Manage who can create Office 365 Groups

https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide

Manage who can create Office 365 Groups

03/02/2020

5 minutes to read

Because it's so easy for users to create Office 365 Groups, you aren't inundated with requests to create them on behalf of other people. Depending on your business, however, you might want to control who has the ability to create groups.

This article explains how to disable the ability to create groups in all Office 365 services that use groups:

Outlook

SharePoint

Yammer

Microsoft Teams

Microsoft Stream

StaffHub

Planner

PowerBI

Roadmap

You can restrict Office 365 Group creation to the members of a particular security group. To configure this, you use Windows PowerShell. This article walks you through the needed steps.

The steps in this article won't prevent members of certain roles from creating Groups. Office 365 Global admins can create Groups via any means, such as the Microsoft 365 admin center, Planner, Teams, Exchange, and SharePoint Online. Other roles can create Groups via limited means, listed below.

Exchange Administrator: Exchange Admin center, Azure AD

Partner Tier 1 Support: Microsoft 365 Admin center, Exchange Admin center, Azure AD

Partner Tier 2 Support: Microsoft 365 Admin center, Exchange Admin center, Azure AD

Directory Writers: Azure AD

SharePoint Administrator: SharePoint Admin center, Azure AD

Teams Service Administrator: Teams Admin center, Azure AD

User Management Administrator: Microsoft 365 Admin center, Yammer, Azure AD

If you're a member of one of these roles, you can create Office 365 Groups for restricted users, and then assign the user as the owner of the group. Users that have this role are able to create connected groups in Yammer, regardless of any PowerShell settings that might prevent creation.

Licensing requirements

To manage who creates Groups, the following people need Azure AD Premium licenses or Azure AD Basic EDU licenses assigned to them:

The admin who configures these group creation settings

The members of the security group who are allowed to create Groups

The following people don't need Azure AD Premium or Azure AD Basic EDU licenses assigned to them:

People who are members of Office 365 groups and who don't have the ability to create other groups.

Step 1: Create a security group for users who need to create Office 365 Groups

Only one security group in your organization can be used to control who is able to create Groups. But, you can nest other security groups as members of this group. For example, the group named Allow Group Creation is the designated security group, and the groups named Microsoft Planner Users and Exchange Online Users are members of that group.

Admins in the roles listed above do not need to be members of this group: they retain their ability to create groups.

Important

Be sure to use a security group to restrict who can create groups. If you try to use an Office 365 Group, members won't be able to create a group from SharePoint because it checks for a security group.

In the admin center, go to the Groups > Groups page.

Click on Add a Group.

Choose Security as the group type. Remember the name of the group! You'll need it later.

Finish setting up the security group, adding people or other security groups who you want to be able to create Groups in your org.

For detailed instructions, see Create, edit, or delete a security group in the Microsoft 365 admin center.

Step 2: Install the preview version of the Azure Active Directory PowerShell for Graph

These procedures require the preview version of the Azure Active Directory PowerShell for Graph. The GA version will not work.

Important

You cannot install both the preview and GA versions on the same computer at the same time. You can install the module on Windows 10, Windows Server 2016.

As a best practice, we recommend always staying current: uninstall the old AzureADPreview or old AzureAD version and get the latest one.

In your search bar, type Windows PowerShell.

Right-click on Windows PowerShell and select Run as Administrator.

Open PowerShell as "Run as administrator."

Set the policy to RemoteSigned by using Set-ExecutionPolicy.

Copy

```
Set-ExecutionPolicy RemoteSigned
```

Check installed module:

Copy

```
Get-InstalledModule -Name "AzureAD*"
```

To uninstall a previous version of AzureADPreview or AzureAD, run this command:

Copy

Uninstall-Module AzureADPreview

or

Copy

Uninstall-Module AzureAD

To install the latest version of AzureADPreview, run this command:

Copy

Install-Module AzureADPreview

At the message about an untrusted repository, type Y. It will take a minute or so for the new module to install.

Leave the PowerShell window open for Step 3, below.

Step 3: Run PowerShell commands

Copy the script below into a text editor, such as Notepad, or the Windows PowerShell ISE.

Replace <SecurityGroupName> with the name of the security group that you created. For example:

$GroupName = "Group Creators"

Save the file as GroupCreators.ps1.

In the PowerShell window, navigate to the location where you saved the file (type "CD ").

Run the script by typing:

.\GroupCreators.ps1

and sign in with your administrator account when prompted.

PowerShell

Copy

```
$GroupName = "<SecurityGroupName>"

$AllowGroupCreation = "False"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id

if(!$settingsObjectID)

{

  $template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}

    $settingsCopy = $template.CreateDirectorySetting()
```

```
    New-AzureADDirectorySetting -DirectorySetting $settingsCopy

    $settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id

}



$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID

$settingsCopy["EnableGroupCreation"] = $AllowGroupCreation



if($GroupName)

{

$settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid

}

 else {

$settingsCopy["GroupCreationAllowedGroupId"] = $GroupName

}

Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy



(Get-AzureADDirectorySetting -Id $settingsObjectID).Values
```

The last line of the script will display the updated settings:

This is what your settings will look like when you're done.

If in the future you want to change which security group is used, you can rerun the script with the name of the new security group.

If you want to turn off the group creation restriction and again allow all users to create groups, set $GroupName to "" and $AllowGroupCreation to "True" and rerun the script.

Step 4: Verify that it works

Sign in to Office 365 with a user account of someone who should NOT have the ability to create groups. That is, they are not a member of the security group you created or an administrator.

Select the Planner tile.

In Planner, select New Plan in the left navigation to create a plan.

You should get a message that plan and group creation is disabled.

Try the same procedure again with a member of the security group.

Note

If members of the security group aren't able to create groups, check that they aren't being blocked through their OWA mailbox policy.

Related articles

Getting started with Office 365 PowerShell

Set up self-service group management in Azure Active Directory

Set-ExecutionPolicy

Azure Active Directory cmdlets for configuring group settings

Revision #1
Created 23 December 2023 04:38:00 by ColtM
Updated 13 June 2024 01:28:01 by ColtM