

Product

Version

Latest

Version

2012

Version

2012 R2

New-ADUser

Creates an Active Directory user.

In this article

Syntax

Description

Examples

Required Parameters

Optional Parameters

Inputs

Outputs

Notes

Related Links

```
PowerShell
```

Copy

```
New-ADUser  
[-WhatIf]  
[-Confirm]  
[-AccountExpirationDate <DateTime>]  
[-AccountNotDelegated <Boolean>]  
[-AccountPassword <SecureString>]  
[-AllowReversiblePasswordEncryption <Boolean>]  
[-AuthenticationPolicy <ADAuthenticationPolicy>]  
[-AuthenticationPolicySilo <ADAuthenticationPolicySilo>]  
[-AuthType <ADAuthType>]  
[-CannotChangePassword <Boolean>]  
[-Certificates <X509Certificate[]>]  
[-ChangePasswordAtLogon <Boolean>]  
[-City <String>]  
[-Company <String>]
```

```
[-CompoundIdentitySupported <Boolean>]
[-Country <String>]
[-Credential <PSCredential>]
[-Department <String>]
[-Description <String>]
[-DisplayName <String>]
[-Division <String>]
[-EmailAddress <String>]
[-EmployeeID <String>]
[-EmployeeNumber <String>]
[-Enabled <Boolean>]
[-Fax <String>]
[-GivenName <String>]
[-HomeDirectory <String>]
[-HomeDrive <String>]
[-HomePage <String>]
[-HomePhone <String>]
[-Initials <String>]
[-Instance <ADUser>]
[-KerberosEncryptionType <ADKerberosEncryptionType>]
[-LogonWorkstations <String>]
[-Manager <ADUser>]
[-MobilePhone <String>]
[-Name] <String>
[-Office <String>]
[-OfficePhone <String>]
[-Organization <String>]
[-OtherAttributes <Hashtable>]
[-OtherName <String>]
[-PassThru]
[-PasswordNeverExpires <Boolean>]
[-PasswordNotRequired <Boolean>]
[-Path <String>]
[-POBox <String>]
[-PostalCode <String>]
[-PrincipalsAllowedToDelegateToAccount <ADPrincipal[]>]
[-ProfilePath <String>]
[-SamAccountName <String>]
[-ScriptPath <String>]
[-Server <String>]
[-ServicePrincipalNames <String[]>]
[-SmartcardLogonRequired <Boolean>]
[-State <String>]
[-StreetAddress <String>]
[-Surname <String>]
[-Title <String>]
[-TrustedForDelegation <Boolean>]
[-Type <String>]
[-UserPrincipalName <String>]
[<CommonParameters>]
```

Description

The **New-ADUser** cmdlet creates an Active Directory user. You can set commonly used user property values by using the cmdlet parameters.

You can set property values that are not associated with cmdlet parameters by using the *OtherAttributes* parameter. When using this parameter, be sure to place single quotes around the attribute name.

You must specify the *SamAccountName* parameter to create a user.

You can use the **New-ADUser** cmdlet to create different types of user accounts such as *iNetOrgPerson* accounts. To do this in Active Directory Domain Services (AD DS), set the *Type* parameter to the Lightweight Directory Access Protocol (LDAP) display name for the type of account you want to create. This type can be any class in the Active Directory schema that is a subclass of user and that has an object category of person.

The *Path* parameter specifies the container or organizational unit (OU) for the new user. When you do not specify the *Path* parameter, the cmdlet creates a user object in the default container for user objects in the domain.

The following methods explain different ways to create an object 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. To do this, create a new user object or retrieve a copy of an existing user object and set the *Instance* parameter to this object. The object provided to the *Instance* parameter is used as a template for the new object. You can override property values from the template by setting cmdlet parameters. For examples and more information, see the *Instance* parameter description for this cmdlet.

Method 3: Use the **Import-Csv** cmdlet with the **New-ADUser** cmdlet to create multiple Active Directory user objects. To do this, use the **Import-Csv** cmdlet to create the custom objects from a comma-separated value (CSV) file that contains a list of object properties. Then pass these objects through the pipeline to the **New-ADUser** cmdlet to create the user objects.

Examples

Example 1: Create a user with an imported certificate

PowerShell	 Copy
<pre>PS C:\> New-ADUser -Name "ChewDavid" -Certificate (New-Object System.Security.Cryptography.X509Certificates.X509Certificate -ArgumentList "Export.cer")</pre>	

This command creates a user named ChewDavid with a certificate imported from the file Export.cer.

Example 2: Create a user and set properties

PowerShell

 Copy

```
PS C:\> New-ADUser -Name "ChewDavid" -OtherAttributes
@{'title'="director";'mail'="chewdavid@fabrikam.com"}
```

This command creates a new user named ChewDavid and sets the **title** and **mail** properties on the new object.

Example 3: Create an inetOrgPerson user

PowerShell

 Copy

```
PS C:\> New-ADUser -Name "ChewDavid" -Type iNetOrgPerson -Path "DC=AppNC" -Server
lds.fabrikam.com:50000
```

This command creates an **inetOrgPerson**-class user named ChewDavid on an AD LDS instance.

Required Parameters

-Name

Specifies the name of the object. This parameter sets the **Name** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is name.

Type:
String

Position:
1

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

Optional Parameters

-AccountExpirationDate

Specifies the expiration date for an account. When you set this parameter to 0, the account never expires. This parameter sets the **AccountExpirationDate** property of an account object. The LDAP display name (**IdapDisplayName**) for this property is accountExpires.

Use the **DateTime** syntax when you specify this parameter. Time is assumed to be local time unless otherwise specified. When a time value is not specified, the time is assumed to 12:00:00 AM local time. When a date is not specified, the date is assumed to be the current date.

Type:
DateTime

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-AccountNotDelegated

Indicates whether 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. This parameter sets the **AccountNotDelegated** property for an Active Directory account. This parameter also sets the **ADS_UF_NOT_DELEGATED** flag of the Active Directory User Account Control (UAC) attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:
Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-AccountPassword

Specifies a new password value for an account. This value is stored as an encrypted string.

The following conditions apply based on the manner in which the password parameter is used:

- \$Null password is specified: No password is set and the account is disabled unless it is requested to be enabled.
- No password is specified: No password is set and the account is disabled unless it is requested to be enabled.
- User password is specified: Password is set and the account is disabled unless it is requested to be enabled.

User accounts, by default, are created without a password. If you provide a password, an attempt will be made to set that password however, this can fail due to password policy restrictions. The user account will still be created and you may use Set-ADAccountPassword to set the password on that account. 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.

The account is created if the password fails for any reason.

Type:
SecureString

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-AllowReversiblePasswordEncryption

Indicates whether reversible password encryption is allowed for the account. This parameter sets the **AllowReversiblePasswordEncryption** property of the account. This parameter also sets the **ADS_UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED** flag of the Active Directory User Account Control (UAC) attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:
Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-AuthType

Specifies the authentication method to use. The acceptable values for this parameter are:

- 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.

Type:
ADAuthType

Accepted values:
Negotiate, Basic

Position:
Named

Default value:
None

Accept pipeline input:

False

Accept wildcard characters:

False

-AuthenticationPolicy

Specifies an Active Directory Domain Services authentication policy object. Specify the authentication policy object in one of the following formats:

- Distinguished name
- GUID
- Name

This parameter can also get this object through the pipeline or you can set this parameter to an object instance.

The cmdlet searches the default naming context or partition to find the object. If the cmdlet finds two or more objects, the cmdlet returns a non-terminating error.

Type:

ADAuthenticationPolicy

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-AuthenticationPolicySilo

Specifies an Active Directory Domain Services authentication policy silo object. Specify the authentication policy silo object in one of the following formats:

- Distinguished name
- GUID
- Name

This parameter can also get this object through the pipeline or you can set this parameter to an object instance.

The cmdlet searches the default naming context or partition to find the object. If the cmdlet finds two or more objects, the cmdlet returns a non-terminating error.

Type:

ADAuthenticationPolicySilo

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-CannotChangePassword

Indicates whether the account password can be changed. This parameter sets the **CannotChangePassword** property of an account. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:

Boolean

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Certificates

Use the **DateTime** syntax when you specify this parameter. Time is assumed to be local time unless otherwise specified. When a time value is not specified, the time is assumed to 12:00:00 AM local time. When a date is not specified, the date is assumed to be the current date.

Type:

X509Certificate[]

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-ChangePasswordAtLogon

Indicates whether a password must be changed during the next logon attempt. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

This parameter cannot be set to \$True or 1 for an account that also has the **PasswordNeverExpires** property set to \$True.

Type:

Boolean

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-City

Specifies the user's town or city. This parameter sets the **City** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is l.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Company

Specifies the user's company. This parameter sets the **Company** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is company.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-CompoundIdentitySupported

Specifies whether an account supports Kerberos service tickets which includes the authorization data for the user's device. This value sets the compound identity supported flag of the Active Directory **msDS-SupportedEncryptionTypes** attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Warning: Domain-joined Windows systems and services such as clustering manage their own **msDS-SupportedEncryptionTypes** attribute. Therefore any changes to the flag on the **msDS-SupportedEncryptionTypes** attribute are overwritten by the service or system that manages the setting.

Type:
Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Confirm

Prompts you for confirmation before running the cmdlet.

Type:
SwitchParameter

Aliases:
cf

Position:
Named

Default value:
False

Accept pipeline input:

False

Accept wildcard characters:

False

-Country

Specifies the country or region code for the user's language of choice. This parameter sets the **Country** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is c. This value is not used by Windows 2000.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Credential

Specifies the user account credentials to use to perform this task. The default credentials are the credentials of the currently logged on user unless the cmdlet is run from an Active Directory PowerShell provider drive. If the cmdlet is run from such a provider drive, the account associated with the drive is the default.

To specify this parameter, you can type a user name, such as User1 or Domain01\User01 or you can specify a **PSCredential** object. If you specify a user name for this parameter, the cmdlet prompts for a password.

You can also create a **PSCredential** object by using a script or by using the **Get-Credential** cmdlet. You can then set the *Credential* parameter to the **PSCredential** object.

If the acting credentials do not have directory-level permission to perform the task, Active Directory PowerShell returns a terminating error.

Type:
PSCredential

Position:
Named

Default value:
None

Accept pipeline input:
False

Accept wildcard characters:
False

-Department

Specifies the user's department. This parameter sets the **Department** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is department.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Description

Specifies a description of the object. This parameter sets the value of the **Description** property for the user object. The LDAP display name (**IdapDisplayName**) for this property is description.

Type:
String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-DisplayName

Specifies the display name of the object. This parameter sets the **DisplayName** property of the user object. The LDAP display name (**IdapDisplayName**) for this property is displayName.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Division

Specifies the user's division. This parameter sets the **Division** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is division.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-EmailAddress

Specifies the user's e-mail address. This parameter sets the **EmailAddress** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is mail.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-EmployeeID

Specifies the user's employee ID. This parameter sets the **EmployeeID** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is employeeID.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:

False

-EmployeeNumber

Specifies the user's employee number. This parameter sets the **EmployeeNumber** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is employeeNumber.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Enabled

Specifies if an account is enabled. An enabled account requires a password. This parameter sets the **Enabled** property for an account object. This parameter also sets the **ADS_UF_ACCOUNTDISABLE** flag of the Active Directory User Account Control (UAC) attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:
Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:

False

-Fax

Specifies the user's fax phone number. This parameter sets the **Fax** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is facsimileTelephoneNumber.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-GivenName

Specifies the user's given name. This parameter sets the **GivenName** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is givenName.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-HomeDirectory

Specifies a user's home directory. This parameter sets the **HomeDirectory** property of a user object. The LDAP display name (**IdapDisplayName**) for this property is homeDirectory.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-HomeDrive

Specifies a drive that is associated with the UNC path defined by the **HomeDirectory** property. The drive letter is specified as `<DriveLetter>` : where `<DriveLetter>` indicates the letter of the drive to associate. The `<DriveLetter>` must be a single, uppercase letter and the colon is required. This parameter sets the **HomeDrive** property of the user object. The LDAP display name (**IdapDisplayName**) for this property is homeDrive.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-HomePage

Specifies the URL of the home page of the object. This parameter sets the **homePage** property of a user object. The LDAP display name (**ldapDisplayName**) for this property is wWWHomePage.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-HomePhone

Specifies the user's home telephone number. This parameter sets the **HomePhone** property of a user object. The LDAP display name (**ldapDisplayName**) of this property is homePhone.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Initials

Specifies the initials that represent part of a user's name. You can use this value for the user's middle initial. This parameter sets the **Initials** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is initials.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Instance

Specifies an instance of a user object to use as a template for a new user object.

You can use an instance of an existing user object as a template or you can construct a new user object for template use. You can construct a new user object using the Windows PowerShell command line or by using a script.

Method 1: Use an existing user object as a template for a new object. To retrieve an instance of an existing user object, use a cmdlet such as **Get-ADUser**. Then provide this object to the *Instance* parameter of the **New-ADUser** cmdlet to create a new user object. You can override property values of the new object by setting the appropriate parameters.

Method 2: Create a new **ADUser** object and set the property values by using the Windows PowerShell command line interface. Then pass this object to the *Instance* parameter of the **New-ADUser** cmdlet to create the new Active Directory user object.

Note: Specified attributes are not validated, so attempting to set attributes that do not exist or cannot be set raises an error.

Type:
ADUser

Position:
Named

Default value:

None

Accept pipeline input:

False

Accept wildcard characters:

False

-KerberosEncryptionType

Specifies whether an account supports Kerberos encryption types which are used during creation of service tickets. This value sets the encryption types supported flags of the Active Directory **msDS-SupportedEncryptionTypes** attribute. Possible values for this parameter are:

- None
- DES
- RC4
- AES128
- AES256

None removes all encryption types from the account, resulting in the KDC being unable to issue service tickets for services using the account.

DES is a weak encryption type that is not supported by default since Windows 7 and Windows Server 2008 R2.

Warning: Domain-joined Windows systems and services such as clustering manage their own **msDS-SupportedEncryptionTypes** attribute. Therefore any changes to the flag on the **msDS-SupportedEncryptionTypes** attribute are overwritten by the service or system that manages the setting.

Type:

ADKerberosEncryptionType

Accepted values:

None, DES, RC4, AES128, AES256

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-LogonWorkstations

Specifies the computers that the user can access. To specify more than one computer, create a single comma-separated list. You can identify a computer by using the Security Account Manager (SAM) account name (sAMAccountName) or the DNS host name of the computer. The SAM account name is the same as the NetBIOS name of the computer.

The LDAP display name (**IdapDisplayName**) for this property is userWorkStations.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Manager

Specifies the user's manager. This parameter sets the **Manager** property of a user object. This parameter is set by providing one of the following property values. Note: The identifier in parentheses is the LDAP display name for the property. The acceptable values for this parameter are:

- A distinguished name
 - A GUID (objectGUID)
 - A security identifier (objectSid)
 - A SAM account name (sAMAccountName)
-

Type:

ADUser

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-MobilePhone

Specifies the user's mobile phone number. This parameter sets the **MobilePhone** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is mobile.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Office

Specifies the location of the user's office or place of business. This parameter sets the **Office** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is office.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-OfficePhone

Specifies the user's office telephone number. This parameter sets the **OfficePhone** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is telephoneNumber.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-Organization

Specifies the user's organization. This parameter sets the **Organization** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is o.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:

False

-OtherAttributes

Specifies object attribute values for attributes that are not represented by cmdlet parameters. You can set one or more parameters at the same time with this parameter. If an attribute takes more than one value, you can assign multiple values. To identify an attribute, specify the LDAP display name (**IdapDisplayName**) defined for it in the Active Directory schema.

To specify a single value for an attribute:

```
-OtherAttributes @{ 'AttributeLDAPDisplayName'=value }
```

To specify multiple values for an attribute:

```
-OtherAttributes @{ 'AttributeLDAPDisplayName'=value1,value2,... }
```

To specify values for multiple attributes:

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

Type:

Hashtable

Position:

Named

Default value:

None

Accept pipeline input:

False

Accept wildcard characters:

False

-OtherName

Specifies a name in addition to a user's given name and surname, such as the user's middle name. This parameter sets the **OtherName** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is middleName.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-POBox

Specifies the user's post office box number. This parameter sets the **POBox** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is postOfficeBox.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-PassThru

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

Type:

SwitchParameter

Position:

Named

Default value:

None

Accept pipeline input:
False

Accept wildcard characters:
False

-PasswordNeverExpires

Specifies whether the password of an account can expire. This parameter sets the **PasswordNeverExpires** property of an account object. This parameter also sets the **ADS_UF_DONT_EXPIRE_PASSWD** flag of the Active Directory User Account Control attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Note: This parameter cannot be set to \$True or 1 for an account that also has the **ChangePasswordAtLogon** property set to \$True.

Type:
Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-PasswordNotRequired

Specifies whether the account requires a password. A password is not required for a new account. This parameter sets the **PasswordNotRequired** property of an account object.

Type:
Boolean

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Path

Specifies the X.500 path of the OU or container where the new object is created.

In many cases, a default value is used for the *Path* parameter if no value is specified. The rules for determining the default value are given below. Note that rules listed first are evaluated first and when a default value can be determined, no further rules are evaluated.

In Active Directory Domain Services (AD DS) environments, a default value for *Path* is set in the following cases:

- If the cmdlet is run from an Active Directory PowerShell provider drive, the parameter is set to the current path of the provider drive.
- If the cmdlet has a default path, this is used. For example: in *New-ADUser*, the *Path* parameter defaults to the Users container.
- If none of the previous cases apply, the default value of *Path* is set to the default partition or naming context of the target domain.

In AD LDS environments, a default value for *Path* is set in the following cases:

- If the cmdlet is run from an Active Directory module for PowerShell provider drive, the parameter is set to the current path of the provider drive.
- If the cmdlet has a default path, this is used. For example: in ***New-ADUser***, the *Path* parameter defaults to the Users container.
- If the target AD LDS instance has a default naming context, the default value of *Path* is set to the default naming context. To specify a default naming context for an AD LDS environment, set the **msDS-defaultNamingContext** property of the Active Directory directory service agent object (**nTDSDSA**) for the AD LDS instance.
- If none of the previous cases apply, the *Path* parameter does not take any default value.

Note: The Active Directory Provider cmdlets, such *New-Item*, *Remove-Item*, *Remove-ItemProperty*, *Rename-Item*, and *Set-ItemProperty* also contain a *Path* property. However, for the Active Directory Provider cmdlets, the *Path* parameter identifies the path of the actual object rather than the container.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-PostalCode

Specifies the user's postal code or zip code. This parameter sets the **PostalCode** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is postalCode.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-PrincipalsAllowedToDelegateToAccount

Specifies an array of principal objects. This parameter sets the **msDS-AllowedToActOnBehalfOfOtherIdentity** attribute of a computer account object.

Type:
ADPrincipal[]

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-ProfilePath

Specifies a path to the user's profile. This value can be a local absolute path or a Universal Naming Convention (UNC) path. This parameter sets the **ProfilePath** property of the user object. The LDAP display name (**IdapDisplayName**) for this property is profilePath.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-SamAccountName

Specifies the Security Account Manager (SAM) account name of the user, group, computer, or service account. The maximum length of the description is 256 characters. To be compatible with older operating systems, create a SAM account name that is 20 characters or less. This parameter sets the **SAMAccountName** for an account object. The LDAP display name (**IdapDisplayName**) for this property is sAMAccountName.

Note: If the string value provided is not terminated with a \$ character, the system adds one if needed.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-ScriptPath

Specifies a path to the user's log on script. This value can be a local absolute path or a Universal Naming Convention (UNC) path. This parameter sets the **ScriptPath** property of the user object. The LDAP display name (**IdapDisplayName**) for this property is scriptPath.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Server

Specifies the AD DS instance to connect to, by providing one of the following values for a corresponding domain name or directory server. The service may be any of the following: AD LDS, AD DS, or Active Directory snapshot instance.

Specify the AD DS instance in one of the following ways:

Domain name values:

- Fully qualified domain name

- NetBIOS name

Directory server values:

- Fully qualified directory server name
- NetBIOS name
- Fully qualified directory server name and port

The default value for this parameter is determined by one of the following methods in the order that they are listed:

- By using the *Server* value from objects passed through the pipeline
- By using the server information associated with the AD DS Windows PowerShell provider drive, when the cmdlet runs in that drive
- By using the domain of the computer running Windows PowerShell

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

False

Accept wildcard characters:

False

-ServicePrincipalNames

Specifies the service principal names for the account. This parameter sets the **ServicePrincipalNames** property of the account. The LDAP display name (**IdapDisplayName**) for this property is `servicePrincipalName`. This parameter uses the following syntax to add remove, replace or clear service principal name values:

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 remove service principal names.

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

The operators are applied in the following sequence:

- Remove
- Add
- Replace

Type:
String[]

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-SmartcardLogonRequired

Specifies whether a smart card is required to logon. This parameter sets the **SmartCardLoginRequired** property for a user object. This parameter also sets the **ADS_UF_SMARTCARD_REQUIRED** flag of the Active Directory User Account Control attribute. The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:

Boolean

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-State

Specifies the user's or Organizational Unit's state or province. This parameter sets the **State** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is st.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-StreetAddress

Specifies the user's street address. This parameter sets the **StreetAddress** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is streetAddress.

Type:
String

Position:
Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Surname

Specifies the user's last name or surname. This parameter sets the **Surname** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is sn.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Title

Specifies the user's title. This parameter sets the **Title** property of a user object. The LDAP display name (**IdapDisplayName**) of this property is title.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-TrustedForDelegation

Indicates whether 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. This parameter sets the **TrustedForDelegation** property of an account object. This value also sets the **ADS_UF_TRUSTED_FOR_DELEGATION** flag of the Active Directory User Account Control attribute.

The acceptable values for this parameter are:

- \$False or 0
- \$True or 1

Type:

Boolean

Position:

Named

Default value:

None

Accept pipeline input:

True (ByPropertyName)

Accept wildcard characters:

False

-Type

Specifies the type of object to create. Set the *Type* parameter to the LDAP display name of the Active Directory schema class that represents the type of object that you want to create. The selected type must be a subclass of the User schema class. If this parameter is not specified it defaults to User.

Type:

String

Position:

Named

Default value:

None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-UserPrincipalName

Specifies a user principal name (UPN) in the format `<user>@<DNS-domain-name>`. A UPN is a friendly name assigned by an administrator that is shorter than the LDAP distinguished name used by the system and easier to remember. The UPN is independent of the user object's distinguished name, so a user object can be moved or renamed without affecting the user logon name. When logging on using a UPN, users no longer have to choose a domain from a list on the logon dialog box.

Type:
String

Position:
Named

Default value:
None

Accept pipeline input:
True (ByPropertyName)

Accept wildcard characters:
False

-WhatIf

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Type:
SwitchParameter

Aliases:
wi

Position:
Named

Default value:

False

Accept pipeline input:

False

Accept wildcard characters:

False

Inputs

None or Microsoft.ActiveDirectory.Management.ADUser

A user object that is a template for the new user object is received by the *Instance* parameter.

Outputs

None or Microsoft.ActiveDirectory.Management.ADUser

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

Notes

- This cmdlet does not work with an Active Directory snapshot.
- This cmdlet does not work with a read-only domain controller.

Related Links

- [Get-ADUser](#)
- [Remove-ADUser](#)
- [Set-ADUser](#)
- [Set-ADAccountPassword](#)