WhatIf]
```

-AuthType <ADAuthType>

- Specifies the **authentication method to use**. Possible values for this parameter include:
  - **Negotiate** or 0
  - **Basic** or 1
- The default authentication method is Negotiate.
- A Secure Sockets Layer (SSL) connection is required for the Basic authentication method.

Required?	false
Position?	named
Default value	Negotiate
Accept pipeline input?	false
Accept wildcard characters?	false

-Credential <PSCredential>

- Specifies the user account credentials to use to perform this task
- default:
  - If the cmdlet is not run from AD provider drive, credentials of the currently logged on user
  - If the cmdlet is run from AD provider drive, **the account associated with the drive is the default.**
- To specify this parameter, you can provide:
  - user name "User1"
  - "Domain01\User01"
  - PSCredential object
- If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a **terminating error**.

Required?	false
Position?	named
Default value	currently logged on user
Accept pipeline input?	false
Accept wildcard characters?	false

-Partition <string>

- Specifies the distinguished name of an Active Directory partition.
- The cmdlet searches this partition to find the object defined by the Identity parameter.
- The rules for determining the default value are given below (in the order of evaluation, first match wins):
  - If the Identity parameter is set to a distinguished name, the Partition is automatically generated from this distinguished name.
  - If running cmdlets from an Active Directory provider drive, the Partition is automatically generated from the current path in the drive.
  - default naming context of the target domain.
  - If none of the previous cases apply, the Partition parameter will not take any default value.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false

-Server <string>

- usually the DC to use (but it may also be AD LDS, AD Domain Services, AD Snapshot instance)
- Domain name values:
  - FQDN: corp.contoso.com
  - NetBIOS name: CORP
- Directory server values:
  - FQDN: corp-DC12.corp.contoso.com
  - NetBIOS name: corp-DC12
  - FQDN + port: corp-DC12.corp.contoso.com:3268

Required?	false
Position?	named
Default value	DC associated with AD drive
Accept pipeline input?	false
Accept wildcard characters?	false

-PassThru <switch>

- Returns the new or modified object.
- By default (i.e. if -PassThru is not specified), this cmdlet does not generate any output.

Required?	false
Position?	named
Default value	
Accept pipeline input?	false
Accept wildcard characters?	false