

A 3D rendering of a puzzle with one red piece in the center, featuring a white warning triangle icon. The puzzle pieces are white and arranged in a grid pattern. The red piece is the central focus, standing out against the white background. The warning triangle icon is a white triangle with a black border and a black dot in the center, pointing downwards.

Solving the Guest User Puzzle in Microsoft 365

*Get 'em in,
Monitor & enforce policies,
Get 'em out!*

John Peluso

Chief Product Officer, Avepoint

John.Peluso@AvePoint.com

Twitter: [@johnconnected](https://twitter.com/johnconnected)

LinkedIn: [in/johnpeluso](https://www.linkedin.com/in/johnpeluso)

<http://johnpeluso.me>



Dux Raymond Sy

Chief Brand Officer, Avepoint

Dux.Sy@AvePoint.com

Twitter: [@meetdux](https://twitter.com/meetdux)

LinkedIn: [in/meetdux](https://www.linkedin.com/in/meetdux)

<http://meetdux.me>



Pieces of the puzzle...



Azure AD

Where Guests are defined

**Global O365
Settings**

Who can invite new Guests?

**Office 365
Groups**

Are guests allowed in Groups?

**What about
Teams?**

What can the Guests do?

**Where does
SharePoint fit in?**

External access to files

**Managing the
process...**

End-to-end Guest lifecycle



The case for external collab in Office 365



Does anyone think this is a
bad idea?



Let's face facts...

The Fear...

- By “letting them in”, you make it easy to over-share outside the org
- I don't trust my users to be careful when sharing, *especially* externally!
- My security team will never go for it
- Once an external person is *in*, how do I get them *out*?

The Reality...

- You are *already* sharing externally... but how?
- Are you leaving it to your users to decide *when* and *how*?
- Once your data leaves your system, what control do you have?
- Do you know *what* your external users are doing with your data?



OK, so what's so
complicated?



Peeling it all apart...



<https://docs.microsoft.com/en-us/microsoftteams/guest-access-checklist>

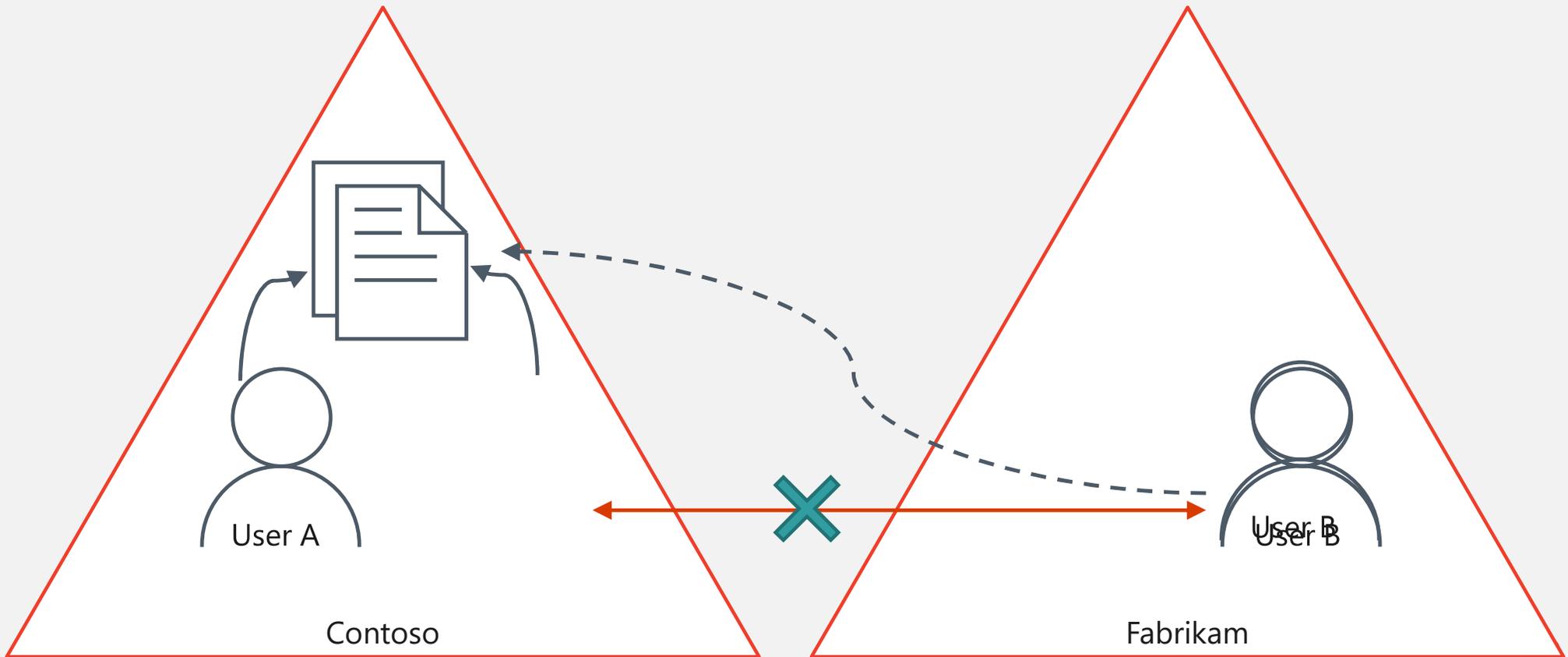
@JohnConnected

What exactly is a “guest”?

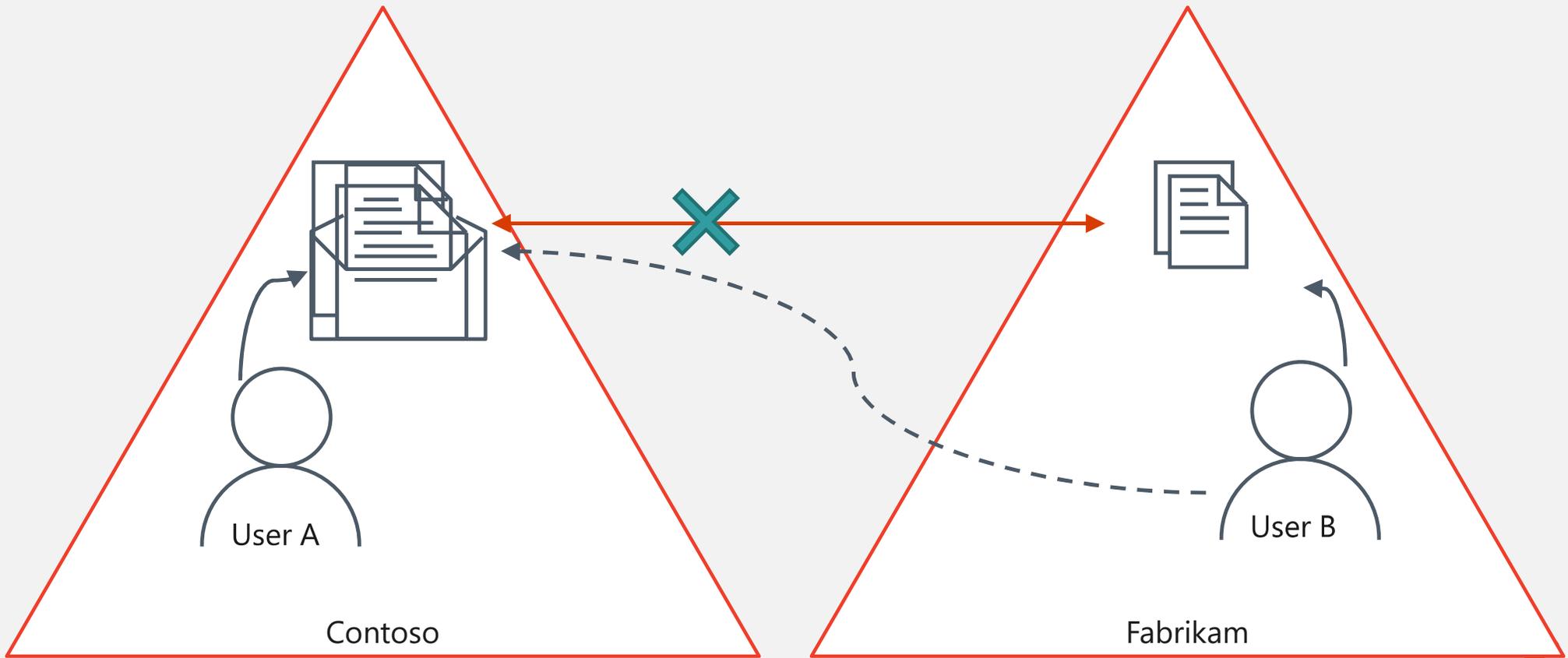
The most common scenarios...



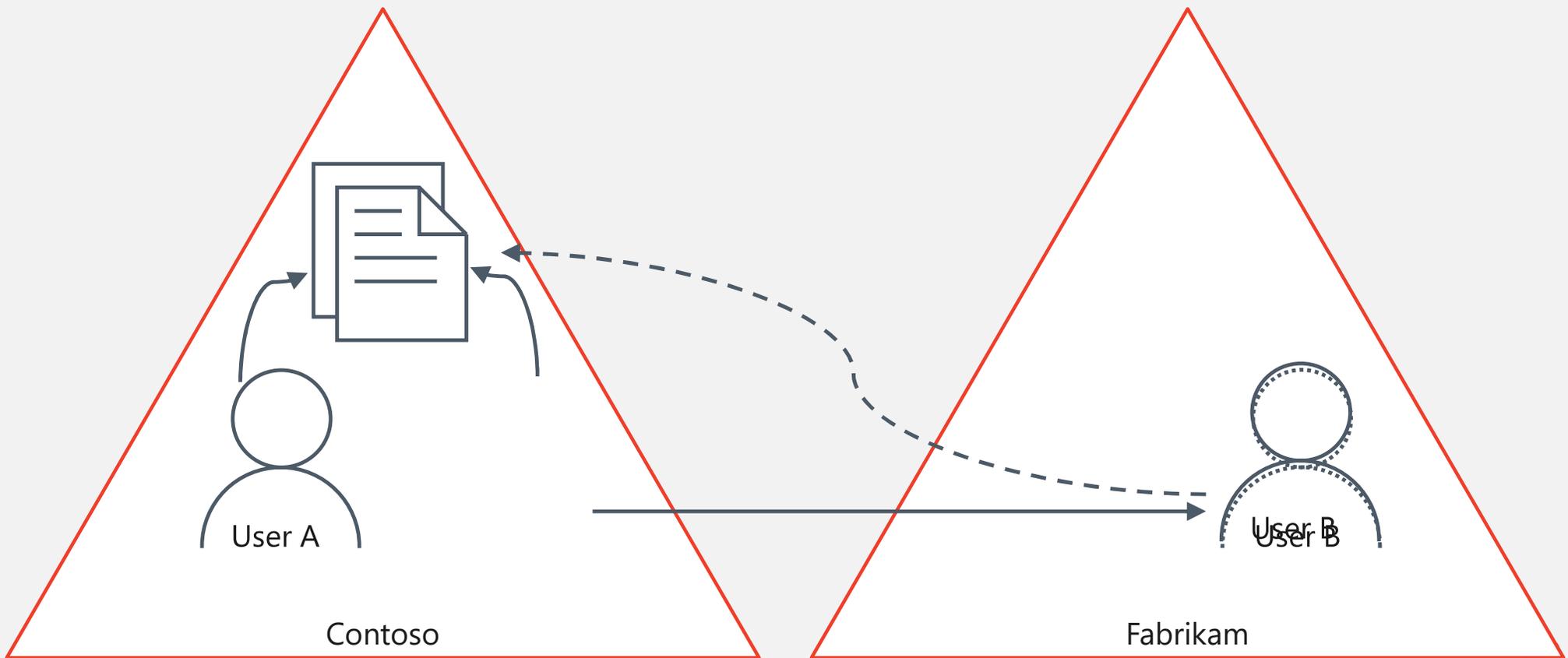
How we've shared externally in the past...



And this is even more common...



"Guest Users" in Azure Active Directory



What's this gonna cost me?

Azure B2B Licensing

- **No special licensing needed**

Azure AD Free capabilities are available for guest users without additional licensing.

- **5:1 ratio: 5 Guests per 1 user license**

An inviting tenant with an Azure AD paid license has B2B collaboration use rights to an additional five B2B guest users invited to the tenant.

- **5:1 licensing is determined by the feature requirements of your B2B users**

Example: A customer wants to invite 100 B2B collaboration users to its Azure AD tenant. The customer assigns access management and provisioning for all users, but 50 users also require MFA and conditional access. This customer must purchase 10 Azure AD Basic licenses and 10 Azure AD Premium P1 licenses to cover these B2B users correctly. If the customer plans to use Identity Protection features with B2B users, they must have Azure AD Premium P2 licenses to cover the invited users in the same 5:1 ratio.

- **Licensing is based on the relationship of the user to the tenant, not authentication**

If these users are not partners, they are treated differently in licensing terms. They are not considered to be a B2B collaboration user for licensing purposes even if their UserType is marked as "Guest." They should be licensed normally, at one license per user.

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/licensing-guidance>

@JohnConnected

Demo:

Configuring Azure AD for "Guest" access

Configuring B2B settings in AAD..

The screenshot displays the Azure Active Directory admin center interface. The top navigation bar shows the breadcrumb path: Dashboard > Contoso > External Identities. The main heading is "External Identities | External collaboration settings" for the "Contoso - Azure Active Directory" tenant. A search bar and "Save" / "Discard" buttons are visible at the top of the settings area.

The left-hand navigation pane includes sections for "Dashboard", "All services", "FAVORITES", "Azure Active Directory", "Users", and "Enterprise applications". The "External collaboration settings" option is highlighted in the left pane.

The main content area is divided into several sections:

- Get started**: Includes "All identity providers" and "External collaboration settings" (selected).
- Self-service sign up**: Includes "Custom user attributes (Preview)", "All API connectors (Preview)", and "User flows (Preview)".
- Subscriptions**: Includes "Linked subscriptions".
- Lifecycle management**: Includes "Terms of use" and "Access reviews".
- Troubleshooting + Support**: Includes "New support request".

The right-hand side of the settings page contains the following configuration options:

- Guest user access restrictions (Preview)**: Includes a "Learn more" link and three radio button options:
 - Guest users have the same access as members (most inclusive)
 - Guest users have limited access to properties and memberships of directory objects
 - Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
- Guest invite settings**: Includes "Admins and users in the guest inviter role can invite" (Yes/No buttons, "Yes" selected), "Members can invite" (Yes/No buttons, "Yes" selected), and "Guests can invite" (Yes/No buttons, "Yes" selected).
- Enable Email One-Time Passcode for guests (Preview)**: Includes a "Learn more" link and Yes/No buttons, with "No" selected.
- Enable guest self-service sign up via user flows (Preview)**: Includes a "Learn more" link and Yes/No buttons, with "No" selected.
- Collaboration restrictions**: Includes three radio button options:
 - Allow invitations to be sent to any domain (most inclusive)
 - Deny invitations to the specified domains
 - Allow invitations only to the specified domains (most restrictive)



Guests in *Groups and Teams*...



The "modern" way to collaborate externally?



Demo:
*Configuring Teams and Groups for Guest
Access*



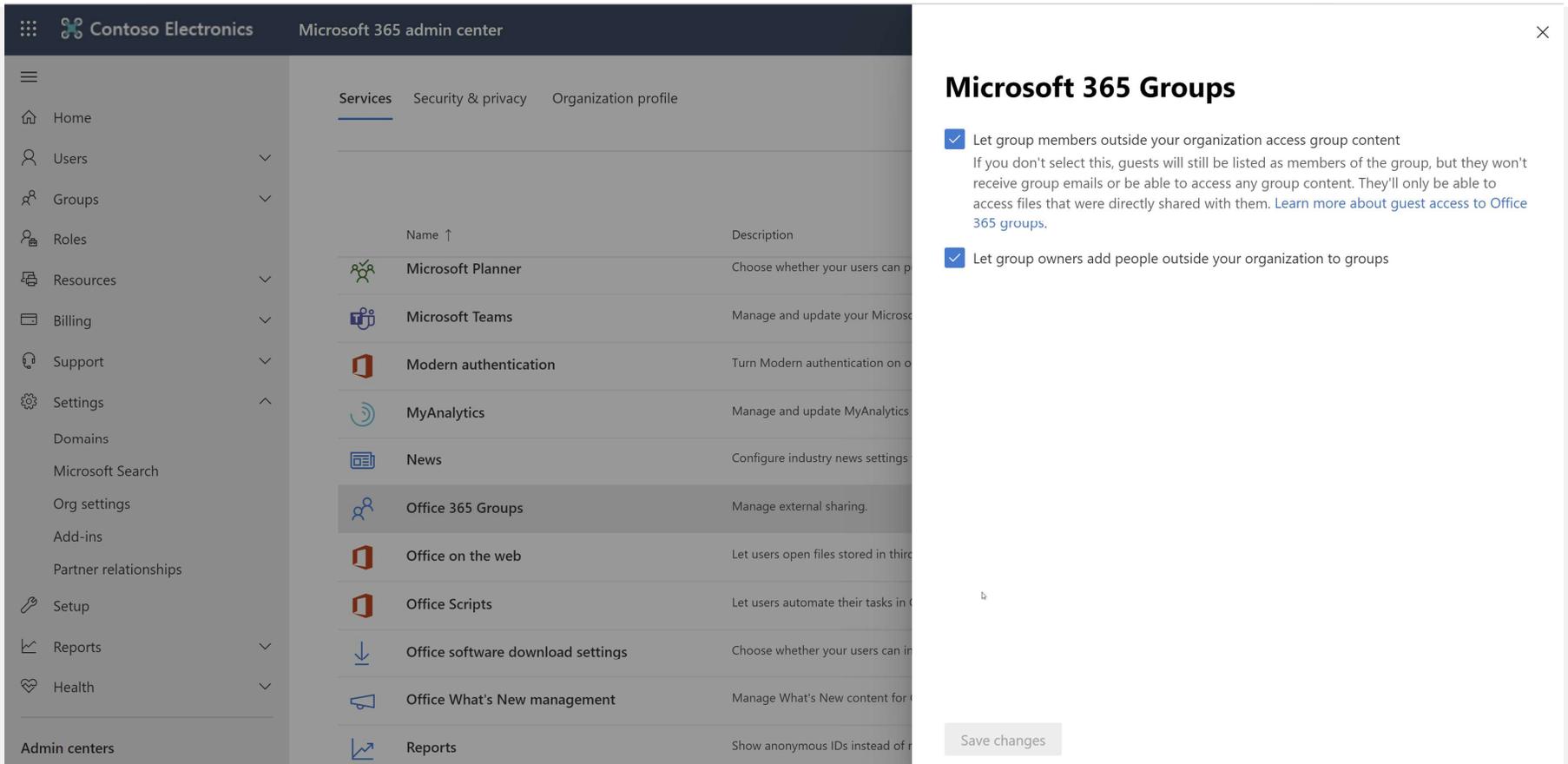
O365 Tenant wide: Owners can invite *new* guests?

The screenshot shows the Microsoft 365 admin center interface for a tenant named 'Contoso Electronics'. The left-hand navigation pane includes sections like Home, Users, Groups, Roles, Resources, Billing, Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is titled 'Org settings' and has tabs for 'Services', 'Security & privacy', and 'Organization profile'. The 'Security & privacy' tab is active, displaying a list of settings. The 'Sharing' setting is highlighted, and a modal dialog is open over it. The dialog title is 'Sharing' and contains the following text: 'When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. [Learn more about guests in your organization.](#) You can also [change the external sharing settings for SharePoint.](#)' Below the text is a checked checkbox labeled 'Let users add new guests to the organization'. At the bottom of the dialog is a 'Save changes' button.

Name ↑	Description
Customer lockbox	Set requirements for data access.
Password expiration policy	Set the password policy for all use
Privacy profile	Set the privacy statement of your
Privileged access	Set scoped access for privilege ta
Self-service password reset	Let users reset their own forgotte
Sharing	Control access for people outside



O365 Groups: Owners can *add* guests?



The screenshot shows the Microsoft 365 admin center for 'Contoso Electronics'. The left navigation pane includes Home, Users, Groups, Roles, Resources, Billing, Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is under 'Services' and lists various services like Microsoft Planner, Microsoft Teams, Modern authentication, MyAnalytics, News, Office 365 Groups, Office on the web, Office Scripts, Office software download settings, Office What's New management, and Reports. The 'Office 365 Groups' service is selected, and its settings are displayed on the right. Two checkboxes are checked: 'Let group members outside your organization access group content' and 'Let group owners add people outside your organization to groups'. A 'Save changes' button is visible at the bottom of the settings panel.

Name ↑	Description
Microsoft Planner	Choose whether your users can p
Microsoft Teams	Manage and update your Micros
Modern authentication	Turn Modern authentication on o
MyAnalytics	Manage and update MyAnalytics
News	Configure industry news settings
Office 365 Groups	Manage external sharing.
Office on the web	Let users open files stored in thir
Office Scripts	Let users automate their tasks in
Office software download settings	Choose whether your users can in
Office What's New management	Manage What's New content for
Reports	Show anonymous IDs instead of r

Microsoft 365 Groups

- Let group members outside your organization access group content
If you don't select this, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access files that were directly shared with them. [Learn more about guest access to Office 365 groups.](#)
- Let group owners add people outside your organization to groups

Save changes



Groups (and Teams): Should *this one* be more restrictive?

The screenshot shows a help article titled "Block guest users from a specific group" in the Microsoft 365 admin center. On the left is a navigation pane with a search filter and a list of topics, including "Manage guest access to groups" which is highlighted. The main content area includes an introduction, a list of prerequisites, a note about global admin rights, and a PowerShell script. On the right, there are feedback buttons and a list of related articles.

Block guest users from a specific group

If you want to allow guest access to most groups, but have some where you want to prevent guest access, you can block guest access for individual groups by using Microsoft PowerShell.

You must use the preview version of [Azure Active Directory PowerShell for Graph](#) (module name `AzureADPreview`) to change the group-level guest access setting:

- If you haven't installed any version of the Azure AD PowerShell module before, see [Installing the Azure AD Module](#) and follow the instructions to install the public preview release.
- If you have the 2.0 general availability version of the Azure AD PowerShell module (AzureAD) installed, you must uninstall it by running `Uninstall-Module AzureAD` in your PowerShell session, and then install the preview version by running `Install-Module AzureADPreview`.
- If you have already installed the preview version, run `Install-Module AzureADPreview` to make sure it's the latest version of this module.

Note

You must have global admin rights to run these commands.

Run the following script, changing / to the name of the group where you want to block guest access.

```
PowerShell
$GroupName = "<GroupName>"
Connect-AzureAD
```

Is this page helpful?
Yes No

In this article

- Manage groups guest access
- Add guests to a Microsoft 365 group from the admin center
- Block guest users from a specific group**
- Allow or block guest access based on their domain
- Add guests to the global address list
- Related articles

<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-guest-access-in-groups?view=o365-worldwide#block-guest-users-from-a-specific-group>



Restrict guests from *THIS* Group (and Team)?

Version
Microsoft 365

Filter by title

- Microsoft 365 admin center help
- Get started
- Overview of the Microsoft 365 admin center
- Manage users and groups
 - Manage users and groups
 - Users
 - Groups
 - Groups overview
 - Compare groups
 - Create a group
 - Manage groups
 - Add or remove group members
 - Restore a deleted group
 - Manage guest access to groups
 - Manage email and calendars
 - Manage domains
 - Manage your data and services
 - Manage subscriptions and billing

Download PDF

Block guest users from a specific group

If you want to allow guest access to most groups, but have some where you want to prevent guest access, you can block guest access for individual groups by using Microsoft PowerShell.

You must use the preview version of [Azure Active Directory PowerShell \(AzureADPreview\)](#) to change the group-level guest access setting:

- If you haven't installed any version of the Azure AD PowerShell Module and follow the instructions to install the public preview version.
- If you have the 2.0 general availability version of the Azure AD PowerShell Module, you must uninstall it by running `Uninstall-Module AzureAD` in your PowerShell console, and then install the preview version by running `Install-Module AzureADPreview`.
- If you have already installed the preview version, run `Install-Module AzureADPreview -Force` to get the latest version of this module.

Note
You must have global admin rights to run these commands.

Run the following script, changing / to the name of the group where you want to restrict guest access:

```
PowerShell

$GroupName = "<GroupName>"

Connect-AzureAD

$template = Get-AzureADDirectorySettingTemplate | ? {$_.displayName -eq "group.unified.guest"}
$settingsCopy = $template.CreateDirectorySetting()
$settingsCopy["AllowToAddGuests"] = $False
$groupID = (Get-AzureADGroup -SearchString $GroupName).ObjectId
New-AzureADObjectSetting -TargetType Groups -TargetObjectId $groupID -DirectorySetting $settingsCopy
```

Is this page helpful?

Yes No

In this article

```
Windows PowerShell
ObjectSetting
PS C:\Users\johnp> $GroupName = "Retail"
>>
>> Connect-AzureAD
>> $template = Get-AzureADDirectorySettingTemplate | ? {$_.displayName -eq "group.unified.guest"}
>> $settingsCopy = $template.CreateDirectorySetting()
>> $settingsCopy["AllowToAddGuests"] = $False
>> $groupID = (Get-AzureADGroup -SearchString $GroupName).ObjectId
>> New-AzureADObjectSetting -TargetType Groups -TargetObjectId $groupID -DirectorySetting $settingsCopy

Account Environment TenantId TenantDomain AccountType
-----
admin@365me.net AzureCloud 5ced927d-5ca8-4692-8bfb-cd038eb8724f 365me.net User

Id : 62df821a-fb92-4693-8e1d-32302b094230
DisplayName : 
TemplateId : 08d542b9-071f-4e16-94b0-74abb372e3d9
Values : {class SettingValue {
        Name: AllowToAddGuests
        Value: False
    }}

PS C:\Users\johnp>
```



SharePoint- *tenant wide*:

The screenshot shows the Microsoft 365 admin center for Contoso Electronics. The left navigation pane includes sections like Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, Health, and Admin centers. The main content area is titled 'Services' and lists various services. The 'SharePoint' service is highlighted, and a modal window is open to its configuration page.

SharePoint

Choose how your users can share SharePoint sites created within your organization.

Users can share with:

- Only people in your organization – no external sharing allowed
- Existing guests only – only guests already in your organization's directory
- New and existing guests – guests must sign in or provide a verification code
- Anyone – users can share files and folders using links that don't require sign-in

Advanced external sharing options

Limit external sharing by domain, allow external sharing for only specified security groups, and more in the SharePoint admin center. [Go to SharePoint admin center](#)

Save



Microsoft Teams: Are guests allowed in Teams?

The screenshot shows the Microsoft Teams admin center interface for 'Contoso Electronics'. The left-hand navigation pane includes options like Dashboard, Teams, Devices, Locations, Users, Meetings, Messaging policies, Teams apps, Voice, Policy packages, Analytics & reports, and Org-wide settings. The 'Guest access' option is highlighted. The main content area is titled 'Guest access' and contains the following settings:

- Guest access:** A toggle switch for 'Allow guest access in Teams' is turned 'On'.
- Calling:** A section titled 'Calling' with the subtitle 'Manage calling specific controls for guest users.' It includes a toggle switch for 'Make private calls' which is turned 'On'.
- Meeting:** A section titled 'Meeting' with the subtitle 'Turn on or turn off settings for guests in meetings.' It includes a toggle switch for 'Allow IP video' which is turned 'On', and a dropdown menu for 'Screen sharing mode' set to 'Entire screen'.

If "YES", owner invitation of new guests dictated by Office 365 Groups setting



Be careful with your “guest” and “external” terminology

Guest access vs. external access (federation)

External access (federation) and guest access are different:

- Guest access gives access permission to an individual. External access gives access permission to an entire domain.
- Guest access, once granted by a team owner, allows a guest to [access resources](#), such as channel discussions and files, for a specific team, and chat with other users in the team they have been invited to.

With external access (federated chat), the external chat participants have no access to the inviting organization’s teams or team resources. **They can only participate in one-on-one federated chat.** Tenant admins can choose between the two communication options depending on which level of collaboration is desirable with the external party. Admins can choose either approaches or both, depending on their organizational needs, but we recommend enabling guest access for a fuller, collaborative Teams experience.

<https://docs.microsoft.com/en-us/microsoftteams/guest-experience>

@JohnConnected

What about sharing *files* outside the org?



This is where it gets
more... *interesting*



Why are SharePoint and ODFB are a bit...different



<https://docs.microsoft.com/en-us/azure/active-directory/b2b/o365-external-user>

Not built on AAD B2B

- They had external sharing before Azure B2B existed
- Looks like consolidation may be coming but it's early days, some preview functionality

You are *not* seeing double

- Many of the same settings as the AAD model, but independent
- You can *force* more centralization if it fits your use cases by tying sharing to existing users in the directory

@JohnConnected

SharePoint: Is "External Sharing" allowed?

Contoso Electronics Microsoft 365 admin center

Services Security & privacy Organization profile

Name ↑	Description
Office on the web	Let users open files stored in third-party cloud services.
Office Scripts	Let users automate their tasks in Office applications.
Office software download settings	Choose whether your users can install Office software.
Office What's New management	Manage What's New content for Office applications.
Reports	Show anonymous IDs instead of real user IDs in reports.
SharePoint	Control external sharing.
Sway	Manage sharing and content sources for Sway presentations.
User consent to apps	Choose whether users can consent to apps.
User owned apps and services	Allow users to access the Office 365 apps and services.
Whiteboard	Allow users to access Microsoft Whiteboard.

SharePoint

ⓘ Your Microsoft 365 Groups settings let people outside the organization access group content. These guests will receive an error when they try to access SharePoint content. [Change Microsoft 365 Groups settings.](#)

Users can share with:

- Only people in your organization - no external sharing allowed
- Existing guests only – only guests already in your organization's directory
- New and existing guests – guests must sign in or provide a verification code
- Anyone – users can share files and folders using links that don't require sign-in

Save changes Manage additional settings



SharePoint: What are the *global* settings?

The screenshot shows the SharePoint admin center interface for Contoso Electronics. The left-hand navigation pane includes links for Home, Sites, Policies, Settings, Content services, Migration, More features, OneDrive admin center, Customize navigation, and Show all. The main content area is titled 'Sharing' and provides instructions on controlling sharing at the organization level. It features a slider for 'External sharing' with two vertical bars, one for SharePoint and one for OneDrive, both set to the 'Least permissive' position. The sharing options are: 'Anyone' (Users can share files and folders using links that don't require sign-in), 'New and existing guests' (Guests must sign in or provide a verification code), 'Existing guests' (Only guests already in your organization's directory), and 'Only people in your organization' (No external sharing allowed). Below the slider, there is a section for 'More external sharing settings' with four checkboxes: 'Limit external sharing by domain' (unchecked), 'Allow only users in specific security groups to share externally' (checked), 'Guests must sign in using the same account to which sharing invitations are sent' (unchecked), and 'Allow guests to share items they don't own' (checked).

Contoso Electronics SharePoint admin center

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more](#)

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings

- Limit external sharing by domain
- Allow only users in specific security groups to share externally
- Guests must sign in using the same account to which sharing invitations are sent
- Allow guests to share items they don't own



SharePoint: Should *this site* be more restrictive?

The screenshot displays the SharePoint Admin Center interface for 'Contoso Electronics'. The left-hand navigation pane includes options like Home, Sites, Active sites, Deleted sites, Policies, Settings, Content services, Migration, More features, OneDrive admin center, and Customize navigation. The main content area is titled 'Active sites' and contains a table of site information. The 'Conference Team' site is selected, and a 'Sharing' settings panel is open on the right. This panel shows 'External sharing' options: 'Anyone' (disabled), 'New and existing guests' (disabled), 'Existing guests only' (selected), and 'Only people in your organization' (disabled). Under 'Advanced settings for external sharing', 'Limit sharing by domain' is disabled. The 'Default sharing link type' is set to 'Same as organization-level setting (Only people in your organization)'. Buttons for 'Save', 'Cancel', and 'Reset to organization-level settings' are visible at the bottom of the panel.

Site name ↑	URL	Storage used
Brand	.../sites/Brand	0.06
Communication site	https://m365x864957.sharepoint.com	0.02
<input checked="" type="checkbox"/> Conference Team	.../sites/ConferenceTeam	0.00
Contoso Landings	.../sites/ContosoLandings	0.14
Contoso Web 1	.../sites/ContosoWeb1	0.33
Contoso Web 2	.../sites/ContosoWeb2	0.01
Contoso Web 3	.../sites/ContosoWeb3	0.14
Core Services	.../sites/CoreServices	0.00
Deployment team	.../sites/DeploymentTeam	0.00
DTC Workshop Planning	.../sites/DTCWorkshopPlanning	0.00
Executive Corner	.../sites/Exec	0.02

Sharing

External sharing

Site content can be shared with:

- Anyone
Users can share files and folders using links that don't require sign-in.
- New and existing guests
Guests must sign in or provide a verification code.
- Existing guests only
Only guests already in your organization's directory.
- Only people in your organization
No external sharing allowed.

Advanced settings for external sharing

- Limit sharing by domain

Default sharing link type

- Same as organization-level setting (Only people in your organization)

Save Cancel Reset to organization-level settings



External user reporting for SPO and ODFB is at the *site collection* level

The screenshot displays the SharePoint interface for the 'DTC Workshop Planning' site. A 'Run report' dialog box is open, prompting the user to choose a destination to save the report. The dialog shows a list of folders: 'General' and 'Presentation Prep'. The 'Presentation Prep' folder is selected. The background shows the site's main content area with a table of files and folders.

Name	Modified	Modified By	Size	Location
Run report				
._siteicon_.png	6 days ago	System Account		/SiteAssets
Presentation Prep	2/26/2020	MDO Administrator	0 bytes	/Shared Documents
DTC Workshop Planning Notebook	2/26/2020	MDO Administrator	0 bytes	/SiteAssets
General	2/26/2020	MDO Administrator	0 bytes	/Shared Documents

Settings

SharePoint

- Add a page
- Add an app
- Site contents
- Site information
- Site permissions
- Site usage
- Change the look
- Site designs

Office 365

View all

Quick links

- Learn about a team site
- Learn how to add a page

Documents

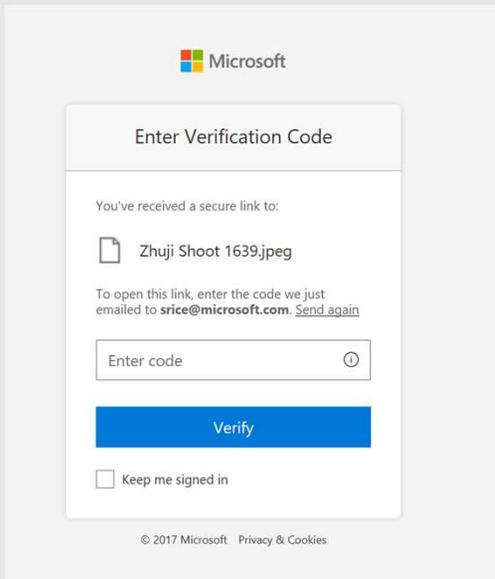
- New
- All Documents
- General
- Presentation Prep

Run report

Save Cancel

@JohnConr

NEW! Azure AD B2B for one-time passcode users



Share securely with anyone in the world

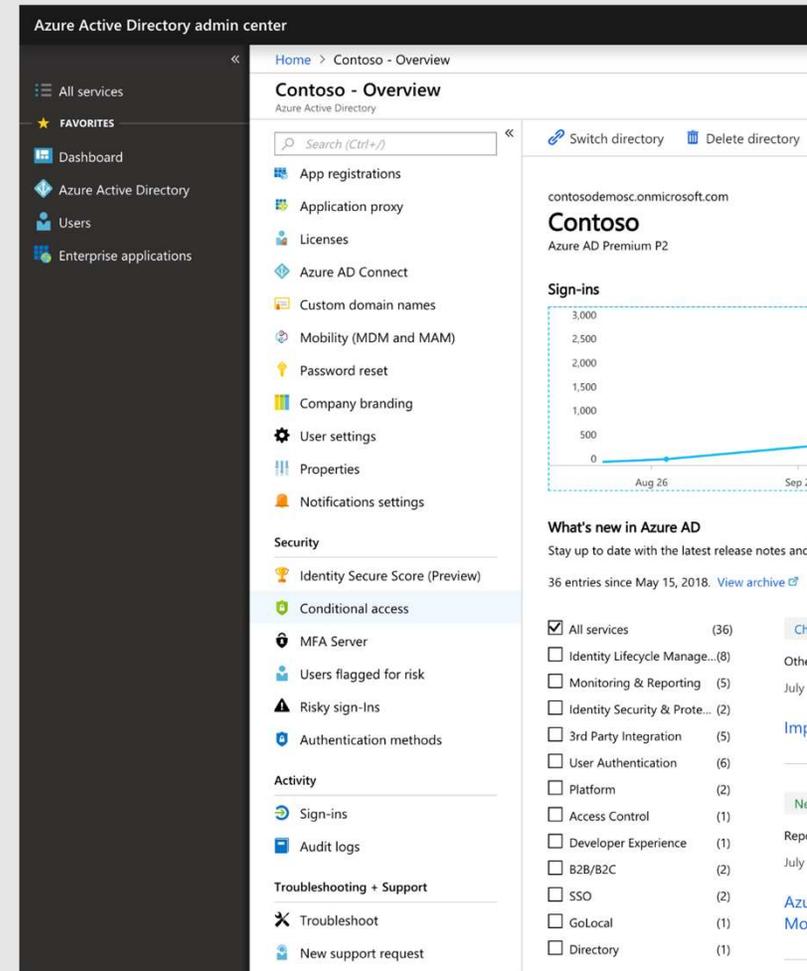
Simple verification with one-time passcode

AAD B2B guest management

Conditional access

Google auth federation

Guest do not require O365 licenses



Demo:

*Configuring external file sharing options in
SharePoint Online and OneDrive*

How can you manage all of this *at scale* with *minimal* burden on your IT/Operations teams?



Key considerations...

Who and where?

Do you need to collaborate externally? If so, what does that collaboration look like?

How do you want to onboard *new* external collaborators?

Controlled, subject to approval? Open to owner invites? Manual or automated?

How will you handle the lifecycle of guests?

Monitoring, reporting, need for access, off-boarding.... How will this happen?

Governing Guest access in *Groups/Teams* and
External Sharing for *SPO and ODFB* with
AvePoint

AvePoint Cloud Governance Approach

The screenshot shows a web interface for a 'New Request' in the 'Project Management Questionnaire' section. The interface includes a header with the word 'governance' and navigation icons. Below the header, there is a breadcrumb trail 'New Request > Project Management Questionnaire'. A grey box contains the text: 'Before we get started... We want to help you ensure that all your data is secure and that you have the right tools for the right job. Please answer the following questions to the best of your ability!'. The form contains three questions: 1. 'Is this a new or existing project?' with a dropdown menu set to 'New Project'. 2. 'How would you describe this project's collaboration?' with two radio button options: 'Traditional Workstream' and 'Modern Workstream' (which is selected). 3. 'Is this project going to involve sharing/storing any of the following types of information?' with a dropdown menu set to 'Please select an option...'. At the bottom right of the form are 'Cancel' and 'Save as Draft' buttons.

Standardized Services

- Clear definition of ownership, business purpose, and guidelines
- Tailored by role and business units
- Approval process for new workspaces
- Terms of service and use (example: protected health information)

Policy Enforcement

- Apply proactive monitoring/enforcement of permissions and configuration policies



New Request > Project Management Questionnaire

Before we get started...
We want to help you ensure that all your data is secure and that you have the right tools for the right job. Please answer the following questions to the best of your ability.

Is this a new or existing project?

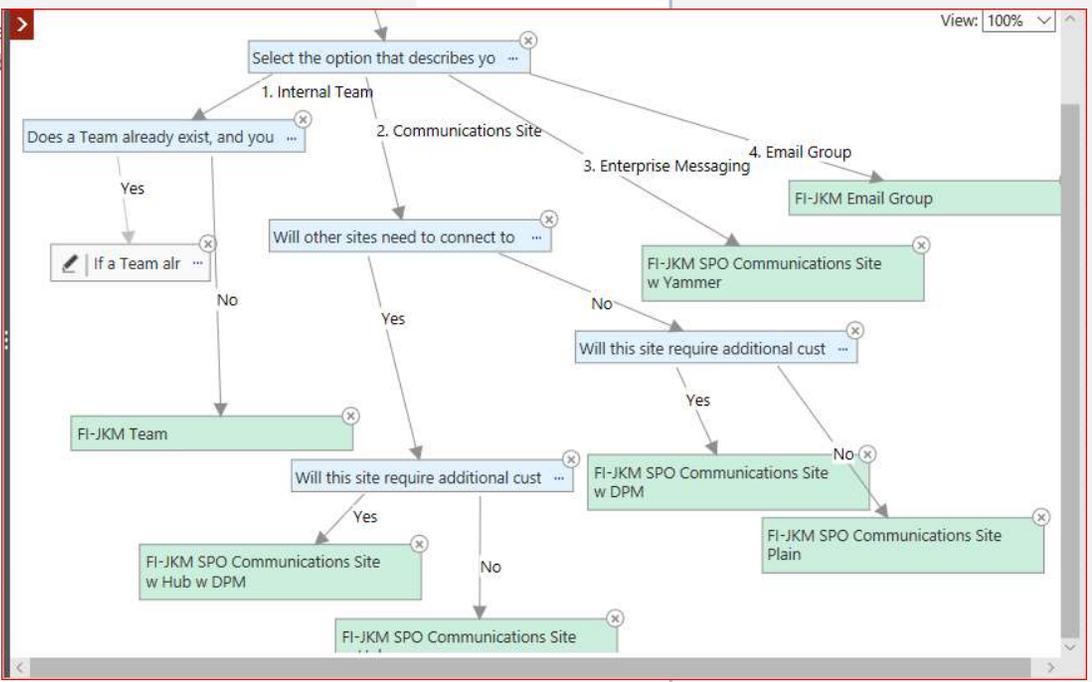
New Project

How would you describe this project's collaboration?

- Traditional Workstream
- Modern Workstream

Is this project going to involve sharing/storing any of the following types of information?

Please select an option...



Governing external access through Policy

MENU ▾

AvePoint Cloud Governance

Ian Anderson ▾     

Policy Management > Teams Public - External ⓘ

 Save  Save and Activate  Cancel

External Sharing

To set unique guest access or external sharing settings here, make sure the external sharing for Office 365 Groups and SharePoint is turned on in Microsoft 365 admin center > Settings > Org settings. If you set unique guest access or external sharing settings for the groups/teams associated with this policy, the groups/teams can have more restrictive settings than the current global configurations in Microsoft 365 admin center.

- Set unique guest access settings for the group/team
 - Allow group/team owners to add people outside the organization to the group/team
 - Allow group/team owners to invite new external users who are not already in Azure Active Directory
 - Set unique external sharing settings for the site collection associated with the group/team
 - Allow users to share the group team site content with people outside the organization
 - Anyone
 - New and existing external users
 - Existing external users
- Access request settings
- Allow members to share the site and individual files and folders
 - Allow members to invite others to the site members group. This setting must be enabled to let members share the site
 - Allow access requests
 - Send access requests to the site owners group
 - Send access requests to the following e-mail address



Defining options available for request

Service Management > Create Service ⓘ



✖ Cancel

Team Member Permissions

Choose the actions you allow team members to perform in the team, or allow business users to configure team member permissions in the service request form.

- Allow members to create and update channels
- Allow members to delete and restore channels
- Allow members to add and remove apps
- Allow members to create, update, and remove tabs
- Allow members to create, update, and remove connectors
- Allow members to delete their messages
- Allow members to edit their messages
- Assign by Business User
- Require Business User Input

Guest Permissions

Choose whether to allow guests to create, edit, and delete channels, or allow business users to configure guest permissions in the service request form.

- Allow guests to create and update channels
- Allow guests to delete channels
- Assign by Business User
- Require Business User Input

@Mentions

Choose whether to allow team members to use @team and @channel mentions, or allow business users to configure this in the service request form.

- Show members the option to @team or @[team name] (this will send a notification to everyone on the team)
- Show members the option to @channel or @[channel name] (this will send a notification to everyone who has favorited the channel being mentioned)
- Assign by Business User
- Require Business User Input



Conditional approval...

MENU ▾ AvePoint Cloud Governance Ian Anderson ▾

Add Conditional Approval Process

Save ✕ Cancel

Name
Enter a name for the conditional approval process.

Condition Settings
Configure the condition settings that will be combined with an approval process to create a conditional approval process.

***Name:**

***Condition Settings:**

Always run this approval process
 Run this approval process if the conditions below are met

***Metadata source:**

***Property name:**

***Condition:**

Select One
Does Not Contain Guests
Contains Existing Guests
Contains New Guests



EXAMPLE

DEPARTMENT



DEPARTMENT



DEPARTMENT



	DEPARTMENT A	DEPARTMENT B	DEPARTMENT C
EXTERNAL SHARING	No external sharing 	External sharing allowed in: 	External sharing only allowed in:
EXPIRATION/RETENTION	6 Months after last accessed	12 Months after last accessed	9 Months after last accessed
ALLOW THESE USERS TO CREATE A TEAM	All requests through Central IT	All requests through Department IT	Only Joe, Sally, and Harold can create
RECERTIFY MEMBERS	after 3 Months	after 6 Months	after 12 Months



Targeting Services & Policies Across Divisions

Tenant Wide General Services

- Available to all/most users
- Address general productivity, security, compliance needs

Core Services
(provisioning, lifecycle, policy, protection)

Address Unique Needs of Specific Departments or Divisions

- LOB specific configurations
- More/less control and restrictions
- Example – External sharing allowed

Division



Division



Division



Specialized Services Smaller Groups

- Unique needs can be addressed
- Pilots of future services

Team C-1
specialized Services



Leveraging "Service Permissions" to map services to the right users...

Service Management > Create Communicatio... ⓘ

Copy Save Save and Activate Cancel

Service Initiation

Choose how users will be able to initiate requests for this service.

- Available in service catalog (the Start a Request page)
- Available as a questionnaire result
 - Users must meet the service permissions below
 - Allow all users to use this service from questionnaire results (Regardless of the service permission conditions)

Service Permissions

Specify users that should have access to this service.

- Local Users or Office 365 Users/Groups** - The specified users/groups can view this service in the Start a Request page and can submit requests via this service. You can specify Office 365 users/groups or AvePoint Online Services local users.

- Allow all users to use this service
- Define conditions for users who can request this service

Conditions:

Local Users or Office 365 Users/Groups ▼

*Allowed values:

Add to List Clear Settings

Type	Allowed Values	Actions
No items to show in this view.		

Clear Table



External sharing review by workspace owners during Renewal process...

The screenshot displays the MyHub interface with a navigation bar at the top containing 'MyHub', 'Chat', 'Home', 'Start a request', 'Workspaces', 'Requests', and 'About'. The main content area is divided into several sections:

- To-do list:** Includes an 'Approvals' section with a task 'Delete Office 365 Group/Microsoft Team Ext...' and a 'Confirmations' section with a task 'PM Extranet Renew Site Collec...'. A red box highlights the 'Q2 Outing Renew Office 365 Group' task in the Confirmations section.
- Group renewal: Q2 Outing:** A detailed view of the renewal process for the 'Q2 Outing' group. It lists renewal steps: Contact renewal, Permission renewal, Membership renewal, and Metadata renewal. A table below shows the user list with columns for Username, User role, Change action, and Access type. A red box highlights the 'Access type' column, showing 'Internal' for most users and 'External' for 'Tom Gawczynski' and 'murugan.balaji'.

Username ↑	User role	Change action	Access type
Barriemore Barlow	Owner		Internal
Ian Anderson	Member		Internal
Ray Hill	Member		Internal
Ray Hill	Owner		Internal
Tom Gawczynski	Member		External
murugan.balaji	Member		External



What about a managed process for *provisioning, management and lifecycle* of guests?



Designing the "Guest User Request" service

The screenshot displays the AvePoint Cloud Governance interface. The left sidebar contains navigation options: Home, Management, Services, Settings, and Directory. The main content area is titled 'Services > Invite New Guest User > Edit' and is divided into three tabs: '1. Basic info', '2. Settings', and '3. Advanced settings'. The 'Settings' tab is active, showing configuration for a 'Guest renewal profile'. The 'Microsoft 365 tenant' is set to 'AvePoint ATS Dev'. The 'Primary contact' is '\$Requester' and the 'Secondary contact' is '\$Manager of Requester'. A toggle switch for 'Allow requesters to add guest users to groups or teams' is turned on. Below this, two checkboxes are checked: 'The requester is the owner of the group or team' and 'The requester is the primary/secondary contact of the group or team'. The 'Renewal profile' is set to 'Guest User Renewal'. At the bottom of the settings pane are 'Cancel', 'Back', and 'Next' buttons.

The right pane is titled 'Create guest user renewal profile' and contains the following fields and options:

- Profile name ***: Text input field containing 'Renew guests every 30d'.
- Description**: Text input field.
- Microsoft 365 tenant ***: Dropdown menu set to 'AvePoint ATS Dev'.
- Category ***: Dropdown menu set to 'Lifecycle Management'.
- Renewal process**: Section with the question 'How often do you want renewal process to initiate? *'.
 - Daily: Includes a sub-field 'Every 30 days'.
 - Weekly
 - Monthly
 - Specify the time to generate the first renewal task
- Renewal task will be overdue if the task assignee doesn't complete it within**: Input field '7' followed by a dropdown 'Days'.
- What user will be responsible for completing the renewal task? * ⓪**: Dropdown menu set to '\$Primary guest contact'.
- Notification e-mail template for assigned renewal tasks ***: Dropdown menu set to 'Built-in Guest User Renewal Process Assignment E-mail Template'.
- Allow renewal task assignees to reassign tasks to other users



Admin monitoring of Guests

The screenshot displays the AvePoint Cloud Governance interface. On the left is a navigation sidebar with options like Home, Management, Services, Guest renewal profil..., Settings, MyHub settings, System settings, Directory, Workspace report, and Guest user report. The main area shows a 'Guest user report' table with columns for Username, E-mail address, and Primary contact. Two rows are visible: 'Gawczynski.Tom' and 'Tom.Gawczynski'. The 'Tom.Gawczynski' row is selected, and its details are shown in a right-hand panel. The details panel includes fields for Username, First name, Last name, E-mail address, Primary contact, Secondary contact, Job title, Department, Renewal profile, Invited by, and Status. Below this is a 'Workspace access' table.

Name	ID	Type
Q2 Outing	Q2Outing@avepointats-dev.com	Microsoft Team
Regional Hospital	RegionalHospital@avepointats-dev.com	Microsoft Team
Project_US	Project_US975@avepointats-dev.com	Microsoft Team

Existing guests can be imported for management as well!



Renewal process for Guests

The screenshot displays the Microsoft Teams MyHub interface. The top navigation bar includes 'Microsoft Teams', a search bar, and a user profile icon. Below this, the 'MyHub' section has tabs for 'Chat', 'Home', 'Start a request', 'Workspaces', 'Requests', and 'About'. The 'Home' tab is active, showing a 'To-do list' with 'Approvals' (no action required) and 'Confirmations' (renewal pending for several items). The 'Confirmations' list includes: Tom.Gawczynski (Renew Guest user), Q2 Outing (Renew Microsoft Team), External_Project X (Renew Microsoft Team), and Product UI Design (Confirm Governance Details). On the right, the 'News & Updates' section lists several announcements with dates from 2019 to 2020, including updates on Office 365 requests, Hubs availability, Crisis Management Team templates, Guest Access, and Microsoft Teams/Office 365 Groups availability.

Microsoft Teams Search

MyHub Chat Home Start a request Workspaces Requests About

Home Hubs Workspaces Requests Start a request

To-do list Search in Home

Approvals Due date ▾ You have no approvals requiring action at this time.

Confirmations Due date ▾

- Tom.Gawczynski**
Renew Guest user
Renewal Pending
- Q2 Outing**
Renew Microsoft Team
Renewal Pending
- External_Project X**
Renew Microsoft Team
Renewal Pending
- Product UI Design**
Confirm Governance Details

News & Updates

New Office 365 requests available!

July 12th, 2020

- Adding Guest users to workspaces is now available. To find this request type look below Security in the services tab. This service is labeled [Invite New Guest User](#)

May 15th, 2020

- Hubs are now available to sort your workspaces and collaboration area based on criteria YOU entered during the request process!

March 30, 2020

- Crisis Management Team template is now available as a result of filling in the New Workspace Questionnaire. If you create a Team using this template, the Team will be populated with a standard of channels deemed necessary by our Executive team.
- [Getting Started With MSFT Teams Resources](#)

February 10, 2020

- Guest Access is now enabled within the organization. In an effort to better protect our data, we will be requiring a security review every 60 days against workspaces that require Guest Access.

April 28th, 2019

- We have enabled Microsoft Teams and Office 365 Groups across the company. You will have access to Internal Private Groups and Teams through Quick Requests. In order to create a public or workspace that can be accessed by individuals outside of our company an approval process will be required throughout your Business Unit.

January 1st, 2019



Proactive monitoring and removal of unneeded guests...

AvePoint Policies For Microsoft 365

- Dashboard
- Policies
- Individual Service
- Tenant
- Tenants
- Containers
- Workspaces
- Job Monitor
- General Settings

Policies / Tenant / Edit Policy

Edit Policy

General Information

A policy allows you to monitor certain user activities and changes using policy rules.

* Name
ATS - Tenant Policy

Description
Checks for inactive Guest Users and identifies users without any membership.

Rules

Ghost User Detection
Detect users who do not have any membership in SharePoint Online sites, Groups, and Teams. ✕ Configure Rule

Remove Inactive Guest Users
Remove users who do not have any activities in SharePoint Online sites, Groups, and Teams. ✕ Configure Rule

Add Rule

Ghost User Detection

Detect users who do not have any membership in SharePoint Online sites, Groups, and Teams.

Rule Settings

If violations are identified, take the following action:

Delete users from A

Remove Inactive Guest Users

Remove users who do not have any activities in SharePoint Online sites, Groups, and Teams.

Rule Settings

* Remove users if they do not have any activities for:

60 Days

If violations are identified, take the following action:

Delete users from Azure AD

Send e-mail notifications of the violations to the following users:

RB Rita Brewer RH Ray Hill WG Wojciech Gajda

Cancel OK

Next Steps:

- “Kick the tires” on our AvePoint Cloud Governance or Policies and Insights at www.avepoint.com
- For a demo or half-day planning session, contact your AvePoint representative or reach out to sales@avepoint.com

On-demand resources!

[See Cloud Governance in action! How to videos available here...](https://www.youtube.com/playlist?list=PlyJFOtpJV3wPXygbKXJwLo5FCpoLrvS8)

<https://www.youtube.com/playlist?list=PlyJFOtpJV3wPXygbKXJwLo5FCpoLrvS8>

[See Policies and Insights in action! How to videos available here...](https://www.youtube.com/results?search_query=avepoint+how+to+policies+insights)

https://www.youtube.com/results?search_query=avepoint+how+to+policies+insights

[The difference between external access and guest access](https://www.avepoint.com/blog/microsoft-teams/microsoft-teams-external-guest-access/)

<https://www.avepoint.com/blog/microsoft-teams/microsoft-teams-external-guest-access/>



thank you

Gracias	ευχαριστώ	Danke	Grazie	благодаря
Hvala	Obrigado	Kiitos	شكراً	Tak
Ahsante	Teşekkürler	متشكراً	Salamat Po	감사합니다
Cám ơn	شكراً	Terima Kasih	Dank u Wel	Děkuji
நன்றி	Köszönöm	ありがとう ございます	ขอบคุณครับ	Dziękuję
谢谢	Tack	Mulțumesc	спасибо	Merci
תודה	多謝晒	дядкую	Ďakujem	



Sales@AvePoint.com | +1 800.661.6588



www.AvePoint.com



[in](#) [twitter](#) [youtube](#) [f](#) [g+](#)