



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://in.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://in.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?



External sharing

Guest access

Guest access in Teams lets people outside your organization access teams and channels. You can use the settings below to control which features guest users can or can't use. [Learn more](#)

Allow guest access in Teams ☒ On

Calling

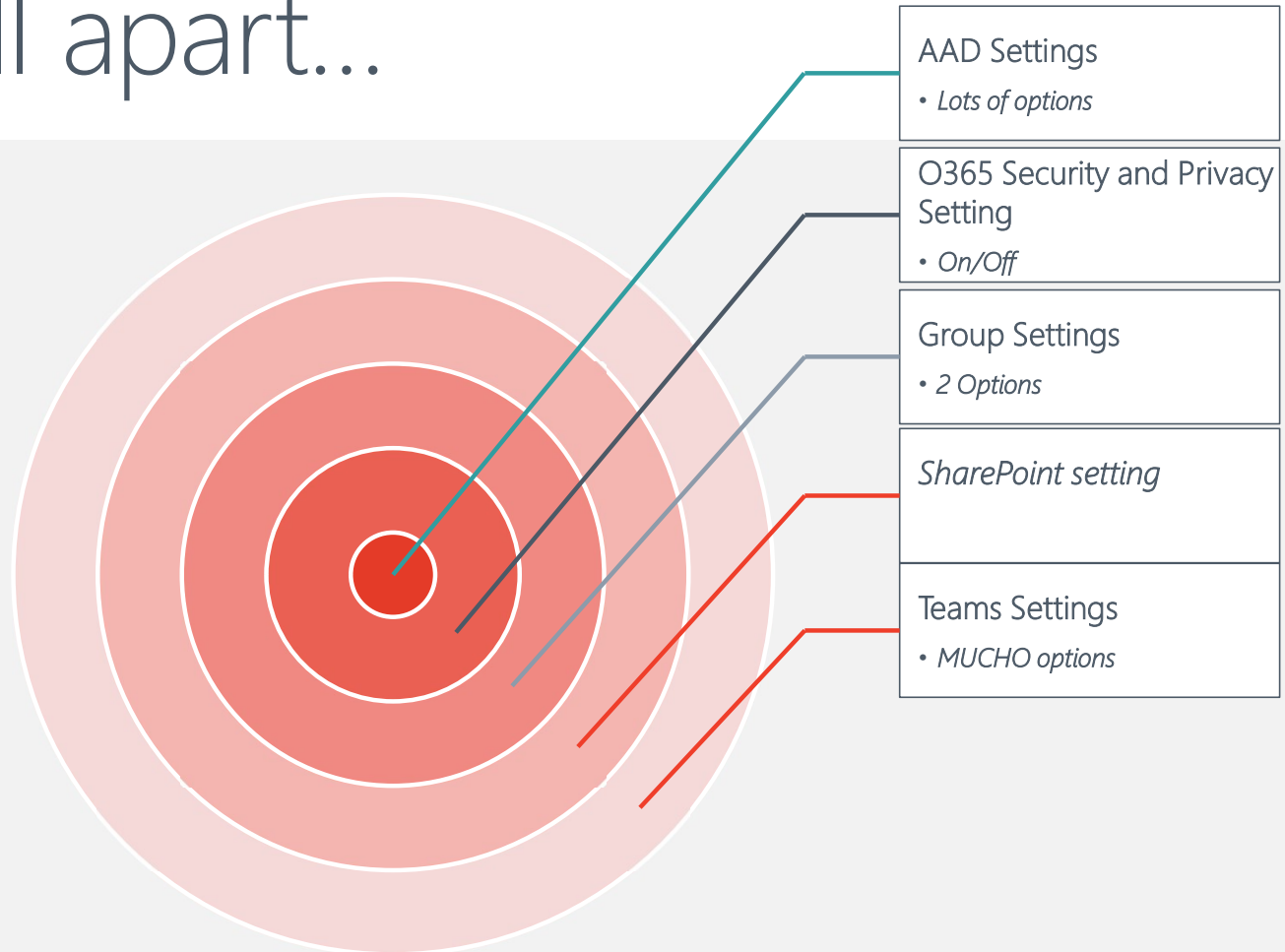
Manage calling specific controls for guest users.

Make private calls ☒ On

Meeting

Turn on or turn off settings for guests in meetings.

Peeling it all apart...



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

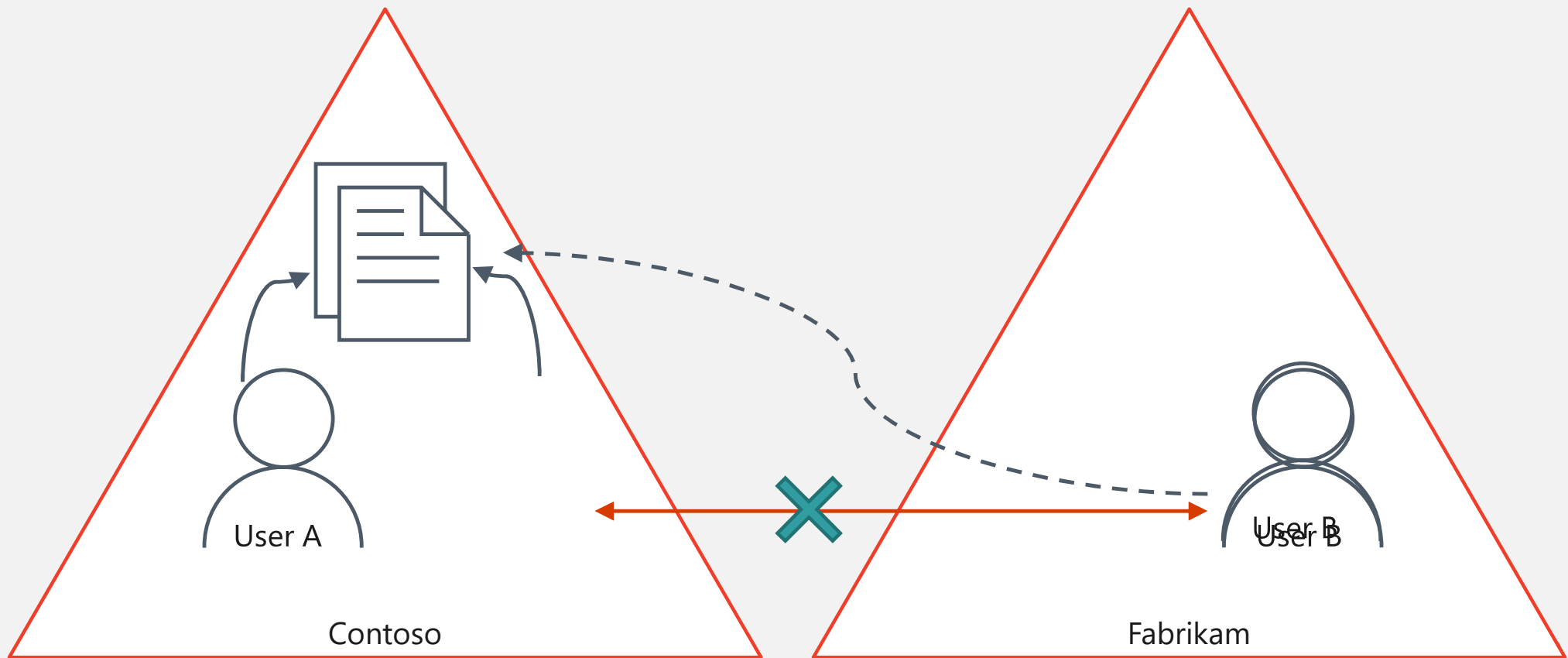
@JohnConnected

What exactly is a “guest”?

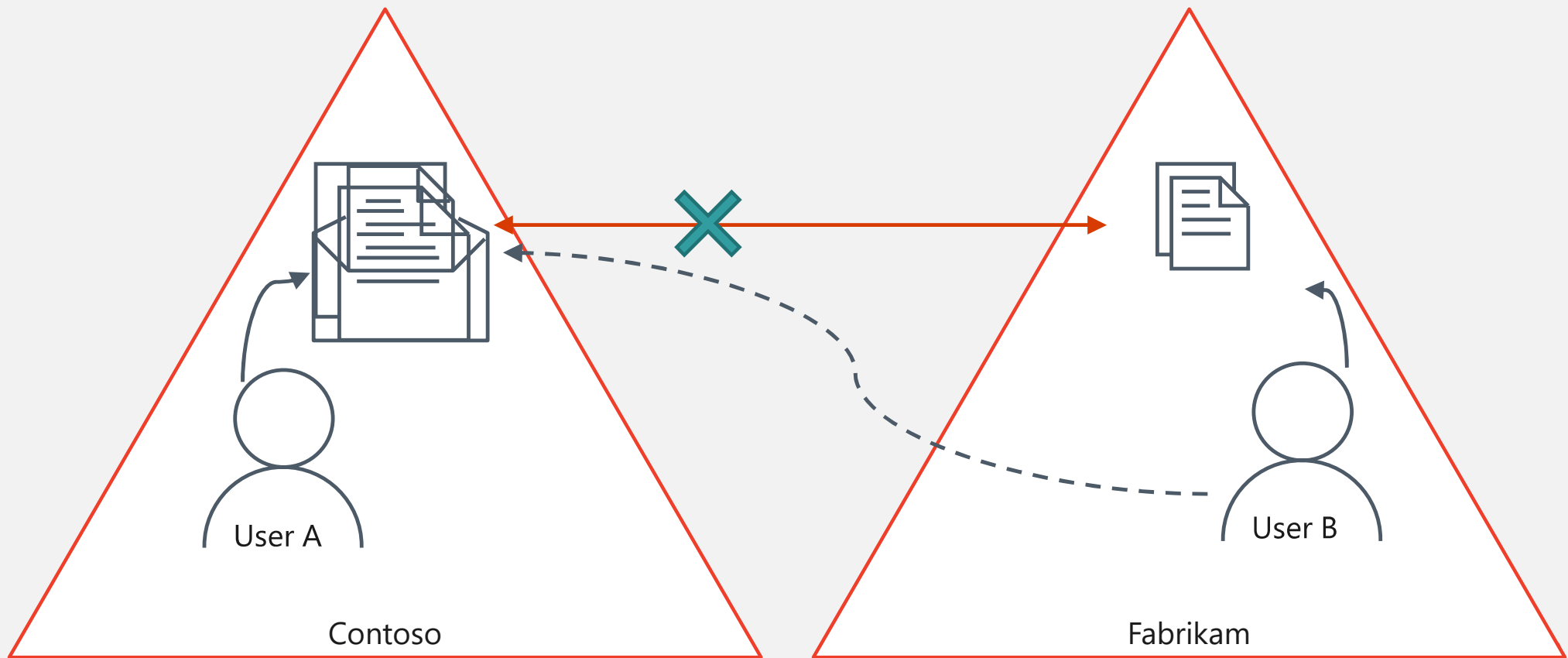
The most common scenarios...



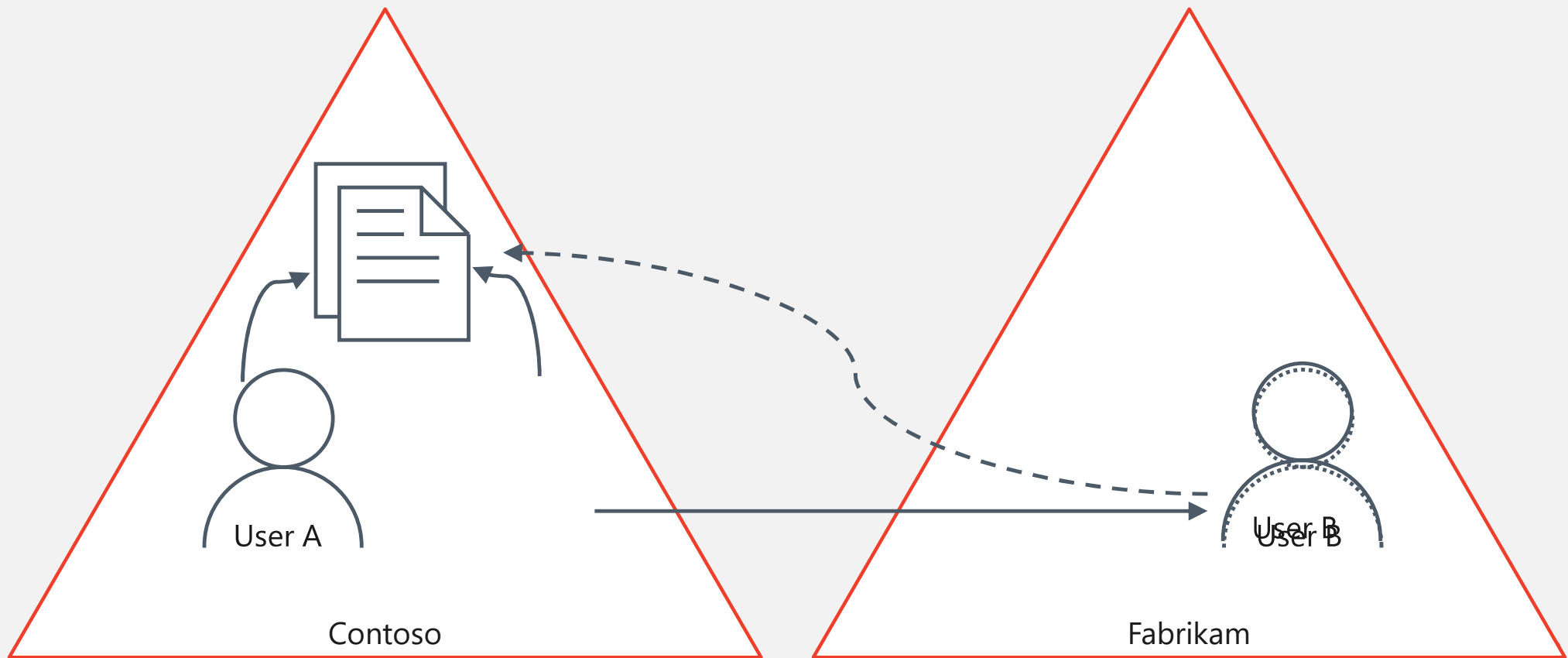
How we've shared externally in the past...



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 left-hand navigation pane includes sections for 'Dashboard', 'All services', 'FAVORITES', and a list of services: 'Azure Active Directory', 'Users', and 'Enterprise applications'. The main content area is titled 'External Identities | External collaboration settings' for the 'Contoso - Azure Active Directory' tenant. It features a search bar and 'Save'/'Discard' buttons. The settings are organized into several sections: 'Guest user access restrictions (Preview)' with three radio button options (the second is selected), 'Guest invite settings' with toggle switches for 'Admins and users in the guest inviter role can invite', 'Members can invite', and 'Guests can invite' (all are 'Yes'), 'Enable Email One-Time Passcode for guests (Preview)' (set to 'No'), 'Enable guest self-service sign up via user flows (Preview)' (set to 'No'), and 'Collaboration restrictions' with three radio button options (the second is selected). A mouse cursor is visible near the bottom right of the settings area.

Azure Active Directory admin center

Dashboard > Contoso > External Identities

External Identities | External collaboration settings

Contoso - Azure Active Directory

Search (Ctrl+/) Save Discard

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- ☐ 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

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

Enable Email One-Time Passcode for guests (Preview) ⓘ

[Learn more](#)

Yes No

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

- ☐ 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*...



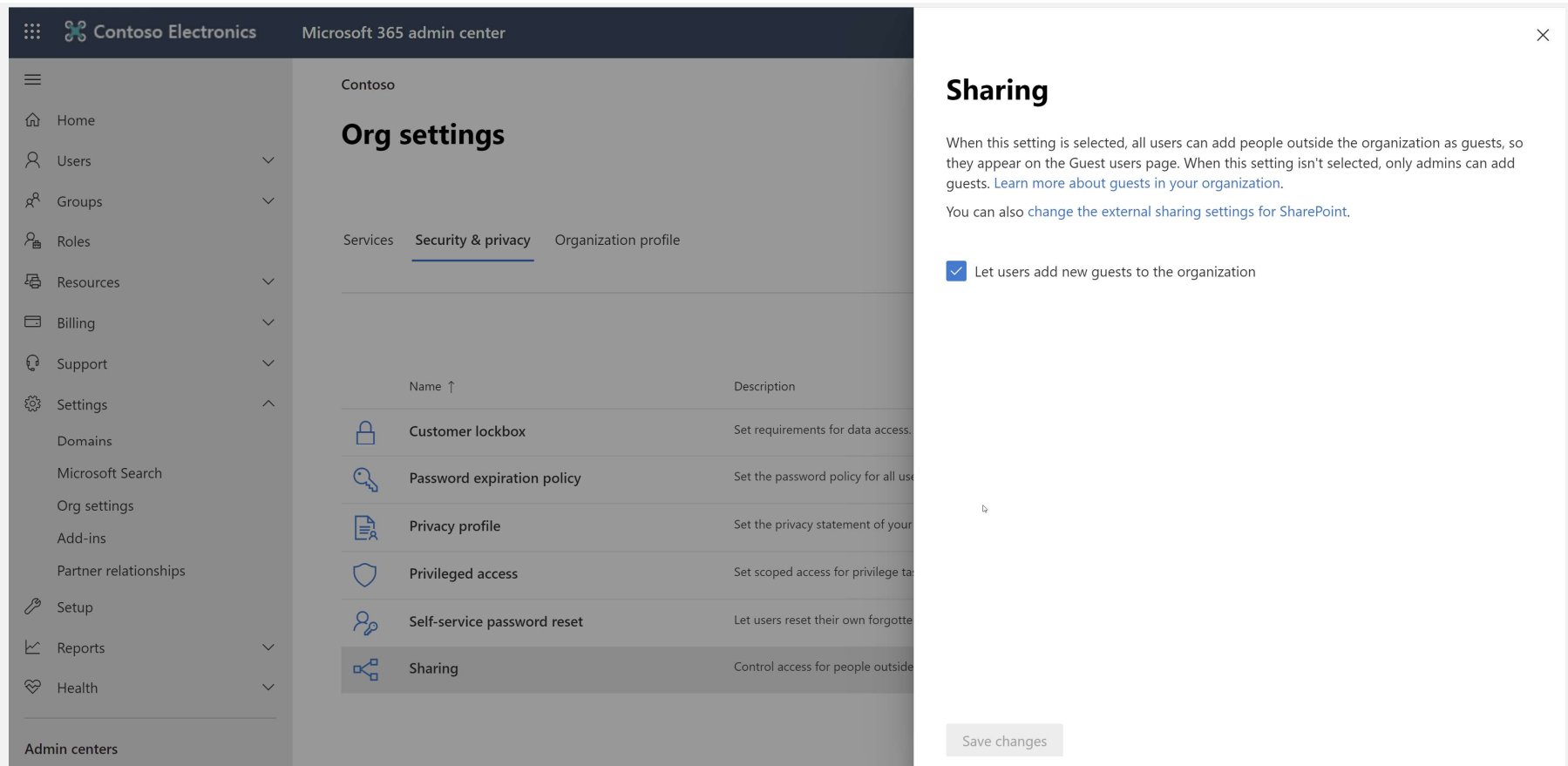
The “modern” way to
collaborate externally?



Demo:
*Configuring Teams and Groups for Guest
Access*



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



The screenshot displays the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar shows navigation options like Home, Users, Groups, Roles, Resources, Billing, Support, and Settings. The main content area is titled 'Org settings' and includes tabs for Services, Security & privacy (selected), and Organization profile. Under the 'Security & privacy' tab, a list of settings is shown, with 'Sharing' selected. The 'Sharing' settings panel on the right explains that when this setting is selected, all users can add people outside the organization as guests. It includes a checkbox labeled 'Let users add new guests to the organization', which is currently checked. A 'Save changes' button is located at the bottom of the panel.

Sharing

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.](#)

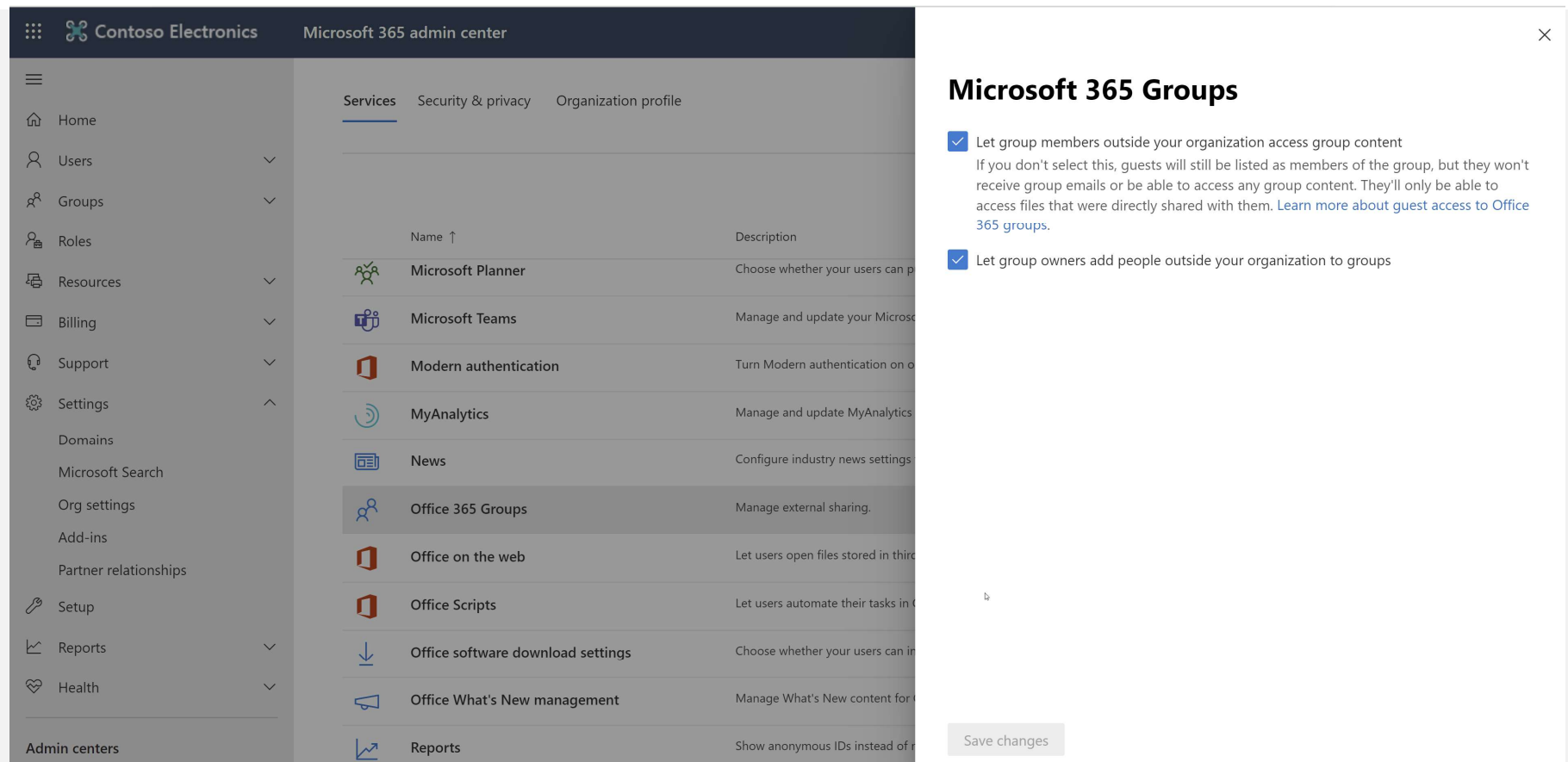
☒ Let users add new guests to the organization

Save changes

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



O365 Groups: Owners can *add* guests?



Contoso Electronics Microsoft 365 admin center

Services Security & privacy Organization profile

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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



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

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 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
```

Copy

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 Module](#) (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` 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 block guest access:

```
PowerShell

$GroupName = "<GroupName>"

Connect-AzureAD
```

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 displays the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar contains navigation options: Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, Health, Admin centers, Security, Compliance, Endpoint Manager, Azure Active Directory, Exchange, and SharePoint. The main content area shows the 'Services' tab with a list of services. The 'SharePoint' service is highlighted, and a settings panel is open on the right.

Name	Description
News	Choose how news about your organization is shared.
Office installation options	Choose how often users get feature updates.
Office on the web	Let users open files stored in third-party cloud storage.
Office Scripts	Let users automate their tasks in Office 365.
Reports	Show anonymous IDs instead of names in reports.
SharePoint	Control external sharing.
Sway	Manage sharing and content sources allowed for Sway.
User consent to apps	Choose whether users can consent to all apps.
User owned apps and services	Allow users to access the Office Store and other apps.
What's new in Office	Manage What's new messages for Office 365.
Whiteboard	Allow users to access Microsoft Whiteboard.

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

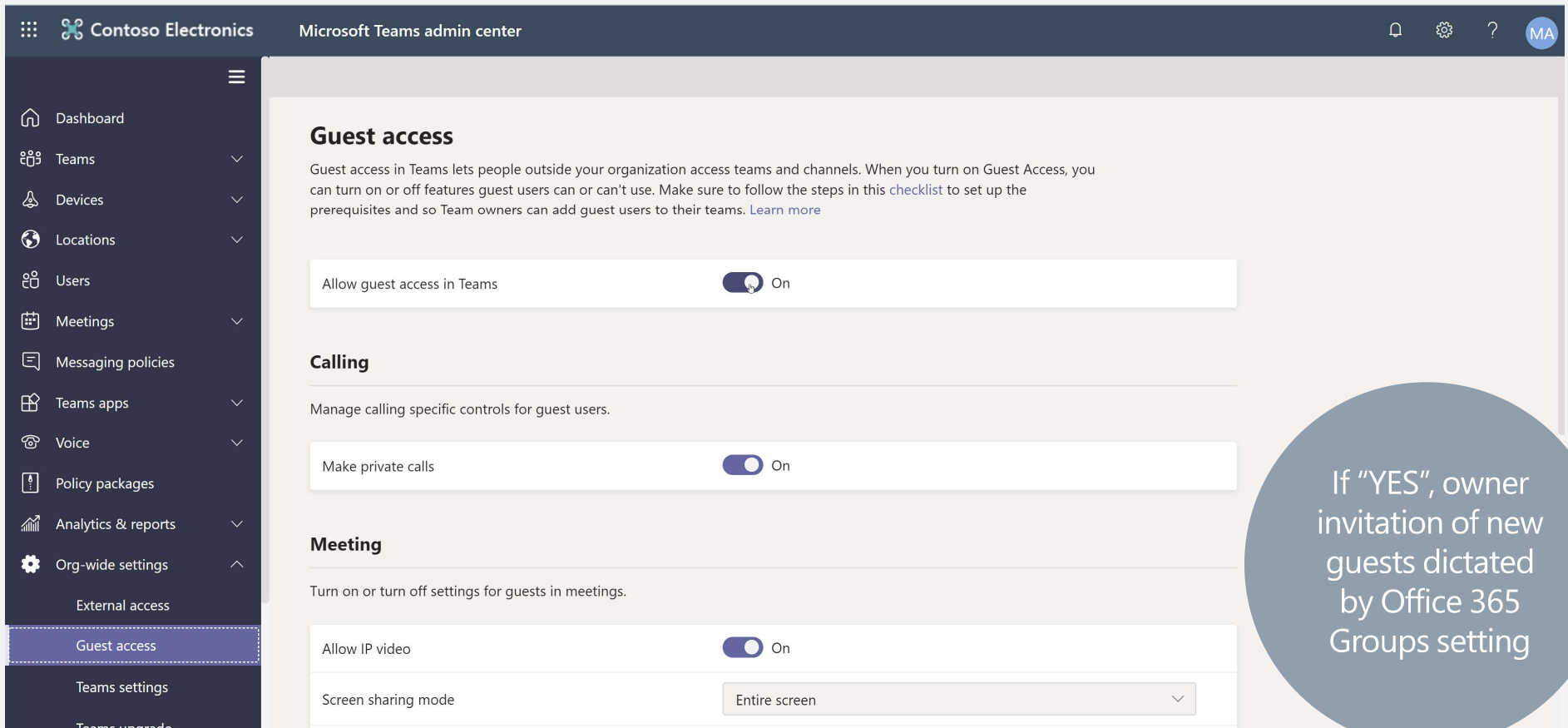
Advanced external sharing options

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 displays the Microsoft Teams admin center interface for 'Contoso Electronics'. The left-hand navigation pane includes options such as Dashboard, Teams, Devices, Locations, Users, Meetings, Messaging policies, Teams apps, Voice, Policy packages, Analytics & reports, Org-wide settings, External access, Guest access (highlighted), Teams settings, and Teams upgrade. The main content area is titled 'Microsoft Teams admin center' and features three sections: 'Guest access', 'Calling', and 'Meeting'. The 'Guest access' section includes a toggle for 'Allow guest access in Teams' which is currently turned 'On'. The 'Calling' section has a toggle for 'Make private calls' also turned 'On'. The 'Meeting' section includes a toggle for 'Allow IP video' turned 'On' and a dropdown for 'Screen sharing mode' set to 'Entire screen'. A blue circular callout on the right side of the interface contains the text: 'If "YES", owner invitation of new guests dictated by Office 365 Groups setting'.

Guest access

Guest access in Teams lets people outside your organization access teams and channels. When you turn on Guest Access, you can turn on or off features guest users can or can't use. Make sure to follow the steps in this [checklist](#) to set up the prerequisites and so Team owners can add guest users to their teams. [Learn more](#)

Allow guest access in Teams ☒ On

Calling

Manage calling specific controls for guest users.

Make private calls ☒ On

Meeting

Turn on or turn off settings for guests in meetings.

Allow IP video ☒ On

Screen sharing mode: Entire screen

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



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

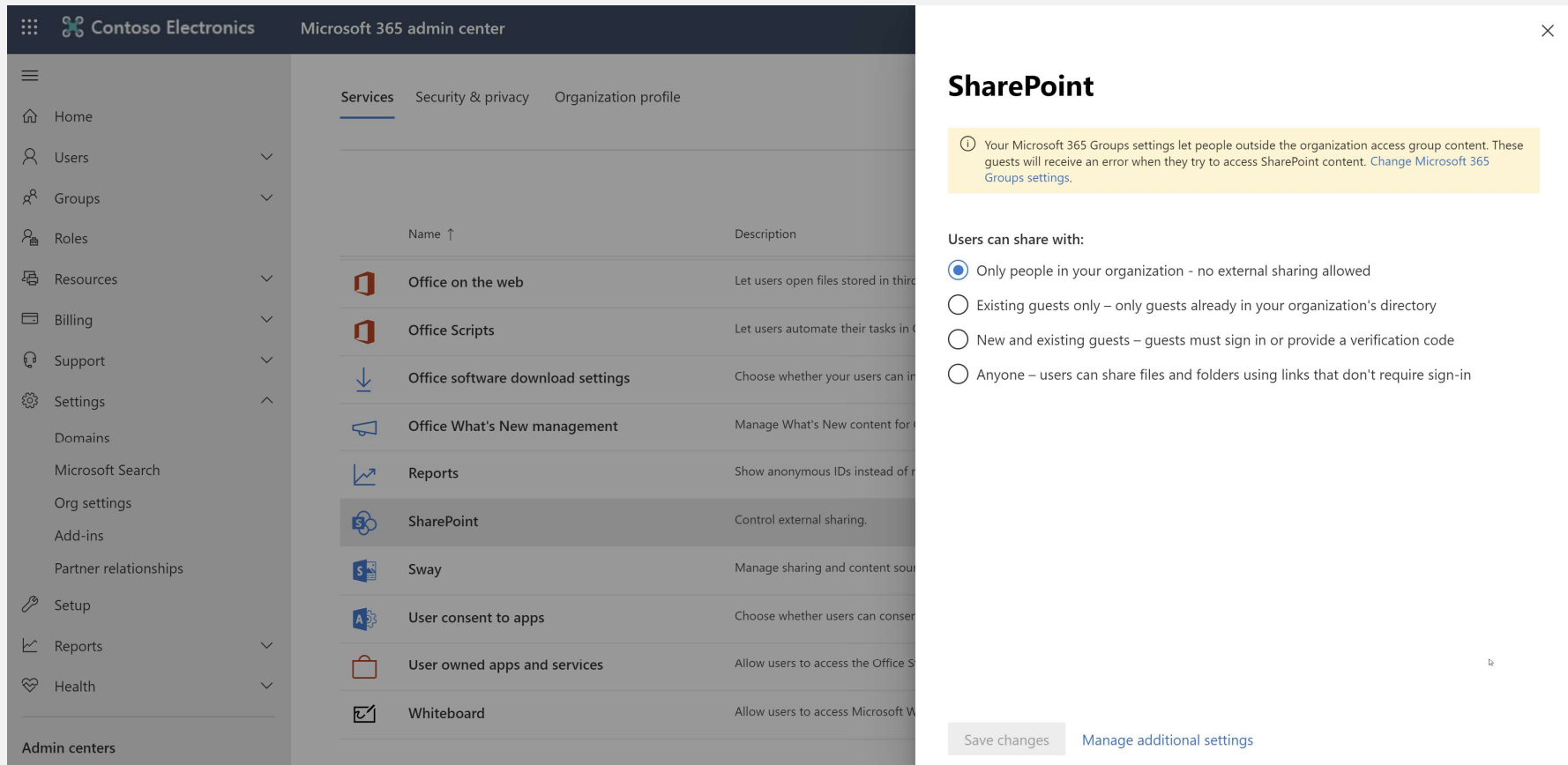
- They had external sharing before Azure B2B existed
- Looks like consolidation may be coming but it's early days, some preview functionality

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 storage 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.
SharePoint	Control external sharing.
Sway	Manage sharing and content sources for Sway.
User consent to apps	Choose whether users can consent to third-party apps.
User owned apps and services	Allow users to access the Office 365 Store.
Whiteboard	Allow users to access Microsoft Whiteboard.

SharePoint

① 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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



SharePoint: What are the *global* settings?

The screenshot shows the SharePoint admin center interface for 'Contoso Electronics'. The left sidebar contains navigation links: Home, Sites, Policies (selected), Settings, Content services, Migration, More features, OneDrive admin center, Customize navigation, and Show all. The main content area is titled 'Sharing' and includes a subtitle: 'Use these settings to control sharing at the organization level in SharePoint and OneDrive. Learn more'. Below this is the 'External sharing' section, which features two sliders for 'SharePoint' and 'OneDrive'. The 'SharePoint' slider is set to 'Least permissive' (bottom), and the 'OneDrive' slider is set to 'New and existing guests' (middle). The sharing levels are listed as follows: '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 sliders, a link states: 'You can further restrict sharing for each individual site and OneDrive. Learn how'. A dropdown menu labeled 'More external sharing settings' is expanded, showing 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).

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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



SharePoint: Should *this* site be more restrictive?

The screenshot displays the SharePoint admin center interface for 'Contoso Electronics'. The left sidebar contains navigation links: Home, Sites, Active sites (selected), Deleted sites, Policies, Settings, Content services, Migration, More features, OneDrive admin center, Customize navigation, and Show all. The main content area is titled 'Active sites' and includes a table of active sites. The 'Conference Team' site is selected, and its 'Sharing' settings are shown in a right-hand pane.

Active sites

Use this page to manage all your sites. [Learn more](#)

+ Create Permissions Hub Sharing Delete

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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



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

The screenshot displays a SharePoint site for 'Contoso Electronics' with the title 'DTC Workshop Planning'. The site is a private group. The main content area shows a list of documents and folders, including 'Presentation Prep', 'DTC Workshop Planning Notebook', and 'General'. A 'Run report' button is visible in the 'Shared with external users' section. A dialog box titled 'Documents' is open, prompting the user to 'Choose a destination to save this report'. The dialog shows a list of folders: 'General' and 'Presentation Prep'. The 'Presentation Prep' folder is selected. The dialog also includes 'Save' and 'Cancel' buttons.

Contoso Electronics SharePoint

DTC Workshop Planning Private group

Home New Page details

Search

Following 3 members

with news on your

able to quickly author report, or even just h...

Quick links

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

Documents

- New
- All Documents
- Name
- General
- Presentation Prep

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

Most unique viewers

Last 7 days

Most viewed

Last 7 days

This folder is empty

Shared with external users

Run report

This folder is empty

Most unique viewers

This folder is empty

Shared with external users

Run report

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

Shared with external users

Run report

Documents

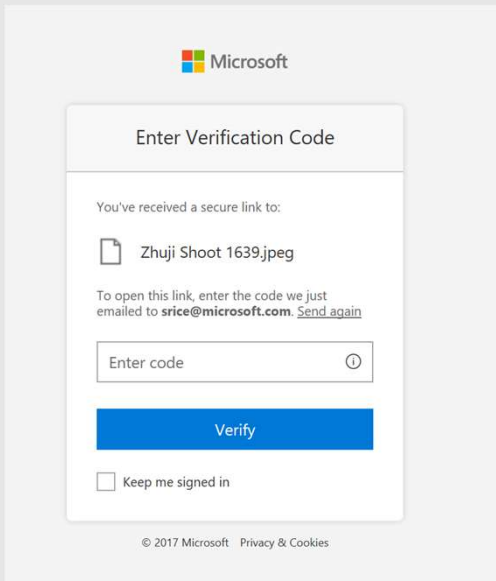
Choose a destination to save this report

- Name
- General
- Presentation Prep

Save Cancel

@JohnConr


NEW! Azure AD B2B for one-time passcode users



Microsoft

Enter Verification Code

You've received a secure link to:

 Zhuji Shoot 1639.jpeg

To open this link, enter the code we just emailed to srice@microsoft.com. [Send again](#)

Enter code

☐ Keep me signed in

© 2017 Microsoft Privacy & Cookies

Share securely with anyone in the world

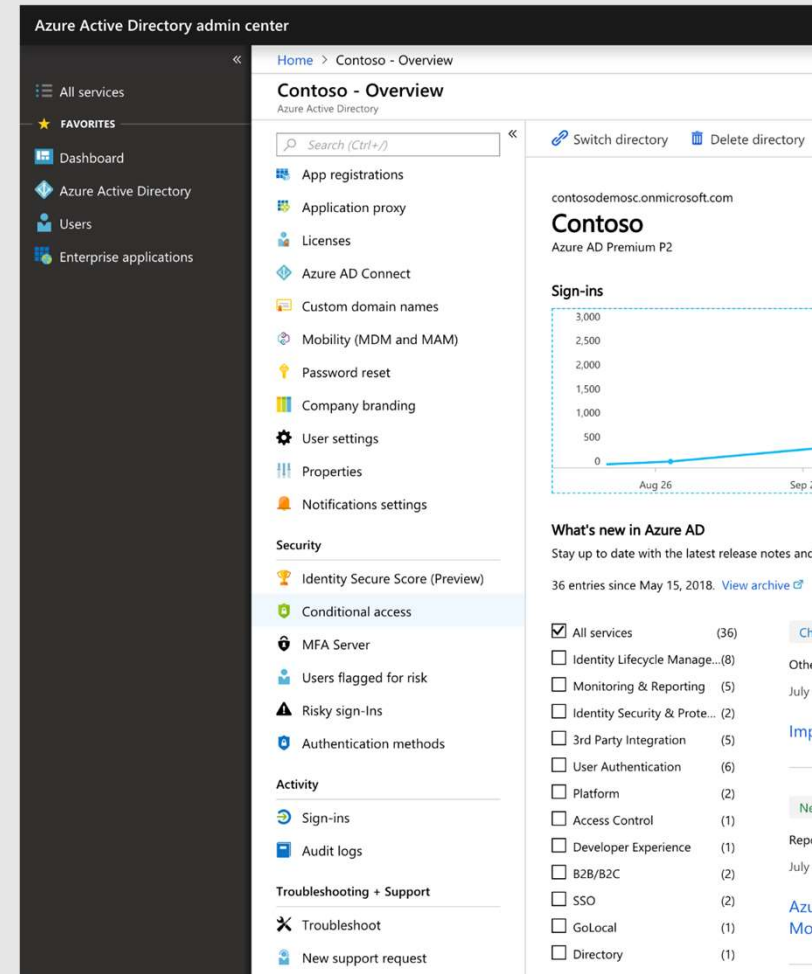
Simple verification with one-time passcode

AAD B2B guest management

Conditional access

Google auth federation

Guest do not require O365 licenses



Azure Active Directory admin center

Home > Contoso - Overview

Contoso - Overview
Azure Active Directory

Search (Ctrl+F)

Switch directory Delete directory

contosodemosc.onmicrosoft.com
Contoso
Azure AD Premium P2

Sign-ins

3,000
2,500
2,000
1,500
1,000
500
0

Aug 26 Sep 2

What's new in Azure AD
Stay up to date with the latest release notes and...
36 entries since May 15, 2018. [View archive](#)

☒ All services (36)
☐ Identity Lifecycle Manage... (8)
☐ Monitoring & Reporting (5)
☐ Identity Security & Prote... (2)
☐ 3rd Party Integration (5)
☐ User Authentication (6)
☐ Platform (2)
☐ Access Control (1)
☐ Developer Experience (1)
☐ B2B/B2C (2)
☐ SSO (2)
☐ GoLocal (1)
☐ Directory (1)

Security

- Identity Secure Score (Preview)
- Conditional access
- MFA Server
- Users flagged for risk
- Risky sign-ins
- Authentication methods

Activity

- Sign-ins
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

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?

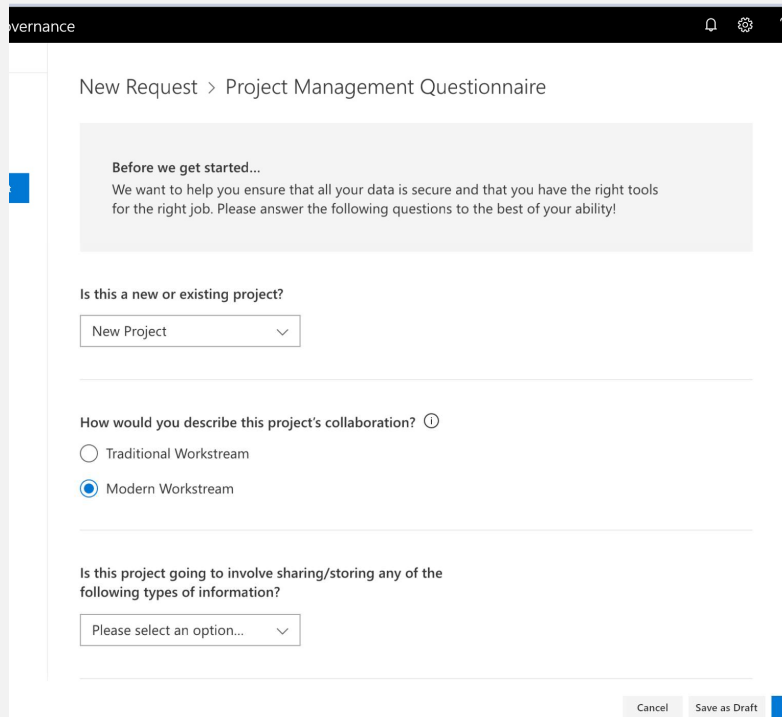
How will you handle the lifecycle of guests?

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 'Governance' with a 'New Request > Project Management Questionnaire' header. 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!'. Below this, the first question is 'Is this a new or existing project?' with a dropdown menu showing 'New Project'. The second question is 'How would you describe this project's collaboration?' with two radio button options: 'Traditional Workstream' and 'Modern Workstream' (which is selected). The third question is 'Is this project going to involve sharing/storing any of the following types of information?' with a dropdown menu showing 'Please select an option...'. At the bottom right 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



Search To-do List

- Home
- Workspace
- Requests

+ New Request

New Request > Project Management Questionnaire

Before we get started...

We want to help you ensure that all your data is secure and that you are using the right tools for the right job. Please answer the following questions to the best of your knowledge.

Is this a new or existing project?

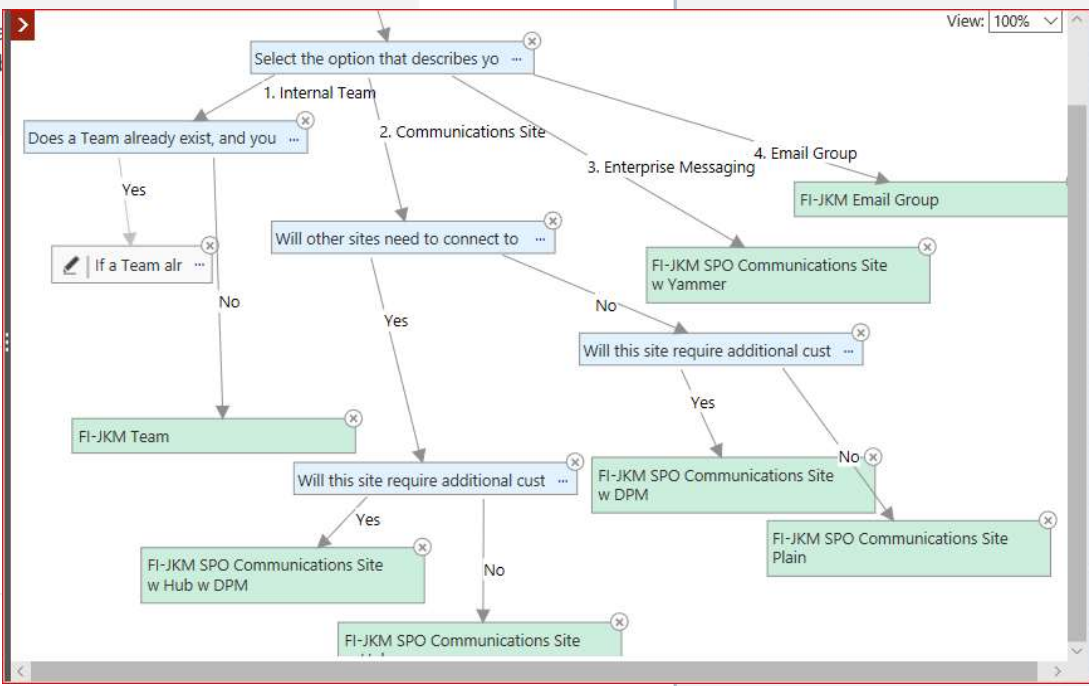
New Project

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

someone@example.com

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

The AvePoint logo, which is a stylized red 'A' shape with a small circle at the top right.

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:**

Group Property

***Property name:**

Newly Added Group/Team Members

***Condition:**

Select One

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



EXAMPLE

DEPARTMENT



DEPARTMENT



DEPARTMENT



**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.

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.

☒ 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)

☐ 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...

 **MyHub**

[Chat](#) [Home](#) [Start a request](#) [Workspaces](#) [Requests](#) [About](#)

To-do list

Approvals

Delete Office 365 Group/Microsoft Team Ext...

Group/Team Lifecycle Management

AT Auto-generated task

Confirmations

PM Extranet

Renew Site Collec

Renewal Pending

Q2 Outing

Renew Office 365 Group

Renewal Pending

Group renewal: Q2 Outing

Renewal steps

✓ Contact renewal

Confirm that the primary and secondary contacts are still correct. If necessary, you can assign the roles to other users.

✓ Permission renewal

Confirm that the group team site permissions for users and groups are still correct. If necessary, you can update the permissions.

⊞ Membership renewal

Confirm that the owners and members are still correct. If necessary, you can update the membership.


⊞ Metadata renewal

Confirm that the metadata is still correct. If necessary, you can update the metadata values.

[Add owner](#) [Add member](#) [Reset](#)

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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



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. On the left is a navigation pane with links to Home, Management, Services, Settings, and Directory. The main area is titled 'Services > Invite New Guest User > Edit' and contains three tabs: '1. Basic info', '2. Settings' (which is active), and '3. Advanced settings'. The 'Settings' tab includes fields for 'Microsoft 365 tenant' (set to 'AvePoint ATS Dev'), 'Primary contact' (set to '\$Requester'), and 'Secondary contact' (set to '\$Manager of Requester'). There are also checkboxes for 'Allow requesters to add guest users to groups or teams' and 'The requester is the owner of the group or team'. A 'Renewal profile' dropdown is set to 'Guest User Renewal'. On the right, a modal dialog titled 'Create guest user renewal profile' is open. It contains fields for 'Profile name' (set to 'Renew guests every 30d'), 'Description', 'Microsoft 365 tenant' (set to 'AvePoint ATS Dev'), and 'Category' (set to 'Lifecycle Management'). The 'Renewal process' section has radio buttons for 'Daily' (selected), 'Weekly', and 'Monthly', with a text input for 'Every 30 days'. There are also checkboxes for 'Specify the time to generate the first renewal task' and 'Renewal task will be overdue if the task assignee doesn't complete it within 7 Days'. The 'What user will be responsible for completing the renewal task?' field is set to '\$Primary guest contact'. The 'Notification e-mail template for assigned renewal tasks' is set to 'Built-in Guest User Renewal Process Assignment E-mail Template'. At the bottom of the dialog is a checkbox for 'Allow renewal task assignees to reassign tasks to other users'.

Services > Invite New Guest User > Edit

1. Basic info | 2. Settings | 3. Advanced settings

Microsoft 365 tenant *

AvePoint ATS Dev

Primary contact * ⓘ

\$Requester

Show this field as read-only to business users

Secondary contact ⓘ

\$Manager of Requester

Require business users to configure this field

Allow requesters to add guest users to groups or teams ⓘ

☒ The requester is the owner of the group or team

☒ The requester is the primary/secondary contact of the group or team

Renewal profile

Guest User Renewal

[View profile details](#)

Cancel Back Next

Create guest user renewal profile

Profile name *

Renew guests every 30d

Description

Microsoft 365 tenant *

AvePoint ATS Dev

Category *

Lifecycle Management

Renewal process

How often do you want renewal process to initiate? *

☒ Daily

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

7 Days * ⓘ

What user will be responsible for completing the renewal task? * ⓘ

\$Primary guest contact

Notification e-mail template for assigned renewal tasks *

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: Home, Management (Services, Guest renewal profil...), Settings (MyHub settings, System settings), and Directory (Workspace report, Guest user report). The main area shows the 'Guest user report' with a table of users. The user 'Tom.Gawczynski' is selected, and a 'View details' panel is open on the right.

Existing guests can be imported for management as well!

Guest user report

Username	E-mail address	Primary contact
Gawczynski.Tom	tomg.avepoint@gmail.com	Ray Hill
Tom.Gawczynski	tomgawczynski@gmail.com	Ray Hill

View details: Tom.Gawczynski

Username: Tom.Gawczynski
First name: Tom
Last name: Gawczynski
E-mail address: tomgawczynski@gmail.com
Primary contact: Ray Hill
Secondary contact: Ian Anderson
Job title: Security Architect
Department: Collaboration
Renewal profile: Guest User Renewal
Invited by: Ray Hill
Status: Renewal pending

Workspace access

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



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. The left sidebar contains icons for Activity, Chat, AVA, Teams, Calendar, Files, MyHub, Apps, and Help. The main content area is divided into several sections:

- Home**: A tab with sub-tabs for Hubs, Workspaces, Requests, and Start a request.
- To-do list**: A section with a 'Due date' dropdown and a message: 'You have no approvals requiring action at this time.'
- Approvals**: A section with a 'Due date' dropdown and a message: 'You have no approvals requiring action at this time.'
- Confirmations**: A section with a 'Due date' dropdown and a list of items:
 - Tom.Gawczynski**: Renew guest user. Status: Renewal Pending.
 - Q2 Outing**: Renew Microsoft Team. Status: Renewal Pending.
 - External_Project X**: Renew Microsoft Team. Status: Renewal Pending.
 - Product UI Design**: Confirm Governance Details.
- News & Updates**: A section with a 'Search in Home' bar and a list of 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 necessarily 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...

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

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

Send e-mail notification

RB

 Rita Brewer

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

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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

شكريه

Terima Kasih

Dank u Wel

Děkuji

நன்றி

Köszönöm

ありがとう
ございます

ขอขอบคุณ

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+](#)