

# FAQ: OFFICE 365 GROUPS

**Answers to 13 questions that will help you better manage and secure your Office 365 environment**

Quest<sup>®</sup>





## Introduction

Whether your organization has recently completed a migration to Office 365 and you're looking to get started on the right foot with Office 365 groups, or you've been in the cloud for a while but are encountering issues with Office 365 groups, this FAQ is for you. Quest experts answer a baker's dozen of the most common questions about creating, managing and deleting Office 365 groups, so you can make the most of your cloud investment.

# 1. What's the difference between an Office 365 group and an Exchange distribution list (DL)?

Both Exchange distribution lists and Office 365 groups enable you to send email to many recipients at once. So what's the difference? Do you need both?

Exchange DLs have been around a long time and are used as a matter of course in most organizations. Their sole purpose is to provide a convenient way to send email to a set of recipients without having to type all their email addresses each time. For example, managers often create a DL for their direct reports, and HR might create one DL for regular employees and a separate DL for contractors. Distribution lists are available in both on-premises Exchange and Exchange Online.

Distributions lists are for email only; Office 365 groups have far broader reach.

An Office 365 group has far broader reach than a DL. The group itself is nothing more than an Azure AD object that contains members. But when

a group is created, the Office 365 service spins up resources in the associated Office 365 workloads, and members of the group automatically have permissions to access those resources. In particular, each Office 365 group has a shared mailbox and calendar. Emails sent to the group are not only distributed to all members, as they would with an Exchange DL, they are also stored in a separate mailbox.

A group also has an associated SharePoint site collection, a OneNote notebook, and shared group resources in applications like Microsoft Teams, Yammer, Planner and PowerBI. Members can access all of the resources and participate in all the Office 365 workloads attached to the group. Of course, unlike distribution lists, Office 365 groups are a cloud-only construct.

Another important difference between Office 365 groups and Exchange distributions lists is that all the collaboration that happens in an Office 365 group is persistent — if a new member is added to the group, they'll have access to all the content that has been posted since the inception of the group, including but not limited to the content of the group's mailbox. If a new member is added to a DL, on the other hand, they'll only get email communication from that point forward.

So, do you need both? Almost certainly. Exchange DLs are widely used because they are so convenient, and often the limited functionality they provide is exactly what you want — to send email and nothing more. When you create an Office 365 group, you are creating resources and data that need to be secured and managed, so you should create Office 365 groups only when you need the collaboration benefits, not just to send email.



## 2. What's the difference between an Office 365 group and a Team?

Microsoft Teams is a platform that provides chat, meetings, notes and attachments. When you create a Team in the application, you're creating a workspace for collaboration — including an associated Office 365 group that is created automatically. A number of other Microsoft applications, such as Yammer, create Office 365 groups under the covers in the same way. You can also create Office 365 groups directly.

A good way to think of the difference between a group and a Team is that groups are a functional pillar that can be used either on their own or as part of an application like Teams.

Office 365 groups are a functional pillar that can be used either on their own or as part of an application like Microsoft Teams.



Which do you want? It depends on your needs. If you create your own Office 365 group directly, you'll have a shared mailbox and shared calendaring, as well as the other resources and workloads described earlier. Your team can interact with the associated Office 365 functionality directly in the associated Office 365 applications like the group SharePoint site collection.

When you create a Team, the Teams application automatically creates an Office 365 group and its associated resources and workflows, but you don't use them directly; the Teams application uses them on your behalf. For example, when you chat on a Team channel, the application stores that content in the SharePoint Online site collection associated with the Office 365 group for the Team, and members can view it later from the Teams interface; they don't need to open SharePoint Online or even know that's where it is stored. But when you create an Office 365 group directly, you have to go to SharePoint Online yourself to see the content stored there.

### 3. How do I create an Office 365 group and add members to it?

Office 365 groups are created automatically by various applications, such as Microsoft Teams, Yammer, SharePoint Online and Planner. Both end users and administrators can also create Office 365 groups directly. By default, anyone in your organization can create Office 365 groups.

The most common way for end users to create Office 365 groups manually is by using Outlook, Outlook on the Web (formerly called Outlook Web Access) or Outlook Mobile. In Outlook 2016, for example, you simply select **Home > New Group** and then specify a name, description and other requested details. Once you've created the group, you can add members to it.

Administrators have several options as well. Both the Office 365 Admin Center and the Exchange Admin Center enable administrators to create groups. Alternatively, they can do it through PowerShell, which provides a couple of advanced setting that you don't get through the administrative portals.

End users can create Office 365 groups directly in Outlook; administrators can use either the administrative portals or PowerShell.

Note that, by default, groups are created as Private — membership requires approval and only members can see what's inside the group. If the Privacy setting is set to Public, anyone in your organization can view the group's content and become a member. Note that Private does not mean "hidden"; private groups are included in the global address list (GAL), for example.





## 4. How do I delete an Office 365 group?

Group owners and administrators can delete group using the same tools they use to create them. That is, end users can use the various Outlook applications, and administrators can use the administrative portals or PowerShell.

When you delete an Office 365 group, all the resources created for that group are deleted as well.

Note that when you delete an Office 365 group, all the resources tied to that group — the emails, the files, the OneNote and SharePoint documents, any Planner tasks, and so on — get deleted with it. So delete with care!

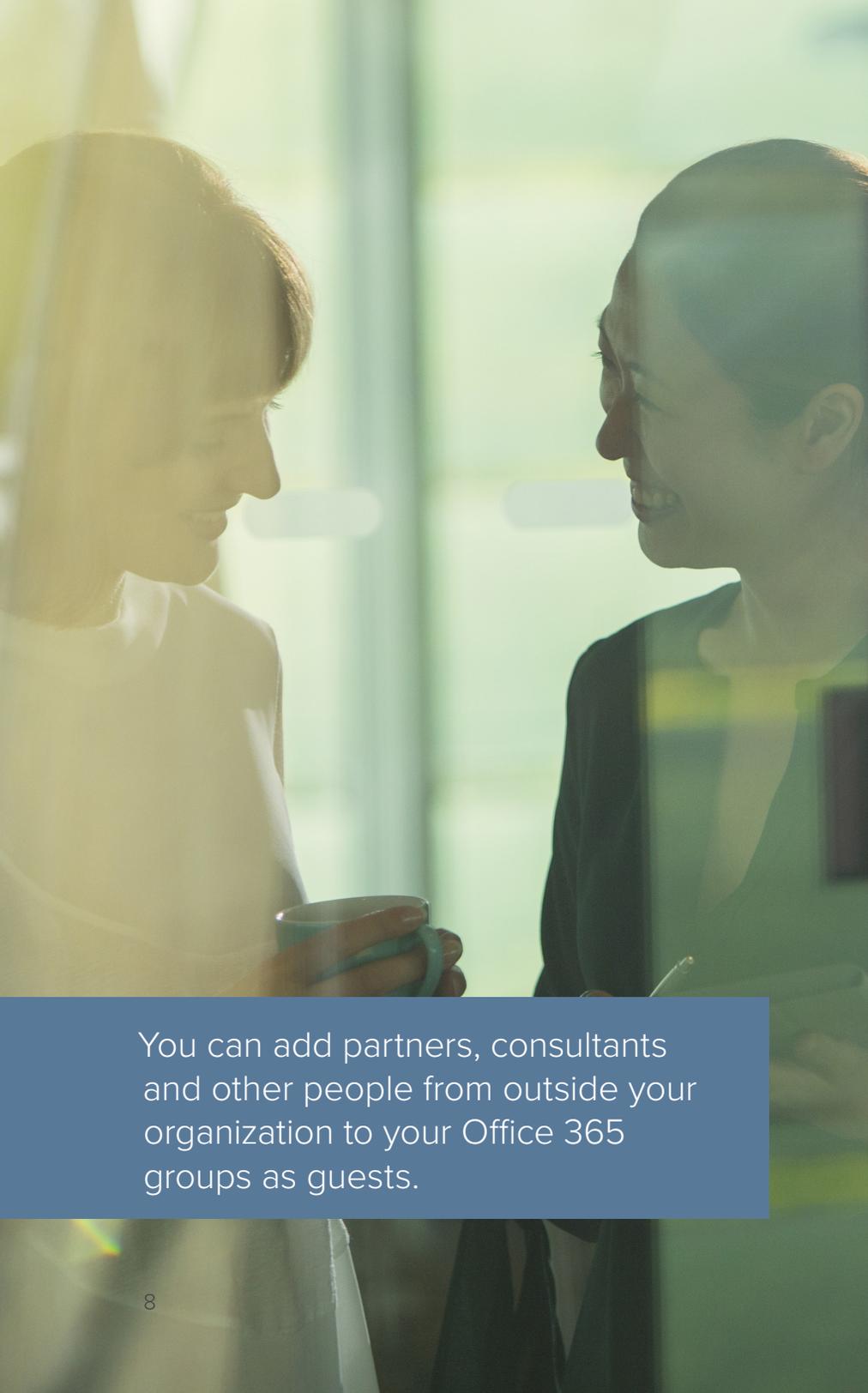
## 5. Can users manage the Office 365 groups they own?

Yes. Basic group management capabilities are provided natively by the applications used to create the groups. Using Outlook, owners can add and delete members and guests, change the name of the group or the Privacy setting, and so on. Applications that create and use groups under the covers, such as Teams, provide much of the same management functionality.

Note that there is no way to granularly remove management functions. For example, you cannot disable a group owner's ability to change the group's name. Also, each group can have up to 100 owners, all with the same complete management powers. There are no native capabilities to delegate specific group management functions.

Basic group management capabilities are provided natively by the applications used to create the groups.





You can add partners, consultants and other people from outside your organization to your Office 365 groups as guests.

## 6. Can I add someone from outside my organization to my Office 365 group?

You might want to include partners, vendors, suppliers, consultants or others from outside your organization in your Office 365 group. You can invite these people to become “guests” in the group. Members can nominate guests, but only group owners can add them to the group.

To add a guest, a group owner simply specifies that user’s email address in the “Add member” dialog in Outlook. The guest will receive a welcome email with some information about the group and how they can participate. Depending on how the group was created, you might also need to take steps to [let people outside the organization email the group](#).

All of a guest’s group interactions are through their email inbox; they can’t access the group site directly. If the guest is participating in the group through an Office 365 application such as Teams, they will participate through the functionality in that application. They can receive calendar invitations, participate in email conversations, and open shared files using a link or attachment (provided the tenant admin has not disabled this functionality). For details about exactly what guests can and cannot do, please refer to this [Microsoft Support article](#). All group emails and calendar invitations will include a link the guest can use to leave the group, and of course the group owner can delete guests as well.

## 7. How do I standardize the naming of my Office 365 groups?

Organizations have valid reasons for wanting some control over how groups are named. In particular, good, consistent group names can help users find the group they want more easily in the global address list, and understand the intended use for the group.

However, there is currently no way to enforce standards on the naming of Office 365 groups; a user who creates a group can name it whatever they like. Instead, enterprises still have to approach group naming as they did before Office 365 groups came along — by establishing standards, publishing them and training users to follow them.

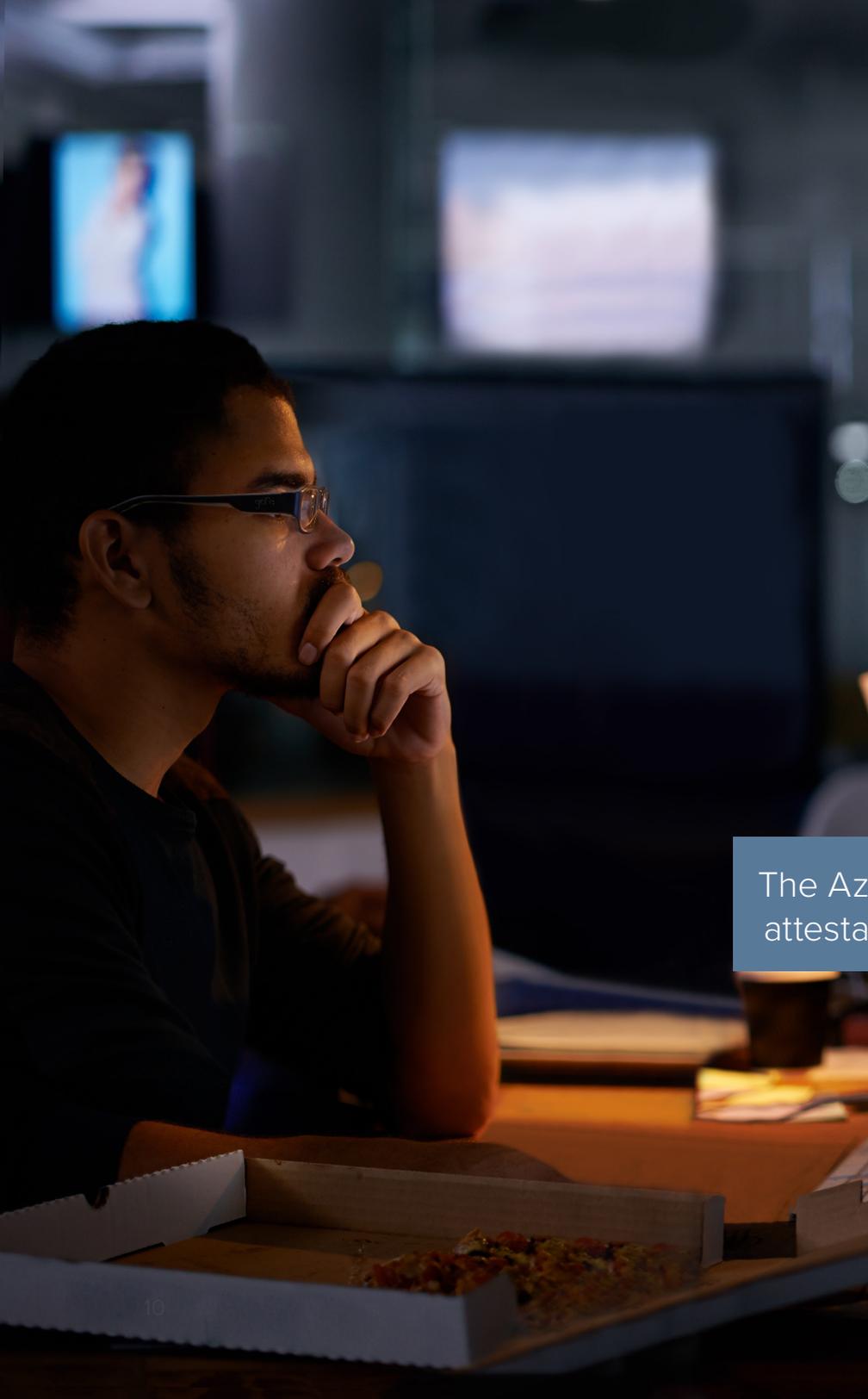
That being said, Microsoft does have an Office 365 group naming policy feature in public preview. You can use this policy to do two things:

- **Block specific words from being used in group name** — You can specify a set of words that cannot be used in group names, such as offensive terms or words that might attract attention from malicious insiders, like “CEO” or “Payroll.”
- **Add a prefix or suffix to group names** — You can also have a prefix or suffix automatically added to a group name. You can specify a fixed string, or you can enter a user attribute like “[Department]” and the appropriate value will be filled in based on the associated attribute of the user creating the group.

This feature should help to some degree with enforcing naming standards, though user training will surely still be required. But it comes at a price — you’ll need Azure AD Premium P1 licenses for all users who are members of Office 365 groups in the tenant.

Users can choose any name they like for the groups they create.





## 8. Is there a way to conduct attestation for Office 365 groups?

It's important to regularly conduct attestation for your Office 365 groups to ensure that the group is still required. The term 'attestation' refers to the recertification (usually by the group owners and members) that all members and guests still have a true business need to be in the group and be able to access its resources and workloads. As previously discussed, there are enterprise data and services associated with every Office 365 group, so regular attestation is critical to stay secure, compliant, and prevent data loss and breaches. Unfortunately, there is no native mechanism that provides end-to-end attestation. Instead, organizations must create PowerShell scripts to enumerate the membership of each group and develop a custom solution to process the PowerShell output and email it to the group owners for attestation.

The Azure AD access review feature helps simplify attestation, but it requires a Premium P2 license.

Microsoft has another new feature in preview, Azure AD access review, to help address this need. For each group, you can choose to have each user recertify their own access, or to have one or more users review everyone's access. From a cost perspective, this access review feature requires the Premium P2 edition of Azure AD.

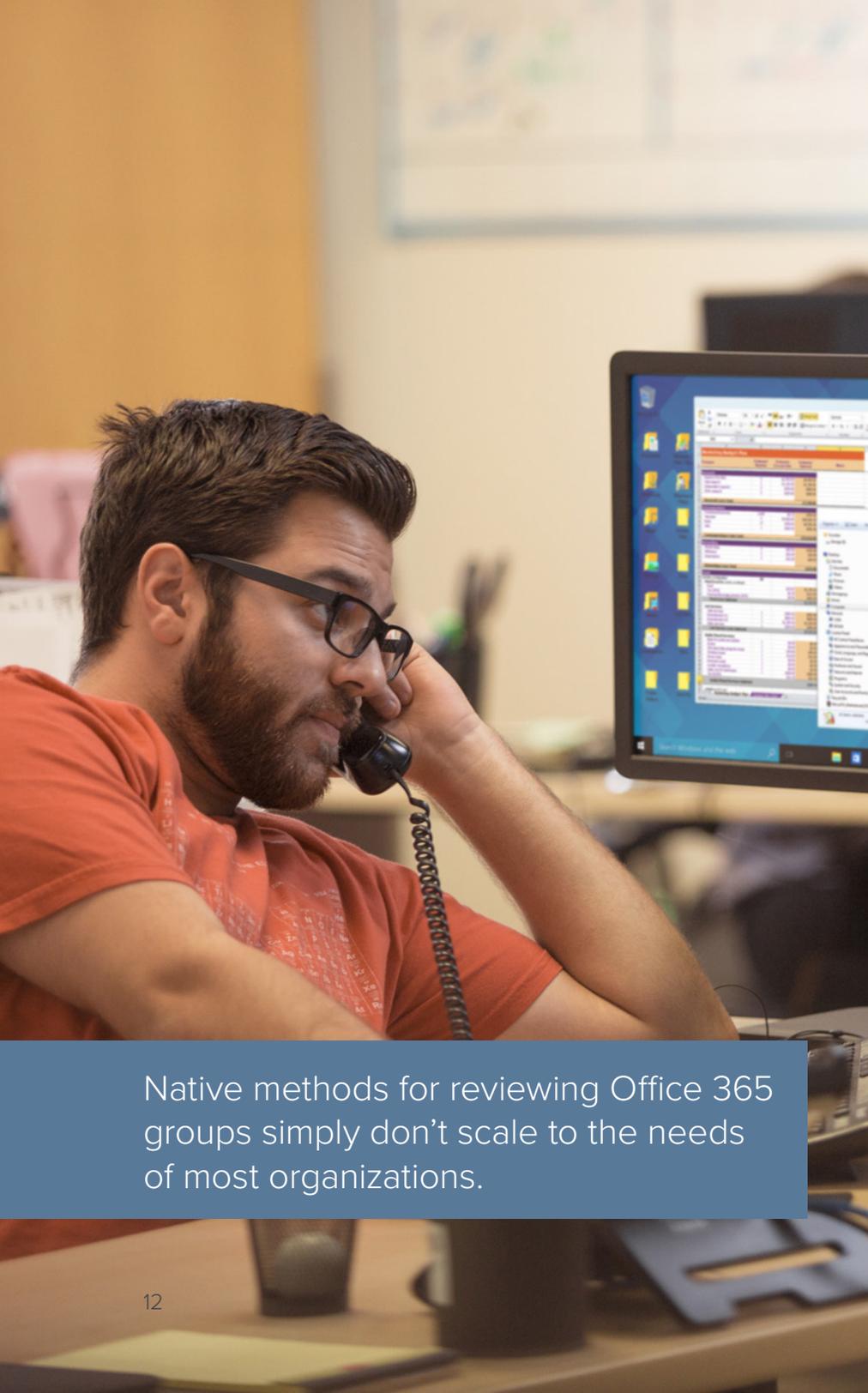
## 9. How can I implement an approval flow for provisioning Office 365 groups?

Organizations are justifiably concerned about not having control over what Office 365 groups their employees are creating. Unfortunately, there are no native tools in the base Office 365 licenses that provide an approval workload for group creation.

Instead, organizations have to create internal workflows in order to require steps like management approval for group creation. This can be completely manual, such as a form that users need to download from a SharePoint site and submit. Or you can automate it to some degree using helpdesk or ticket management tools that have an approval workflow, like ServiceNow,

There are no native Office 365 tools that provide an approval workload for group creation.





Native methods for reviewing Office 365 groups simply don't scale to the needs of most organizations.

## 10. How can I keep track of our Office 365 groups?

Using native tools, there are two ways that administrators can review what Office 365 groups exist and who their members are. Unfortunately, both of them involve substantial manual work, so they don't scale well.

### **Manual reviews through the admin portals**

The simplest way to review your Office 365 groups and their membership is to use either the Office 365 Admin Portal or the Exchange Admin Center. Guests are usually fairly easy to spot in the lists because of their external email addresses.

If you're at a 100-seat organization that recently adopted Office 365, manually checking your Office 365 groups this way might work for you, at least for a while. But if you're at a larger enterprise or you've been using Office 365 for a while, you may well have tens of thousands of groups, and therefore this won't be a viable approach.

### **PowerShell**

Alternatively, you can use PowerShell cmdlets to enumerate all the groups and their members. You can even cobble together scripts that, for example, identify all the groups with external members. But again, you're facing manual review of massive amounts of data on a regular basis.

Therefore, it's often wise to invest in third-party tools that simplify the process of reviewing groups and group membership.



## 11. Should I be concerned about Office 365 group sprawl?

Group sprawl is a huge concern in on-premises environments today. If you fail to hold your Exchange groups and public folders in close check, they tend to proliferate and accumulate lots of data — which is very expensive to store, back up and manage, especially if it has to remain highly available.

But in the cloud, your Office 365 subscription gives you plenty of storage by default. Why is group sprawl a problem in the cloud if you're not really paying any hard costs for it?

The answer is that hard costs are only part of the total cost of group sprawl, whether on-prem or in the cloud. In an on-prem environment, the hard costs are so high that they often dwarf the other costs. Once you move to the cloud, however, the other costs of sprawl come into sharper focus, especially in terms of usability and security. It's harder to put a price tag on these costs than it is to calculate how much you're spending on storage, but that doesn't make these concerns less real or less important.

Office 365 group sprawl has limited direct costs, but it hurts both productivity and security.

First of all, having a large number of groups leads to confusion and loss of productivity. Your global address list — which people use all the time — can grow by thousands of entries, making it harder for users to find the recipients they need to use email efficiently. And then the problem snowballs: It's hard for users to know if a group already exists to meet a given need, so someone creates a new group that is essentially a duplicate, and you have multiple groups with different owners trying to achieve similar goals. As a result, group sprawl tends to defeat the purpose of having Office 365 groups in the first place — to improve communication and collaboration.

Even more important, group sprawl also increases security risks because you lose accountability. Owners leave the organization and their groups get orphaned. Since attestation is difficult, even groups with conscientious owners often have members who no longer have a legitimate business need to access the resources available to them — a violation of the least-privilege principle that is central to strong security. Moreover, groups that have guests can get lost in the shuffle, so data is exposed externally. And since groups can provide access to sensitive and regulated data, compliance is a huge challenge as well.



## 12. Can I at least hide some of my Office 365 groups from the GAL?

Yes. You can reduce some of the costs associated with group sprawl by hiding some of your Office 365 groups from the GAL. To hide an Office 365 group from the GAL, an administrator has to use PowerShell to set a property on the group using this command:

```
Set-UnifiedGroup -Id  
<group> -HiddenFromAddressListsEnabled $True
```

Hiding groups, especially private groups, from the GAL can also help reduce security concerns; although the groups will still exist, at least they won't be out in plain sight. To hide all private groups in bulk, use the following command:

```
Get-UnifiedGroup | Where-Object {$_.  
AccessType -eq 'Private'} | Set-UnifiedGroup  
-HiddenFromAddressListsEnabled $true
```

However, note that even if a group is hidden from the GAL, it can still appear in other places, such as Planner.

To hide an Office 365 group from the GAL, you have to use PowerShell to set a property on the group.

## 13. How can I balance the desire for self-service group creation and the need to manage group sprawl?

This is the toughest and most important question in this FAQ. Unfortunately, the answer is that there is no good method to granularly control group creation — you either grant users the right to create whatever groups you want, which leads to sprawl, or you deny all users that right, which severely limits the value of your Office 365 investment by shutting down a key avenue for communication and collaboration.

There is one native method to allow only specific users to create Office 365 groups in the associated services that use them, but it is complex and requires an Azure AD Premium license, use of PowerShell and a Preview version of a PowerShell module. The process is described in this [Microsoft Support article](#). Another option to help manage sprawl, provided you have Azure AD Premium P1 licensing or better, is to [set an expiration policy](#) for each group.

Given these limited options, traditional manual methods are needed — guardrails that enforce basic organizational hygiene. Good governance practices include developing clear naming policies, educating users on best practices for when and how to create a group, enforcing regular attestation routines, and implementing a regular review of all new groups to look for duplicates. Alternatively, you can prevent users from creating groups themselves but implement a process for them to request new groups, such as creating a ticket or filling out a SharePoint form.

You should implement strong governance procedures to help minimize Office 365 group sprawl.



## Conclusion

Office 365 groups are a powerful tool for communication and collaboration. However, it's essential to manage them properly. As you move to the cloud, be sure to develop policies and procedures around all of the following:

- **Group creation and naming** — To minimize clutter and ensure users can find the groups they need
- **Inclusion of guests from outside the organization** — To help ensure corporate information stays private
- **Ongoing management and regular attestation** — To ensure your groups are still needed and have the right membership

Complement these policies and procedures with careful oversight to enjoy the benefits of self-service group creation while minimizing the costs and risks associated with group sprawl.

When properly managed, Office 365 groups are a powerful feature for communication and collaboration.

## ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our website ([www.quest.com](http://www.quest.com)) for regional and international office information.

© 2018 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

### Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at [www.quest.com/legal](http://www.quest.com/legal)

### Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit [www.quest.com/legal/trademark-information.aspx](http://www.quest.com/legal/trademark-information.aspx). All other trademarks are property of their respective owners.