## **What is an Office 365 Tenant?**

Tenant is a term used for an Office 365 Organization. Each tenant has its own Azure AD and any services enabled for those users will tie back to the tenant. A user of Office 365 in the organization is a member of the tenant.

## **What is an Office 365 Guest Account?**

When enabled, an Office 365 user (in tenant) can:

* Invites someone external of the tenant to join a M365 group, e.g Microsoft Teams team, Planner, Form
* Shares files to someone external of the tenant specially via SharePoint or OneDrive for Business (which leverages Azure Active Directory B2B Collaboration)
* A “guest account” is automatically created in the tenant for the person that has been invited into the group or shared to.
* The guest account represents their activities and access on the tenant and controls the guest’s access.
* Guest accounts have a UPN in the format

**[username\_domain#EXT#@tenantname.onmicrosoft.com](mailto:%23)**

## **What are guest default permissions?**

According to Microsoft [**documentation**](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#compare-member-and-guest-default-permissions) [Jun 23 2020] the guest users have the following permissions to Azure AD:

| **Area** | **Guest user permissions** |
| --- | --- |
| Users and contacts | Read own properties. Read display name, email, sign in name, photo, user principal name, and user type **properties of other users and contacts**. Change own password |
| Groups | Read all **properties of groups**. Read non-hidden group memberships. Read hidden Office 365 group memberships for joined groups. Manage owned groups. Add guests to owned groups (if allowed). Delete owned groups. Restore owned Office 365 groups. Read **properties of groups they belong to**, including membership. |
| Applications | Read properties of registered and enterprise applications. Manage application properties, assignments, and credentials for owned applications. Delete owned applications. Restore owned applications |
| Devices | Delete owned devices |
| Directory | **Read display name and verified domains** |
| Roles and scopes | No permissions |
| Subscriptions | No permissions |
| Policies | No permissions |

* *A guest user****can retrieve information about another user by providing the User Principal Name or objectId****.*
* *A guest user****can read properties of groups they belong to****, including group membership, regardless of the Guest users’ permissions are limited setting.*
* *A guest****cannot view information about any other tenant objects****.*

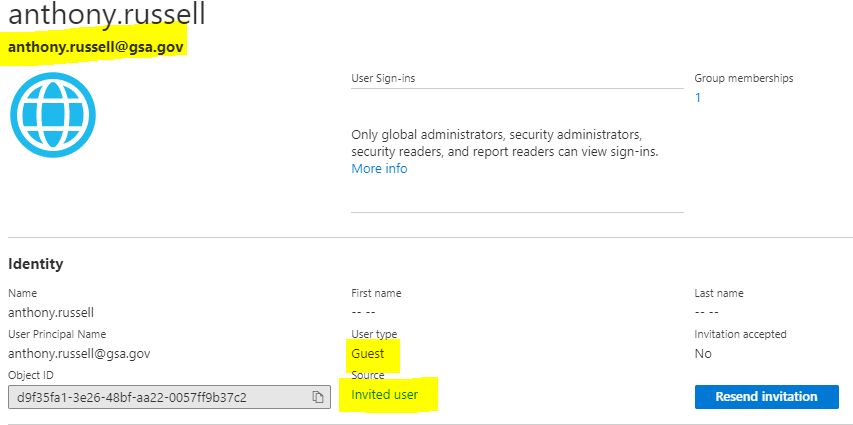
To sum up, guest users **CAN NOT list objects** (such as users or groups), but they **CAN read object properties**, as long as the id (or user name) of the object is known.

## **How can report on Office 365 Guest Accounts?**

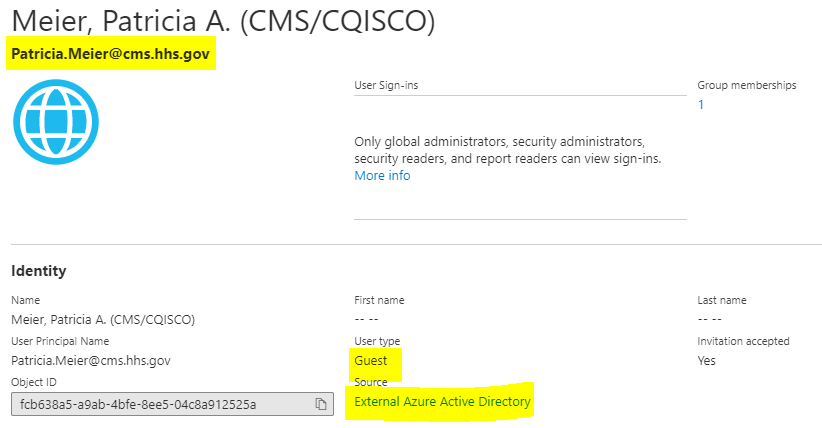
From the Azure Active Directory UI [https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/UsersManagementMenuBlade/AllUsers](https://portal.azure.com/%23blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/AllUsers)

Azure Active Directory portal will show the source of the user:

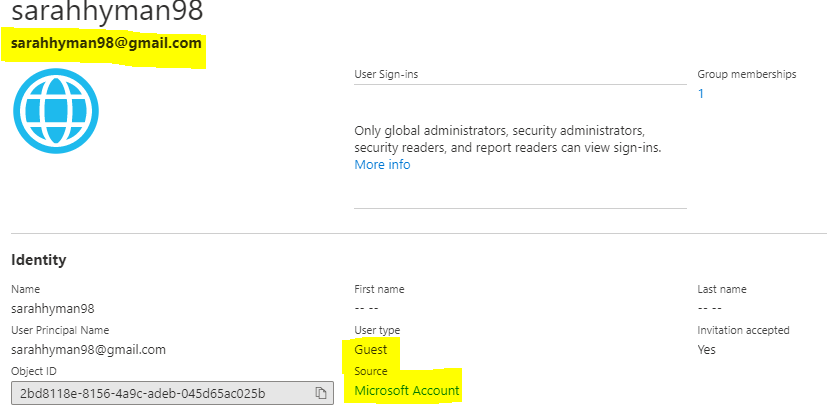
* Members
  + **Azure Active Directory**: This user belongs to the tenant and authenticates by using an Azure AD for this tenant
  + **Windows Server Active Directory**: This user is signed in from on-premises Active Directory that belongs to this organization.
* Guests
  + **Invited User**: This user has been invited but has not yet redeemed an invitation



* + **External Azure Active Directory**: This use is homed in an external Office 365 organization and authenticates by using an Azure AD account that belongs to the other organization.



* + **Microsoft account**: This user is homed in a Microsoft account (e.g the old LiveID or consumer accounts) and authenticates by using a Microsoft account.



## **Can a guest user leave the organization?**

A guest user can decide to leave an organization at any time if they no longer need to use apps from that organizations or maintain any association. A guest user can’t leave an organization if their account is disabled.

When a user leaves an organization, the user account is “soft deleted” in the directory. By default, the user object moves to the Deleted users’ area in Azure AD but isn’t permanently deleted for 30 days.

## **Report on which guests are in which M365 Groups?**

* Finds all guest accounts in the tenant using Graph API
* Look for its group membership by running the Get-Recipient cmdlet to check the account’s distinguished name against the membership of M365 groups.
* Writes the discovered information out to an array.
* After all guest accounts are processed, writes the contents of the array to a CSV file.

$token = Connect-NIHO365Graph -profilePath 'D:\Scripting\O365DevOps\Common\Config\PROFILE.psd1'

$GuestUsers = Get-NIHO365GuestUsers -AuthToken $token

$TenantName = "citspdev.onmicrosoft.com"

$appId = "986b8748-6f77-4d2c-a197-dd738b2d3119"

$thumprint = '01FE80EDA90C00BF58D36BD588CAC10915F39723'

Connect-ExchangeOnline -AppId $appId -Organization $TenantName -CertificateThumbprint $thumprint

$Report = [System.Collections.Generic.List[Object]]::new()

ForEach ($Guest in $GuestUsers) {

    #$AADAccountAge = ($Guest.RefreshTokensValidFromDateTime | New-TimeSpan).Days

    $AADAccountAge = ($Guest.createdDateTime | New-TimeSpan).Days

    Write-Host "Processing" $Guest.DisplayName

    $i = 0;

    $GroupNames = $Null

    $GroupIds = $Null

    # Find what Office 365 Groups the guest belongs to... if any

    $DN = (Get-Recipient -Identity $Guest.UserPrincipalName).DistinguishedName

    $GuestGroups = (Get-Recipient -Filter "Members -eq '$Dn'" -RecipientTypeDetails GroupMailbox | Select DisplayName, ExternalDirectoryObjectId)

    #$GuestGroups = (Get-EXORecipient -Filter "Members -eq '$Dn'" -RecipientTypeDetails GroupMailbox | Select DisplayName, ExternalDirectoryObjectId)

    If ($GuestGroups -ne $Null) {

        ForEach ($G in $GuestGroups) {

        If ($i -eq 0) {

            $GroupNames = $G.DisplayName;

            $GroupIds = $G.ExternalDirectoryObjectId

            $i++ }

        Else

        {

            $GroupNames = $GroupNames + "; " + $G.DisplayName

            $GroupIds = $GroupIds + "; " + $G.ExternalDirectoryObjectId

         }

    }}

    $ReportLine = [PSCustomObject]@{

        UPN     = $Guest.UserPrincipalName

        Name    = $Guest.DisplayName

        Age     = $AADAccountAge

        Created = $Guest.createdDateTime

        GroupIds = $GroupIds

        Groups  = $GroupNames

        DN      = $DN}

    $Report.Add($ReportLine) }

Disconnect-ExchangeOnline -Confirm:$false

$Report | Sort Name | Export-CSV -NoTypeInformation D:\Scripting\O365DevOps\Common\Data\Other\GuestAccounts.csv

## **Discover who creates guest account in Office applications?**

Office 365 won’t tell you who did what to create a new guest account, but the answer is available if you go looking in the Office 365 audit log. The audit log holds a lot of information gathered from many different parts of Office 365. The trick in finding what we’re looking for is to focus in on the actions people take that result in a new guest account being created.

The first action we need to look for is when a guest is added to an Office 365 group in an application like Outlook, Teams, Planner, or Yammer. When this happens, Azure B2B collaboration creates and sends an invitation to the guest to notify them that they have been granted access to an application. If the guest account doesn’t already exist in Azure Active Directory, it is created.

Office 365 audit log helps us understand how and when guest accounts are created.

* “Add User” event is captured when a new Azure Active Directory account is created. This event tells us the name of the guest user and who created them

$Records = (Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate -Operations "Add User" -ResultSize 2000 -Formatted)

* “Add member to group” event find the name of the group the guest joined.

$Records = (Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate -Operations "Add Member to Group" -ResultSize 2000 -Formatted)

* Validate whether the guest is a new or existing account by checking “createdDateTime” of guest user: if it holds the same timestamp as when the user joined the group => new guest account, else existing account.

**Note: Turn on audit log is required:** Go to the [Security & Compliance Center](https://protection.office.com)> In the Security & Compliance Center, go to Search > Audit log search

## **Identifying obsolete Guest accounts in an Office 365 Tenant?**

How to figure out if a guest account is active

## **Report Old Guest Accounts and their membership of M365 Groups?**

## **Control lifecycle Guest account through PowerShell?**