Windows PowerShell Get-Help on Cmdlet 'Remove-AzADUser'

PS:\>Get-HELP Remove-AzADUser -Full

NAME

Remove-AzADUser

SYNOPSIS

Deletes entity from users.

SYNTAX

Remove-AzADUser -UPNOrObjectId <String> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]

[-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Remove-AzADUser -ObjectId <String> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-PassThru]

[-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Remove-AzADUser -UserPrincipalName <String> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]

[-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Remove-AzADUser -DisplayName <String> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]
[-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Remove-AzADUser -InputObject <IMicrosoftGraphUser> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend
<SendAsyncStep[]>] [-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Deletes entity from users.

PARAMETERS

-UPNOrObjectId <String>

The userPrincipalName or ObjectId of the user to be deleted.

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

-ObjectId <String>

key: id of user

Required? true
Position? named
Default value

Accept pipeline input? false

Accept wildcard characters? false

-UserPrincipalName <String>

user principal name

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayName <String>

user display name

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-InputObject <IMicrosoftGraphUser>

user input object

To construct, see NOTES section for INPUTOBJECT properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-DefaultProfile <PSObject>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-PassThru [<SwitchParameter>]

Returns true when the command succeeds

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

Microsoft.Azure.PowerShell.Cmdlets.Resources.MSGraph.Models.ApiV10.IMicrosoftGraphUser

OUTPUTS

System.Boolean

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help about_Hash_Tables.

INPUTOBJECT <IMicrosoftGraphUser>: user input object

[(Any) <Object>]: This indicates any property can be added to this object.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AccountEnabled <Boolean?>]: true if the account is enabled; otherwise, false. This property is required when a user is created. Supports $filter (eq, ne, NOT, and in).

[AgeGroup <String>]: Sets the age group of the user. Allowed values: null, minor, notAdult and adult. Refer to the legal age group property definitions for further information. Supports $filter (eq, ne, NOT, and in).

[ApproximateLastSignInDateTime <DateTime?>]: The timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only. Supports $filter (eq, ne, not, ge, le, and eq on null values) and $orderBy.

[City <String>]: The city in which the user is located. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[CompanyName <String>]: The company name which the user is associated. This property can be useful for describing the company that an external user comes from. The maximum length of the company name is 64 characters.Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[ComplianceExpirationDateTime <DateTime?>]: The timestamp when the device is no longer deemed compliant. The timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[ConsentProvidedForMinor <String>]: Sets whether consent has been obtained for minors. Allowed values: null, granted, denied and notRequired. Refer to the legal

age group property definitions for further information. Supports $filter (eq, ne, NOT, and in).

[Country <String>]: The country/region in which the user is located; for example, US or UK. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge,

le, in, startsWith).

[Department <String>]: The name for the department in which the user works. Maximum length is 64 characters.Supports $filter (eq, ne, NOT , ge, le, and in

operators).

[DeviceVersion <Int32?>]: For internal use only.

[EmployeeHireDate <DateTime?>]: The date and time when the user was hired or will start work in case of a future hire. Supports $filter (eq, ne, NOT , ge, le,

in).

[EmployeeId <String>]: The employee identifier assigned to the user by the organization. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[EmployeeOrgData <IMicrosoftGraphEmployeeOrgData>]: employeeOrgData

[(Any) <Object>]: This indicates any property can be added to this object.

[CostCenter <String>]: The cost center associated with the user. Returned only on $select. Supports $filter.

[Division <String>]: The name of the division in which the user works. Returned only on $select. Supports $filter.

[EmployeeType <String>]: Captures enterprise worker type. For example, Employee, Contractor, Consultant, or Vendor. Supports $filter (eq, ne, NOT , ge, le, in,

startsWith).

[ExternalUserState <String>]: For an external user invited to the tenant using the invitation API, this property represents the invited user's invitation

status. For invited users, the state can be PendingAcceptance or Accepted, or null for all other users. Supports $filter (eq, ne, NOT , in).

[ExternalUserStateChangeDateTime <DateTime?>]: Shows the timestamp for the latest change to the externalUserState property. Supports $filter (eq, ne, NOT , in).

[FaxNumber <String>]: The fax number of the user. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[GivenName <String>]: The given name (first name) of the user. Maximum length is 64 characters. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[Identity <IMicrosoftGraphObjectIdentity[]>]: Represents the identities that can be used to sign in to this user account. An identity can be provided by

Microsoft (also known as a local account), by organizations, or by social identity providers such as Facebook, Google, and Microsoft, and tied to a user account.

May contain multiple items with the same signInType value. Supports $filter (eq) only where the signInType is not userPrincipalName.

[Issuer <String>]: Specifies the issuer of the identity, for example facebook.com.For local accounts (where signInType is not federated), this property is the

local B2C tenant default domain name, for example contoso.onmicrosoft.com.For external users from other Azure AD organization, this will be the domain of the

federated organization, for example contoso.com.Supports $filter. 512 character limit.

[IssuerAssignedId <String>]: Specifies the unique identifier assigned to the user by the issuer. The combination of issuer and issuerAssignedId must be unique

within the organization. Represents the sign-in name for the user, when signInType is set to emailAddress or userName (also known as local accounts).When

signInType is set to: emailAddress, (or a custom string that starts with emailAddress like emailAddress1) issuerAssignedId must be a valid email addressuserName,

issuerAssignedId must be a valid local part of an email addressSupports $filter. 100 character limit.

[SignInType <String>]: Specifies the user sign-in types in your directory, such as emailAddress, userName or federated. Here, federated represents a unique

identifier for a user from an issuer, that can be in any format chosen by the issuer. Additional validation is enforced on issuerAssignedId when the sign-in type

is set to emailAddress or userName. This property can also be set to any custom string.

[IsResourceAccount <Boolean?>]: Do not use ??" reserved for future use.

[JobTitle <String>]: The user's job title. Maximum length is 128 characters. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[Mail <String>]: The SMTP address for the user, for example, admin@contoso.com. Changes to this property will also update the user's proxyAddresses collection

to include the value as an SMTP address. While this property can contain accent characters, using them can cause access issues with other Microsoft applications

for the user. Supports $filter (eq, ne, NOT, ge, le, in, startsWith, endsWith).

[MailNickname <String>]: The mail alias for the user. This property must be specified when a user is created. Maximum length is 64 characters. Supports $filter

(eq, ne, NOT, ge, le, in, startsWith).

[Manager <IMicrosoftGraphDirectoryObject>]: Represents an Azure Active Directory object. The directoryObject type

is the base type for many other directory

entity types.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AssignedPlan <IMicrosoftGraphAssignedPlan[]>]: The collection of service plans associated with the tenant. Not nullable.

[AssignedDateTime <DateTime?>]: The date and time at which the plan was assigned. The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z.

[CapabilityStatus <String>]: Condition of the capability assignment. The possible values are Enabled, Warning, Suspended, Deleted, LockedOut. See a detailed

description of each value.

[Service <String>]: The name of the service; for example, exchange.

[ServicePlanId <String>]: A GUID that identifies the service plan. For a complete list of GUIDs and their equivalent friendly service names, see Product

names and service plan identifiers for licensing.

[Branding <IMicrosoftGraphOrganizationalBranding>]: organizationalBranding

[(Any) <Object>]: This indicates any property can be added to this object.

[BackgroundColor <String>]: Color that will appear in place of the background image in low-bandwidth connections. We recommend that you use the primary

color of your banner logo or your organization color. Specify this in hexadecimal format, for example, white is #FFFFFF.

[BackgroundImage <Byte[]>]: Image that appears as the background of the sign-in page. The allowed types are PNG or JPEG not smaller than 300 KB and not

larger than 1920 A- 1080 pixels. A smaller image will reduce bandwidth requirements and make the page load faster.

[BackgroundImageRelativeUrl <String>]: A relative URL for the backgroundImage property that is combined with a CDN base URL from the cdnList to provide the

version served by a CDN. Read-only.

[BannerLogo <Byte[]>]: A banner version of your company logo that appears on the sign-in page. The allowed types are PNG or JPEG no larger than 36 A- 245

pixels. We recommend using a transparent image with no padding around the logo.

[BannerLogoRelativeUrl <String>]: A relative url for the bannerLogo property that is combined with a CDN base URL from the cdnList to provide the read-only

version served by a CDN. Read-only.

[CdnList <String[]>]: A list of base URLs for all available CDN providers that are serving the assets of the current resource. Several CDN providers are

used at the same time for high availability of read requests. Read-only.

[SignInPageText <String>]: Text that appears at the bottom of the sign-in box. You can use this to communicate additional information, such as the phone

number to your help desk or a legal statement. This text must be Unicode and not exceed 1024 characters.

[SquareLogo <Byte[]>]: A square version of your company logo that appears in Windows 10 out-of-box experiences (OOBE) and when Windows Autopilot is enabled

for deployment. Allowed types are PNG or JPEG no larger than 240 x 240 pixels and no more than 10 KB in size. We recommend using a transparent image with no

padding around the logo.

[SquareLogoRelativeUrl <String>]: A relative url for the squareLogo property that is combined with a CDN base URL from the cdnList to provide the version

served by a CDN. Read-only.

[UsernameHintText <String>]: String that shows as the hint in the username textbox on the sign-in screen. This text must be a Unicode, without links or

code, and can't exceed 64 characters.

[Id <String>]: The unique idenfier for an entity. Read-only.

[Localization <IMicrosoftGraphOrganizationalBrandingLocalization[]>]: Add different branding based on a locale.

[BackgroundColor <String>]: Color that will appear in place of the background image in low-bandwidth connections. We recommend that you use the primary

color of your banner logo or your organization color. Specify this in hexadecimal format, for example, white is #FFFFFF.

[BackgroundImage <Byte[]>]: Image that appears as the background of the sign-in page. The allowed types are PNG or JPEG not smaller than 300 KB and not

larger than 1920 A- 1080 pixels. A smaller image will reduce bandwidth requirements and make the page load faster.

[BackgroundImageRelativeUrl <String>]: A relative URL for the backgroundImage property that is combined with a CDN base URL from the cdnList to provide

the version served by a CDN. Read-only.

[BannerLogo <Byte[]>]: A banner version of your company logo that appears on the sign-in page. The allowed types are PNG or JPEG no larger than 36 A- 245

pixels. We recommend using a transparent image with no padding around the logo.

[BannerLogoRelativeUrl <String>]: A relative url for the bannerLogo property that is combined with a CDN base URL from the cdnList to provide the

read-only version served by a CDN. Read-only.

[CdnList <String[]>]: A list of base URLs for all available CDN providers that are serving the assets of the current resource. Several CDN providers are

used at the same time for high availability of read requests. Read-only.

[SignInPageText <String>]: Text that appears at the bottom of the sign-in box. You can use this to communicate additional information, such as the phone

number to your help desk or a legal statement. This text must be Unicode and not exceed 1024 characters.

[SquareLogo <Byte[]>]: A square version of your company logo that appears in Windows 10 out-of-box experiences (OOBE) and when Windows Autopilot is

enabled for deployment. Allowed types are PNG or JPEG no larger than 240 x 240 pixels and no more than 10 KB in size. We recommend using a transparent image with

no padding around the logo.

[SquareLogoRelativeUrl <String>]: A relative url for the squareLogo property that is combined with a CDN base URL from the cdnList to provide the version

served by a CDN. Read-only.

[UsernameHintText <String>]: String that shows as the hint in the username textbox on the sign-in screen. This text must be a Unicode, without links or

code, and can't exceed 64 characters.

[Id <String>]: The unique idenfier for an entity. Read-only.

[BusinessPhone <String[]>]: Telephone number for the organization. Although this is a string collection, only one number can be set for this property.

[CertificateBasedAuthConfiguration <IMicrosoftGraphCertificateBasedAuthConfiguration[]>]: Navigation property to manage certificate-based authentication

configuration. Only a single instance of certificateBasedAuthConfiguration can be created in the collection.

[Id <String>]: The unique idenfier for an entity. Read-only.

[CertificateAuthority <IMicrosoftGraphCertificateAuthority[]>]: Collection of certificate authorities which creates a trusted certificate chain.

[Certificate <Byte[]>]: Required. The base64 encoded string representing the public certificate.

[CertificateRevocationListUrl <String>]: The URL of the certificate revocation list.

[DeltaCertificateRevocationListUrl <String>]: The URL contains the list of all revoked certificates since the last time a full certificate revocaton list

was created.

[IsRootAuthority <Boolean?>]: Required. true if the trusted certificate is a root authority, false if the trusted certificate is an intermediate authority.

[Issuer <String>]: The issuer of the certificate, calculated from the certificate value. Read-only.

[IssuerSki <String>]: The subject key identifier of the certificate, calculated from the certificate value. Read-only.

[City <String>]: City name of the address for the organization.

[Country <String>]: Country/region name of the address for the organization.

[CountryLetterCode <String>]: Country or region abbreviation for the organization in ISO 3166-2 format.

[CreatedDateTime <DateTime?>]: Timestamp of when the organization was created. The value cannot be modified and is automatically populated when the

organization is created. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan

1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[Extension <IMicrosoftGraphExtension[]>]: The collection of open extensions defined for the organization. Read-only. Nullable.

[Id <String>]: The unique idenfier for an entity. Read-only.

[MarketingNotificationEmail <String[]>]: Not nullable.

[MobileDeviceManagementAuthority <MdmAuthority?>]: Mobile device management authority.

[OnPremisesLastSyncDateTime <DateTime?>]: The time and date at which the tenant was last synced with the on-premises directory. The Timestamp type represents

date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[OnPremisesSyncEnabled <Boolean?>]: true if this object is synced from an on-premises directory; false if this object was originally synced from an

on-premises directory but is no longer synced. Nullable. null if this object has never been synced from an on-premises directory (default).

[PostalCode <String>]: Postal code of the address for the organization.

[PreferredLanguage <String>]: The preferred language for the organization. Should follow ISO 639-1 Code; for example, en.

[PrivacyProfile <IMicrosoftGraphPrivacyProfile>]: privacyProfile

[(Any) <Object>]: This indicates any property can be added to this object.

[ContactEmail <String>]: A valid smtp email address for the privacy statement contact. Not required.

[StatementUrl <String>]: A valid URL format that begins with http:// or https://. Maximum length is 255 characters.

The URL that directs to the company's

privacy statement. Not required.

[ProvisionedPlan <IMicrosoftGraphProvisionedPlan[]>]: Not nullable.

[CapabilityStatus <String>]: For example, 'Enabled'.

[ProvisioningStatus <String>]: For example, 'Success'.

[Service <String>]: The name of the service; for example, 'AccessControlS2S'

[SecurityComplianceNotificationMail <String[]>]:

[SecurityComplianceNotificationPhone <String[]>]:

[State <String>]: State name of the address for the organization.

[Street <String>]: Street name of the address for organization.

[TechnicalNotificationMail <String[]>]: Not nullable.

[TenantType <String>]:

[VerifiedDomain <IMicrosoftGraphVerifiedDomain[]>]: The collection of domains associated with this tenant. Not nullable.

[Capability <String>]: For example, Email, OfficeCommunicationsOnline.

[IsDefault <Boolean?>]: true if this is the default domain associated with the tenant; otherwise, false.

[IsInitial <Boolean?>]: true if this is the initial domain associated with the tenant; otherwise, false.

[Name <String>]: The domain name; for example, contoso.onmicrosoft.com.

[Type <String>]: For example, Managed.

[AddIn <IMicrosoftGraphAddIn[]>]: Defines custom behavior that a consuming service can use to call an app in specific contexts. For example, applications that

can render file streams may set the addIns property for its 'FileHandler' functionality. This will let services like Office 365 call the application in the

context of a document the user is working on.

[Id <String>]:

[Property <IMicrosoftGraphKeyValue[]>]:

[Key <String>]: Key.

[Value <String>]: Value.

[Type <String>]:

[Api <IMicrosoftGraphApiApplication>]: apiApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[AcceptMappedClaim <Boolean?>]: When true, allows an application to use claims mapping without specifying a custom signing key.

[KnownClientApplication <String[]>]: Used for bundling consent if you have a solution that contains two parts: a client app and a custom web API app. If you

set the appID of the client app to this value, the user only consents once to the client app. Azure AD knows that consenting to the client means implicitly

consenting to the web API and automatically provisions service principals for both APIs at the same time. Both the client and the web API app must be registered

in the same tenant.

[Oauth2PermissionScope <IMicrosoftGraphPermissionScope[]>]: The definition of the delegated permissions exposed by the web API represented by this

application registration. These delegated permissions may be requested by a client application, and may be granted by users or administrators during consent.

Delegated permissions are sometimes referred to as OAuth 2.0 scopes.

[AdminConsentDescription <String>]: A description of the delegated permissions, intended to be read by an administrator granting the permission on behalf

of all users. This text appears in tenant-wide admin consent experiences.

[AdminConsentDisplayName <String>]: The permission's title, intended to be read by an administrator granting the permission on behalf of all users.

[Id <String>]: Unique delegated permission identifier inside the collection of delegated permissions defined for a resource application.

[IsEnabled <Boolean?>]: When creating or updating a permission, this property must be set to true (which is the default). To delete a permission, this

property must first be set to false. At that point, in a subsequent call, the permission may be removed.

[Origin <String>]:

[Type <String>]: Specifies whether this delegated permission should be considered safe for non-admin users to consent to on behalf of themselves, or

whether an administrator should be required for consent to the permissions. This will be the default behavior, but each customer can choose to customize the

behavior in their organization (by allowing, restricting or limiting user consent to this delegated permission.)

[UserConsentDescription <String>]: A description of the delegated permissions, intended to be read by a user granting the permission on their own behalf.

This text appears in consent experiences where the user is consenting only on behalf of themselves.

[UserConsentDisplayName <String>]: A title for the permission, intended to be read by a user granting the permission on their own behalf. This text

appears in consent experiences where the user is consenting only on behalf of themselves.

[Value <String>]: Specifies the value to include in the scp (scope) claim in access tokens. Must not exceed 120 characters in length. Allowed characters

are : ! # $ % & ' ( ) * + , - . / : ; = ? @ [ ] ^ + _ { } ~, as well as characters in the ranges 0-9, A-Z and a-z. Any other character, including the space

character, are not allowed. May not begin with ..

[PreAuthorizedApplication <IMicrosoftGraphPreAuthorizedApplication[]>]: Lists the client applications that are pre-authorized with the specified delegated

permissions to access this application's APIs. Users are not required to consent to any pre-authorized application (for the permissions specified). However, any

additional permissions not listed in preAuthorizedApplications (requested through incremental consent for example) will require user consent.

[AppId <String>]: The unique identifier for the application.

[DelegatedPermissionId <String[]>]: The unique identifier for the oauth2PermissionScopes the application requires.

[RequestedAccessTokenVersion <Int32?>]: Specifies the access token version expected by this resource. This changes the version and format of the JWT

produced independent of the endpoint or client used to request the access token. The endpoint used, v1.0 or v2.0, is chosen by the client and only impacts the

version of id_tokens. Resources need to explicitly configure requestedAccessTokenVersion to indicate the supported access token format. Possible values for

requestedAccessTokenVersion are 1, 2, or null. If the value is null, this defaults to 1, which corresponds to the v1.0 endpoint. If signInAudience on the

application is configured as AzureADandPersonalMicrosoftAccount, the value for this property must be 2

[AppRole <IMicrosoftGraphAppRole[]>]: The collection of roles assigned to the application. With app role assignments, these roles can be assigned to users,

groups, or service principals associated with other applications. Not nullable.

[AllowedMemberType <String[]>]: Specifies whether this app role can be assigned to users and groups (by setting to ['User']), to other application's (by

setting to ['Application'], or both (by setting to ['User', 'Application']). App roles supporting assignment to other applications' service principals are also

known as application permissions. The 'Application' value is only supported for app roles defined on application entities.

[Description <String>]: The description for the app role. This is displayed when the app role is being assigned and, if the app role functions as an

application permission, during consent experiences.

[DisplayName <String>]: Display name for the permission that appears in the app role assignment and consent experiences.

[Id <String>]: Unique role identifier inside the appRoles collection. When creating a new app role, a new Guid identifier must be provided.

[IsEnabled <Boolean?>]: When creating or updating an app role, this must be set to true (which is the default). To delete a role, this must first be set to

false. At that point, in a subsequent call, this role may be removed.

[Value <String>]: Specifies the value to include in the roles claim in ID tokens and access tokens authenticating an assigned user or service principal.

Must not exceed 120 characters in length. Allowed characters are : ! # $ % & ' ( ) * + , - . / : ; = ? @ [ ] ^ + _ { } ~, as well as characters in the ranges

0-9, A-Z and a-z. Any other character, including the space character, are not allowed. May not begin with ..

[ApplicationTemplateId <String>]: Unique identifier of the applicationTemplate.

[CreatedOnBehalfOfDeletedDateTime <DateTime?>]:

[CreatedOnBehalfOfDisplayName <String>]: The name displayed in directory

[Description <String>]: An optional description of the application. Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith) and $search.

[DisabledByMicrosoftStatus <String>]: Specifies whether Microsoft has disabled the registered application. Possible values are: null (default value),

NotDisabled, and DisabledDueToViolationOfServicesAgreement (reasons may include suspicious, abusive, or malicious activity, or a violation of the Microsoft

Services Agreement). Supports $filter (eq, ne, NOT).

[FederatedIdentityCredentials <IMicrosoftGraphFederatedIdentityCredential[]>]: Federated identities for applications. Supports $expand and $filter (eq when

counting empty collections).

[Audience <String[]>]: Lists the audiences that can appear in the external token. This field is mandatory, and defaults to 'api://AzureADTokenExchange'. It

says what Microsoft identity platform should accept in the aud claim in the incoming token. This value represents Azure AD in your external identity provider and

has no fixed value across identity providers - you may need to create a new application registration in your identity

provider to serve as the audience of this
token. Required.
[Description <String>]: The un-validated, user-provided description of the federated identity credential. Optional.
[Issuer <String>]: The URL of the external identity provider and must match the issuer claim of the external token being exchanged. The combination of the
values of issuer and subject must be unique on the app. Required.
[Name <String>]: is the unique identifier for the federated identity credential, which has a character limit of 120 characters and must be URL friendly. It
is immutable once created. Required. Not nullable. Supports $filter (eq).
[Subject <String>]: Required. The identifier of the external software workload within the external identity provider. Like the audience value, it has no
fixed format, as each identity provider uses their own - sometimes a GUID, sometimes a colon delimited identifier, sometimes arbitrary strings. The value here
must match the sub claim within the token presented to Azure AD. The combination of issuer and subject must be unique on the app. Supports $filter (eq).
[GroupMembershipClaim <String>]: Configures the groups claim issued in a user or OAuth 2.0 access token that the application expects. To set this attribute,
use one of the following string values: None, SecurityGroup (for security groups and Azure AD roles), All (this gets all security groups, distribution groups, and
Azure AD directory roles that the signed-in user is a member of).
[HomeRealmDiscoveryPolicy <IMicrosoftGraphHomeRealmDiscoveryPolicy[]>]:
[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:
[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition
differs for each derived policy type. Required.
[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be
activated as the organization default. Optional, default value is false.
[Description <String>]: Description for this policy.
[DeletedDateTime <DateTime?>]:
[DisplayName <String>]: The name displayed in directory
[IdentifierUri <String[]>]: The URIs that identify the application within its Azure AD tenant, or within a verified custom domain if the application is

multi-tenant. For more information, see Application Objects and Service Principal Objects. The any operator is required for filter expressions on multi-valued

properties. Not nullable. Supports $filter (eq, ne, ge, le, startsWith).

[Info <IMicrosoftGraphInformationalUrl>]: informationalUrl

[(Any) <Object>]: This indicates any property can be added to this object.

[MarketingUrl <String>]: Link to the application's marketing page. For example, https://www.contoso.com/app/marketing

[PrivacyStatementUrl <String>]: Link to the application's privacy statement. For example, https://www.contoso.com/app/privacy

[SupportUrl <String>]: Link to the application's support page. For example, https://www.contoso.com/app/support

[TermsOfServiceUrl <String>]: Link to the application's terms of service statement. For example, https://www.contoso.com/app/termsofservice

[IsDeviceOnlyAuthSupported <Boolean?>]: Specifies whether this application supports device authentication without a user. The default is false.

[IsFallbackPublicClient <Boolean?>]: Specifies the fallback application type as public client, such as an installed application running on a mobile device.

The default value is false which means the fallback application type is confidential client such as a web app. There are certain scenarios where Azure AD cannot

determine the client application type. For example, the ROPC flow where the application is configured without specifying a redirect URI. In those cases Azure AD

interprets the application type based on the value of this property.

[KeyCredentials <IMicrosoftGraphKeyCredential[]>]: The collection of key credentials associated with the application. Not nullable. Supports $filter (eq, NOT,

ge, le).

[CustomKeyIdentifier <Byte[]>]: Custom key identifier

[DisplayName <String>]: Friendly name for the key. Optional.

[EndDateTime <DateTime?>]: The date and time at which the credential expires.The Timestamp type represents date and time information using ISO 8601 format

and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Key <Byte[]>]: Value for the key credential. Should be a base 64 encoded value.

[KeyId <String>]: The unique identifier (GUID) for the key.

[StartDateTime <DateTime?>]: The date and time at which the credential becomes valid.The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Type <String>]: The type of key credential; for example, 'Symmetric'.

[Usage <String>]: A string that describes the purpose for which the key can be used; for example, 'Verify'.

[Logo <Byte[]>]: The main logo for the application. Not nullable.

[Note <String>]: Notes relevant for the management of the application.

[Oauth2RequirePostResponse <Boolean?>]:

[OptionalClaim <IMicrosoftGraphOptionalClaims>]: optionalClaims

[(Any) <Object>]: This indicates any property can be added to this object.

[AccessToken <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the JWT access token.

[AdditionalProperty <String[]>]: Additional properties of the claim. If a property exists in this collection, it modifies the behavior of the optional

claim specified in the name property.

[Essential <Boolean?>]: If the value is true, the claim specified by the client is necessary to ensure a smooth authorization experience for the specific

task requested by the end user. The default value is false.

[Name <String>]: The name of the optional claim.

[Source <String>]: The source (directory object) of the claim. There are predefined claims and user-defined claims from extension properties. If the

source value is null, the claim is a predefined optional claim. If the source value is user, the value in the name property is the extension property from the

user object.

[IdToken <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the JWT ID token.

[Saml2Token <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the SAML token.

[ParentalControlSetting <IMicrosoftGraphParentalControlSettings>]: parentalControlSettings

[(Any) <Object>]: This indicates any property can be added to this object.

[CountriesBlockedForMinor <String[]>]: Specifies the two-letter ISO country codes. Access to the application will be blocked for minors from the countries

specified in this list.

[LegalAgeGroupRule <String>]: Specifies the legal age group rule that applies to users of the app. Can be set to one of the following values:

ValueDescriptionAllowDefault. Enforces the legal minimum. This means parental consent is required for minors in the European Union and

Korea.RequireConsentForPrivacyServicesEnforces the user to specify date of birth to comply with COPPA rules.

RequireConsentForMinorsRequires parental consent for

ages below 18, regardless of country minor rules.RequireConsentForKidsRequires parental consent for ages below 14, regardless of country minor

rules.BlockMinorsBlocks minors from using the app.

[PasswordCredentials <IMicrosoftGraphPasswordCredential[]>]: The collection of password credentials associated with the application. Not nullable.

[CustomKeyIdentifier <Byte[]>]: Do not use.

[DisplayName <String>]: Friendly name for the password. Optional.

[EndDateTime <DateTime?>]: The date and time at which the password expires represented using ISO 8601 format and is always in UTC time. For example,

midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

[KeyId <String>]: The unique identifier for the password.

[StartDateTime <DateTime?>]: The date and time at which the password becomes valid. The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

[PublicClient <IMicrosoftGraphPublicClientApplication>]: publicClientApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access

tokens are sent.

[RequiredResourceAccess <IMicrosoftGraphRequiredResourceAccess[]>]: Specifies the resources that the application needs to access. This property also specifies

the set of OAuth permission scopes and application roles that it needs for each of those resources. This configuration of access to the required resources drives

the consent experience. Not nullable. Supports $filter (eq, NOT, ge, le).

[ResourceAccess <IMicrosoftGraphResourceAccess[]>]: The list of OAuth2.0 permission scopes and app roles that the application requires from the specified

resource.

[Id <String>]: The unique identifier for one of the oauth2PermissionScopes or appRole instances that the resource application exposes.

[Type <String>]: Specifies whether the id property references an oauth2PermissionScopes or an appRole. Possible values are Scope or Role.

[ResourceAppId <String>]: The unique identifier for the resource that the application requires access to. This

should be equal to the appId declared on the
target resource application.
[SignInAudience <String>]: Specifies the Microsoft accounts that are supported for the current application. Supported values are: AzureADMyOrg,
AzureADMultipleOrgs, AzureADandPersonalMicrosoftAccount, PersonalMicrosoftAccount. See more in the table below. Supports $filter (eq, ne, NOT).
[Spa <IMicrosoftGraphSpaApplication>]: spaApplication
[(Any) <Object>]: This indicates any property can be added to this object.
[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access
tokens are sent.
[Tag <String[]>]: Custom strings that can be used to categorize and identify the application. Not nullable.Supports $filter (eq, NOT, ge, le, startsWith).
[TokenEncryptionKeyId <String>]: Specifies the keyId of a public key from the keyCredentials collection. When configured, Azure AD encrypts all the tokens it
emits by using the key this property points to. The application code that receives the encrypted token must use the matching private key to decrypt the token
before it can be used for the signed-in user.
[TokenIssuancePolicy <IMicrosoftGraphTokenIssuancePolicy[]>]:
[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:
[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition
differs for each derived policy type. Required.
[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be
activated as the organization default. Optional, default value is false.
[Description <String>]: Description for this policy.
[DeletedDateTime <DateTime?>]:
[DisplayName <String>]: The name displayed in directory
[TokenLifetimePolicy <IMicrosoftGraphTokenLifetimePolicy[]>]: The tokenLifetimePolicies assigned to this application. Supports $expand.
[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:
[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy.

The syntax for the definition

differs for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be

activated as the organization default. Optional, default value is false.

[Description <String>]: Description for this policy.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[Web <IMicrosoftGraphWebApplication>]: webApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[HomePageUrl <String>]: Home page or landing page of the application.

[ImplicitGrantSetting <IMicrosoftGraphImplicitGrantSettings>]: implicitGrantSettings

[(Any) <Object>]: This indicates any property can be added to this object.

[EnableAccessTokenIssuance <Boolean?>]: Specifies whether this web application can request an access token using the OAuth 2.0 implicit flow.

[EnableIdTokenIssuance <Boolean?>]: Specifies whether this web application can request an ID token using the OAuth 2.0 implicit flow.

[LogoutUrl <String>]: Specifies the URL that will be used by Microsoft's authorization service to logout an user using front-channel, back-channel or SAML

logout protocols.

[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access

tokens are sent.

[DataType <String>]: Specifies the data type of the value the extension property can hold. Following values are supported. Not nullable. Binary - 256 bytes

maximumBooleanDateTime - Must be specified in ISO 8601 format. Will be stored in UTC.Integer - 32-bit value.LargeInteger - 64-bit value.String - 256 characters

maximum

[Name <String>]: Name of the extension property. Not nullable.

[TargetObject <String[]>]: Following values are supported. Not nullable. UserGroupOrganizationDeviceApplication

[Description <String>]: Description for this policy.

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy.

The syntax for the definition differs

for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be activated

as the organization default. Optional, default value is false.

[AccountEnabled <Boolean?>]: true if the service principal account is enabled; otherwise, false. Supports $filter (eq, ne, NOT, in).

[AddIn <IMicrosoftGraphAddIn[]>]: Defines custom behavior that a consuming service can use to call an app in specific contexts. For example, applications that

can render file streams may set the addIns property for its 'FileHandler' functionality. This will let services like Microsoft 365 call the application in the

context of a document the user is working on.

[AlternativeName <String[]>]: Used to retrieve service principals by subscription, identify resource group and full resource ids for managed identities.

Supports $filter (eq, NOT, ge, le, startsWith).

[AppDescription <String>]: The description exposed by the associated application.

[AppDisplayName <String>]: The display name exposed by the associated application.

[AppId <String>]: The unique identifier for the associated application (its appId property).

[AppOwnerOrganizationId <String>]: Contains the tenant id where the application is registered. This is applicable only to service principals backed by

applications.Supports $filter (eq, ne, NOT, ge, le).

[AppRole <IMicrosoftGraphAppRole[]>]: The roles exposed by the application which this service principal represents. For more information see the appRoles

property definition on the application entity. Not nullable.

[AppRoleAssignedTo <IMicrosoftGraphAppRoleAssignment[]>]: App role assignments for this app or service, granted to users, groups, and other service

principals.Supports $expand.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AppRoleId <String>]: The identifier (id) for the app role which is assigned to the principal. This app role must be exposed in the appRoles property on the

resource application's service principal (resourceId). If the resource application has not declared any app roles, a default app role ID of

00000000-0000-0000-0000-000000000000 can be specified to signal that the principal is assigned to the resource app without any specific app roles. Required on

create.

[PrincipalId <String>]: The unique identifier (id) for the user, group or service principal being granted the app role. Required on create.

[ResourceDisplayName <String>]: The display name of the resource app's service principal to which the assignment is made.

[ResourceId <String>]: The unique identifier (id) for the resource service principal for which the assignment is made. Required on create. Supports $filter

(eq only).

[AppRoleAssignment <IMicrosoftGraphAppRoleAssignment[]>]: App role assignment for another app or service, granted to this service principal. Supports $expand.

[AppRoleAssignmentRequired <Boolean?>]: Specifies whether users or other service principals need to be granted an app role assignment for this service

principal before users can sign in or apps can get tokens. The default value is false. Not nullable. Supports $filter (eq, ne, NOT).

[ClaimsMappingPolicy <IMicrosoftGraphClaimsMappingPolicy[]>]: The claimsMappingPolicies assigned to this service principal. Supports $expand.

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition

differs for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be

activated as the organization default. Optional, default value is false.

[Description <String>]: Description for this policy.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[DelegatedPermissionClassification <IMicrosoftGraphDelegatedPermissionClassification[]>]: The permission classifications for delegated permissions exposed by

the app that this service principal represents. Supports $expand.

[Classification <String>]: permissionClassificationType

[PermissionId <String>]: The unique identifier (id) for the delegated permission listed in the

publishedPermissionScopes collection of the servicePrincipal.

Required on create. Does not support $filter.

[PermissionName <String>]: The claim value (value) for the delegated permission listed in the publishedPermissionScopes collection of the servicePrincipal.

Does not support $filter.

[Description <String>]: Free text field to provide an internal end-user facing description of the service principal. End-user portals such MyApps will display

the application description in this field. The maximum allowed size is 1024 characters. Supports $filter (eq, ne, NOT, ge, le, startsWith) and $search.

[DisabledByMicrosoftStatus <String>]: Specifies whether Microsoft has disabled the registered application. Possible values are: null (default value),

NotDisabled, and DisabledDueToViolationOfServicesAgreement (reasons may include suspicious, abusive, or malicious activity, or a violation of the Microsoft

Services Agreement). Supports $filter (eq, ne, NOT).

[Endpoint <IMicrosoftGraphEndpoint[]>]: Endpoints available for discovery. Services like Sharepoint populate this property with a tenant specific SharePoint

endpoints that other applications can discover and use in their experiences.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[FederatedIdentityCredentials <IMicrosoftGraphFederatedIdentityCredential[]>]:

[HomeRealmDiscoveryPolicy <IMicrosoftGraphHomeRealmDiscoveryPolicy[]>]: The homeRealmDiscoveryPolicies assigned to this service principal. Supports $expand.

[Homepage <String>]: Home page or landing page of the application.

[Info <IMicrosoftGraphInformationalUrl>]: informationalUrl

[KeyCredentials <IMicrosoftGraphKeyCredential[]>]: The collection of key credentials associated with the service principal. Not nullable. Supports $filter

(eq, NOT, ge, le).

[LoginUrl <String>]: Specifies the URL where the service provider redirects the user to Azure AD to authenticate. Azure AD uses the URL to launch the

application from Microsoft 365 or the Azure AD My Apps. When blank, Azure AD performs IdP-initiated sign-on for applications configured with SAML-based single

sign-on. The user launches the application from Microsoft 365, the Azure AD My Apps, or the Azure AD SSO URL.

[LogoutUrl <String>]: Specifies the URL that will be used by Microsoft's authorization service to logout an user using

OpenId Connect front-channel,

back-channel or SAML logout protocols.

[Note <String>]: Free text field to capture information about the service principal, typically used for operational purposes. Maximum allowed size is 1024

characters.

[NotificationEmailAddress <String[]>]: Specifies the list of email addresses where Azure AD sends a notification when the active certificate is near the

expiration date. This is only for the certificates used to sign the SAML token issued for Azure AD Gallery applications.

[Oauth2PermissionScope <IMicrosoftGraphPermissionScope[]>]: The delegated permissions exposed by the application. For more information see the

oauth2PermissionScopes property on the application entity's api property. Not nullable.

[PasswordCredentials <IMicrosoftGraphPasswordCredential[]>]: The collection of password credentials associated with the service principal. Not nullable.

[PreferredSingleSignOnMode <String>]: Specifies the single sign-on mode configured for this application. Azure AD uses the preferred single sign-on mode to

launch the application from Microsoft 365 or the Azure AD My Apps. The supported values are password, saml, notSupported, and oidc.

[PreferredTokenSigningKeyThumbprint <String>]: Reserved for internal use only. Do not write or otherwise rely on this property. May be removed in future

versions.

[ReplyUrl <String[]>]: The URLs that user tokens are sent to for sign in with the associated application, or the redirect URIs that OAuth 2.0 authorization

codes and access tokens are sent to for the associated application. Not nullable.

[SamlSingleSignOnSetting <IMicrosoftGraphSamlSingleSignOnSettings>]: samlSingleSignOnSettings

[(Any) <Object>]: This indicates any property can be added to this object.

[RelayState <String>]: The relative URI the service provider would redirect to after completion of the single sign-on flow.

[ServicePrincipalName <String[]>]: Contains the list of identifiersUris, copied over from the associated application. Additional values can be added to hybrid

applications. These values can be used to identify the permissions exposed by this app within Azure AD. For example,Client apps can specify a resource URI which

is based on the values of this property to acquire an access token, which is the URI returned in the 'aud' claim.The any operator is required for filter

expressions on multi-valued properties. Not nullable. Supports $filter (eq, NOT, ge, le, startsWith).

[ServicePrincipalType <String>]: Identifies if the service principal represents an application or a managed identity. This is set by Azure AD internally. For

a service principal that represents an application this is set as Application. For a service principal that represent a managed identity this is set as

ManagedIdentity.

[Tag <String[]>]: Custom strings that can be used to categorize and identify the service principal. Not nullable. Supports $filter (eq, NOT, ge, le,

startsWith).

[TokenEncryptionKeyId <String>]: Specifies the keyId of a public key from the keyCredentials collection. When configured, Azure AD issues tokens for this

application encrypted using the key specified by this property. The application code that receives the encrypted token must use the matching private key to

decrypt the token before it can be used for the signed-in user.

[TokenIssuancePolicy <IMicrosoftGraphTokenIssuancePolicy[]>]: The tokenIssuancePolicies assigned to this service principal. Supports $expand.

[TokenLifetimePolicy <IMicrosoftGraphTokenLifetimePolicy[]>]: The tokenLifetimePolicies assigned to this service principal. Supports $expand.

[TransitiveMemberOf <IMicrosoftGraphDirectoryObject[]>]:

[AppRoleId <String>]: The identifier (id) for the app role which is assigned to the principal. This app role must be exposed in the appRoles property on the

resource application's service principal (resourceId). If the resource application has not declared any app roles, a default app role ID of

00000000-0000-0000-0000-000000000000 can be specified to signal that the principal is assigned to the resource app without any specific app roles. Required on

create.

[CreatedDateTime <DateTime?>]: The time when the app role assignment was created.The Timestamp type represents date and time information using ISO 8601 format

and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[PrincipalDisplayName <String>]: The display name of the user, group, or service principal that was granted the app role assignment. Read-only. Supports

$filter (eq and startswith).

[PrincipalId <String>]: The unique identifier (id) for the user, group or service principal being granted the app role.

Required on create.

[PrincipalType <String>]: The type of the assigned principal. This can either be User, Group or ServicePrincipal. Read-only.

[ResourceDisplayName <String>]: The display name of the resource app's service principal to which the assignment is made.

[ResourceId <String>]: The unique identifier (id) for the resource service principal for which the assignment is made. Required on create. Supports $filter

(eq only).

[AppRoleAssignment <IMicrosoftGraphAppRoleAssignmentAutoGenerated[]>]: Represents the app roles a group has been granted for an application. Supports $expand.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AppRoleId <String>]: The identifier (id) for the app role which is assigned to the principal. This app role must be exposed in the appRoles property on the

resource application's service principal (resourceId). If the resource application has not declared any app roles, a default app role ID of

00000000-0000-0000-0000-000000000000 can be specified to signal that the principal is assigned to the resource app without any specific app roles. Required on

create.

[CreatedDateTime <DateTime?>]: The time when the app role assignment was created.The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[PrincipalDisplayName <String>]: The display name of the user, group, or service principal that was granted the app role assignment. Read-only. Supports

$filter (eq and startswith).

[PrincipalId <String>]: The unique identifier (id) for the user, group or service principal being granted the app role. Required on create.

[PrincipalType <String>]: The type of the assigned principal. This can either be User, Group or ServicePrincipal. Read-only.

[ResourceDisplayName <String>]: The display name of the resource app's service principal to which the assignment is made.

[ResourceId <String>]: The unique identifier (id) for the resource service principal for which the assignment is made. Required on create. Supports $filter

(eq only).

[Classification <String>]: Describes a classification for the group (such as low, medium or high business impact). Valid values for this property are defined

by creating a ClassificationList setting value, based on the template definition.Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith).

[CreatedOnBehalfOf <IMicrosoftGraphDirectoryObject>]: Represents an Azure Active Directory object. The directoryObject type is the base type for many other

directory entity types.

[Description <String>]: An optional description for the group. Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith) and $search.

[GroupType <String[]>]: Specifies the group type and its membership. If the collection contains Unified, the group is a Microsoft 365 group; otherwise, it's

either a security group or distribution group. For details, see groups overview.If the collection includes DynamicMembership, the group has dynamic membership;

otherwise, membership is static. Returned by default. Supports $filter (eq, NOT).

[HasMembersWithLicenseError <Boolean?>]: Indicates whether there are members in this group that have license errors from its group-based license assignment.

This property is never returned on a GET operation. You can use it as a $filter argument to get groups that have members with license errors (that is, filter for

this property being true). Supports $filter (eq).

[IsArchived <Boolean?>]:

[IsAssignableToRole <Boolean?>]: Indicates whether this group can be assigned to an Azure Active Directory role.This property can only be set while creating

the group and is immutable. If set to true, the securityEnabled property must also be set to true and the group cannot be a dynamic group (that is, groupTypes

cannot contain DynamicMembership). Only callers in Global administrator and Privileged role administrator roles can set this property. The caller must also be

assigned the Directory.AccessAsUser.All permission to set this property. For more, see Using a group to manage Azure AD role assignmentsReturned by default.

Supports $filter (eq, ne, NOT).

[MailEnabled <Boolean?>]: Specifies whether the group is mail-enabled. Returned by default. Supports $filter (eq, ne, NOT).

[MailNickname <String>]: The mail alias for the group, unique in the organization. This property must be specified

when a group is created. These characters

cannot be used in the mailNickName: @()/[]';:.<>,SPACE. Returned by default. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[MembershipRule <String>]: The rule that determines members for this group if the group is a dynamic group (groupTypes contains DynamicMembership). For more

information about the syntax of the membership rule, see Membership Rules syntax. Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith).

[MembershipRuleProcessingState <String>]: Indicates whether the dynamic membership processing is on or paused. Possible values are On or Paused. Returned by

default. Supports $filter (eq, ne, NOT, in).

[PermissionGrant <IMicrosoftGraphResourceSpecificPermissionGrant[]>]: The permissions that have been granted for a group to a specific application. Supports

$expand.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[ClientAppId <String>]: ID of the service principal of the Azure AD app that has been granted access. Read-only.

[ClientId <String>]: ID of the Azure AD app that has been granted access. Read-only.

[Permission <String>]: The name of the resource-specific permission. Read-only.

[PermissionType <String>]: The type of permission. Possible values are: Application, Delegated. Read-only.

[ResourceAppId <String>]: ID of the Azure AD app that is hosting the resource. Read-only.

[PreferredDataLocation <String>]: The preferred data location for the group. For more information, see OneDrive Online Multi-Geo. Returned by default.

[PreferredLanguage <String>]: The preferred language for a Microsoft 365 group. Should follow ISO 639-1 Code; for example 'en-US'. Returned by default.

Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[SecurityEnabled <Boolean?>]: Specifies whether the group is a security group. Returned by default. Supports $filter (eq, ne, NOT, in).

[SecurityIdentifier <String>]: Security identifier of the group, used in Windows scenarios. Returned by default.

[Theme <String>]: Specifies a Microsoft 365 group's color theme. Possible values are Teal, Purple, Green, Blue, Pink, Orange or Red. Returned by default.

[Visibility <String>]: Specifies the group join policy and group content visibility for groups. Possible values are: Private, Public, or Hiddenmembership.

Hiddenmembership can be set only for Microsoft 365 groups, when the groups are created. It can't be updated later.

Other values of visibility can be updated after

group creation. If visibility value is not specified during group creation on Microsoft Graph, a security group is created as Private by default and Microsoft 365

group is Public. See group visibility options to learn more. Returned by default.

[ClientAppId <String>]: ID of the service principal of the Azure AD app that has been granted access. Read-only.

[ClientId <String>]: ID of the Azure AD app that has been granted access. Read-only.

[Permission <String>]: The name of the resource-specific permission. Read-only.

[PermissionType <String>]: The type of permission. Possible values are: Application, Delegated. Read-only.

[ResourceAppId <String>]: ID of the Azure AD app that is hosting the resource. Read-only.

[AccountEnabled <Boolean?>]: true if the account is enabled; otherwise, false. This property is required when a user is created. Supports $filter (eq, ne,

NOT, and in).

[AgeGroup <String>]: Sets the age group of the user. Allowed values: null, minor, notAdult and adult. Refer to the legal age group property definitions for

further information. Supports $filter (eq, ne, NOT, and in).

[ApproximateLastSignInDateTime <DateTime?>]: The timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For

example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only. Supports $filter (eq, ne, not, ge, le, and eq on null values) and $orderBy.

[City <String>]: The city in which the user is located. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[CompanyName <String>]: The company name which the user is associated. This property can be useful for describing the company that an external user comes

from. The maximum length of the company name is 64 characters.Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[ComplianceExpirationDateTime <DateTime?>]: The timestamp when the device is no longer deemed compliant. The timestamp type represents date and time

information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[ConsentProvidedForMinor <String>]: Sets whether consent has been obtained for minors. Allowed values: null, granted, denied and notRequired. Refer to the

legal age group property definitions for further information. Supports $filter (eq, ne, NOT, and in).

[Country <String>]: The country/region in which the user is located; for example, US or UK. Maximum length is 128 characters. Supports $filter (eq, ne, NOT,

ge, le, in, startsWith).

[Department <String>]: The name for the department in which the user works. Maximum length is 64 characters.Supports $filter (eq, ne, NOT , ge, le, and in

operators).

[DeviceVersion <Int32?>]: For internal use only.

[EmployeeHireDate <DateTime?>]: The date and time when the user was hired or will start work in case of a future hire. Supports $filter (eq, ne, NOT , ge, le,

in).

[EmployeeId <String>]: The employee identifier assigned to the user by the organization. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[EmployeeOrgData <IMicrosoftGraphEmployeeOrgData>]: employeeOrgData

[EmployeeType <String>]: Captures enterprise worker type. For example, Employee, Contractor, Consultant, or Vendor. Supports $filter (eq, ne, NOT , ge, le,

in, startsWith).

[ExternalUserState <String>]: For an external user invited to the tenant using the invitation API, this property represents the invited user's invitation

status. For invited users, the state can be PendingAcceptance or Accepted, or null for all other users. Supports $filter (eq, ne, NOT , in).

[ExternalUserStateChangeDateTime <DateTime?>]: Shows the timestamp for the latest change to the externalUserState property. Supports $filter (eq, ne, NOT ,

in).

[FaxNumber <String>]: The fax number of the user. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[GivenName <String>]: The given name (first name) of the user. Maximum length is 64 characters. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[Identity <IMicrosoftGraphObjectIdentity[]>]: Represents the identities that can be used to sign in to this user account. An identity can be provided by

Microsoft (also known as a local account), by organizations, or by social identity providers such as Facebook, Google, and Microsoft, and tied to a user account.

May contain multiple items with the same signInType value. Supports $filter (eq) only where the signInType is not userPrincipalName.

[IsResourceAccount <Boolean?>]: Do not use ??" reserved for future use.

[JobTitle <String>]: The user's job title. Maximum length is 128 characters. Supports $filter (eq, ne, NOT , ge, le, in, startsWith).

[Mail <String>]: The SMTP address for the user, for example, admin@contoso.com. Changes to this property will also update the user's proxyAddresses collection

to include the value as an SMTP address. While this property can contain accent characters, using them can cause access issues with other Microsoft applications

for the user. Supports $filter (eq, ne, NOT, ge, le, in, startsWith, endsWith).

[MailNickname <String>]: The mail alias for the user. This property must be specified when a user is created. Maximum length is 64 characters. Supports

$filter (eq, ne, NOT, ge, le, in, startsWith).

[Manager <IMicrosoftGraphDirectoryObject>]: Represents an Azure Active Directory object. The directoryObject type is the base type for many other directory

entity types.

[OfficeLocation <String>]: The office location in the user's place of business. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[OnPremisesImmutableId <String>]: This property is used to associate an on-premises Active Directory user account to their Azure AD user object. This property

must be specified when creating a new user account in the Graph if you are using a federated domain for the user's userPrincipalName (UPN) property. NOTE: The $

and _ characters cannot be used when specifying this property. Returned only on $select. Supports $filter (eq, ne, NOT, ge, le, in)..

[OnPremisesLastSyncDateTime <DateTime?>]: The last time at which the object was synced with the on-premises directory. The Timestamp type represents date and

time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z Read-only. Supports $filter

(eq, ne, not, ge, le, in).

[OnPremisesSyncEnabled <Boolean?>]: true if this object is synced from an on-premises directory; false if this object was originally synced from an

on-premises directory but is no longer synced; null if this object has never been synced from an on-premises directory (default). Read-only. Supports $filter (eq,

ne, not, in, and eq on null values).

[OperatingSystem <String>]: Operating system of the device. Windows, iOS, etc. This property is read-only.

[OperatingSystemVersion <String>]: Operating system version of the device. Required. Supports $filter (eq, ne, not, ge, le, startsWith, and eq on null values).

[OtherMail <String[]>]: A list of additional email addresses for the user; for example: ['bob@contoso.com', 'Robert@fabrikam.com'].NOTE: While this property

can contain accent characters, they can cause access issues to first-party applications for the user.Supports $filter (eq, NOT, ge, le, in, startsWith).

[PasswordPolicy <String>]: Specifies password policies for the user. This value is an enumeration with one possible value being DisableStrongPassword, which

allows weaker passwords than the default policy to be specified. DisablePasswordExpiration can also be specified. The two may be specified together; for example:

DisablePasswordExpiration, DisableStrongPassword.Supports $filter (ne, NOT).

[PasswordProfile <IMicrosoftGraphPasswordProfile>]: passwordProfile

[(Any) <Object>]: This indicates any property can be added to this object.

[ForceChangePasswordNextSignIn <Boolean?>]: true if the user must change her password on the next login; otherwise false. If not set, default is false.

NOTE: For Azure B2C tenants, set to false and instead use custom policies and user flows to force password reset at first sign in. See Force password reset at

first logon.

[ForceChangePasswordNextSignInWithMfa <Boolean?>]: If true, at next sign-in, the user must perform a multi-factor authentication (MFA) before being forced

to change their password. The behavior is identical to forceChangePasswordNextSignIn except that the user is required to first perform a multi-factor

authentication before password change. After a password change, this property will be automatically reset to false. If not set, default is false.

[Password <String>]: The password for the user. This property is required when a user is created. It can be updated, but the user will be required to change

the password on the next login. The password must satisfy minimum requirements as specified by the user??Ts passwordPolicies property. By default, a strong

password is required.

[PhysicalId <String[]>]: For internal use only. Not nullable. Supports $filter (eq, not, ge, le, startsWith).

[PostalCode <String>]: The postal code for the user's postal address. The postal code is specific to the user's country/region. In the United States of

America, this attribute contains the ZIP code. Maximum length is 40 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[PreferredLanguage <String>]: The preferred language for the user. Should follow ISO 639-1 Code; for example

en-US. Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[ShowInAddressList <Boolean?>]: true if the Outlook global address list should contain this user, otherwise false. If not set, this will be treated as true.

For users invited through the invitation manager, this property will be set to false. Supports $filter (eq, ne, NOT, in).

[State <String>]: The state or province in the user's address. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[StreetAddress <String>]: The street address of the user's place of business. Maximum length is 1024 characters. Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[Surname <String>]: The user's surname (family name or last name). Maximum length is 64 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[TrustType <String>]: Type of trust for the joined device. Read-only. Possible values: Workplace (indicates bring your own personal devices), AzureAd (Cloud

only joined devices), ServerAd (on-premises domain joined devices joined to Azure AD). For more details, see Introduction to device management in Azure Active

Directory

[UsageLocation <String>]: A two letter country code (ISO standard 3166). Required for users that will be assigned licenses due to legal requirement to check

for availability of services in countries. Examples include: US, JP, and GB. Not nullable. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[UserPrincipalName <String>]: The user principal name (UPN) of the user. The UPN is an Internet-style login name for the user based on the Internet standard

RFC 822. By convention, this should map to the user's email name. The general format is alias@domain, where domain must be present in the tenant's collection of

verified domains. This property is required when a user is created. The verified domains for the tenant can be accessed from the verifiedDomains property of

organization.NOTE: While this property can contain accent characters, they can cause access issues to first-party applications for the user. Supports $filter (eq,

ne, NOT, ge, le, in, startsWith, endsWith) and $orderBy.

[UserType <String>]: A string value that can be used to classify user types in your directory, such as Member and Guest. Supports $filter (eq, ne, NOT, in,).

[OfficeLocation <String>]: The office location in the user's place of business. Maximum length is 128 characters.

Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[OnPremisesImmutableId <String>]: This property is used to associate an on-premises Active Directory user account to their Azure AD user object. This property

must be specified when creating a new user account in the Graph if you are using a federated domain for the user's userPrincipalName (UPN) property. NOTE: The $

and _ characters cannot be used when specifying this property. Returned only on $select. Supports $filter (eq, ne, NOT, ge, le, in)..

[OnPremisesLastSyncDateTime <DateTime?>]: The last time at which the object was synced with the on-premises directory. The Timestamp type represents date and

time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z Read-only. Supports $filter

(eq, ne, not, ge, le, in).

[OnPremisesSyncEnabled <Boolean?>]: true if this object is synced from an on-premises directory; false if this object was originally synced from an on-premises

directory but is no longer synced; null if this object has never been synced from an on-premises directory (default). Read-only. Supports $filter (eq, ne, not,

in, and eq on null values).

[OperatingSystem <String>]: Operating system of the device. Windows, iOS, etc. This property is read-only.

[OperatingSystemVersion <String>]: Operating system version of the device. Required. Supports $filter (eq, ne, not, ge, le, startsWith, and eq on null values).

[OtherMail <String[]>]: A list of additional email addresses for the user; for example: ['bob@contoso.com', 'Robert@fabrikam.com'].NOTE: While this property can

contain accent characters, they can cause access issues to first-party applications for the user.Supports $filter (eq, NOT, ge, le, in, startsWith).

[PasswordPolicy <String>]: Specifies password policies for the user. This value is an enumeration with one possible value being DisableStrongPassword, which

allows weaker passwords than the default policy to be specified. DisablePasswordExpiration can also be specified. The two may be specified together; for example:

DisablePasswordExpiration, DisableStrongPassword.Supports $filter (ne, NOT).

[PasswordProfile <IMicrosoftGraphPasswordProfile>]: passwordProfile

[PhysicalId <String[]>]: For internal use only. Not nullable. Supports $filter (eq, not, ge, le, startsWith).

[PostalCode <String>]: The postal code for the user's postal address. The postal code is specific to the user's

country/region. In the United States of America,

this attribute contains the ZIP code. Maximum length is 40 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[PreferredLanguage <String>]: The preferred language for the user. Should follow ISO 639-1 Code; for example en-US. Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[ShowInAddressList <Boolean?>]: true if the Outlook global address list should contain this user, otherwise false. If not set, this will be treated as true. For

users invited through the invitation manager, this property will be set to false. Supports $filter (eq, ne, NOT, in).

[State <String>]: The state or province in the user's address. Maximum length is 128 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[StreetAddress <String>]: The street address of the user's place of business. Maximum length is 1024 characters. Supports $filter (eq, ne, NOT, ge, le, in,

startsWith).

[Surname <String>]: The user's surname (family name or last name). Maximum length is 64 characters. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[TrustType <String>]: Type of trust for the joined device. Read-only. Possible values: Workplace (indicates bring your own personal devices), AzureAd (Cloud

only joined devices), ServerAd (on-premises domain joined devices joined to Azure AD). For more details, see Introduction to device management in Azure Active

Directory

[UsageLocation <String>]: A two letter country code (ISO standard 3166). Required for users that will be assigned licenses due to legal requirement to check for

availability of services in countries. Examples include: US, JP, and GB. Not nullable. Supports $filter (eq, ne, NOT, ge, le, in, startsWith).

[UserPrincipalName <String>]: The user principal name (UPN) of the user. The UPN is an Internet-style login name for the user based on the Internet standard RFC

822. By convention, this should map to the user's email name. The general format is alias@domain, where domain must be present in the tenant's collection of

verified domains. This property is required when a user is created. The verified domains for the tenant can be accessed from the verifiedDomains property of

organization.NOTE: While this property can contain accent characters, they can cause access issues to first-party applications for the user. Supports $filter (eq,

ne, NOT, ge, le, in, startsWith, endsWith) and $orderBy.

[UserType <String>]: A string value that can be used to classify user types in your directory, such as Member and Guest. Supports $filter (eq, ne, NOT, in,).

---------- EXAMPLE 1 ----------

PS C:\>Remove-AzADUser -DisplayName $name

---------- EXAMPLE 2 ----------

PS C:\>Get-AzADUser -UserPrincipalName $id | Remove-AzADUser

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.resources/remove-azaduser