

Office 365 Transformation Beyond the Perimeter

*Episode 2: Secure Collaboration in
Microsoft Teams - Office 365 across
public sector departments and
externally across agencies.*

16 July, 2020 @ 14:00 BST

Reserve Your Spot



Introduction...



John Peluso

CTO, AvePoint Public Sector
Microsoft Regional Director

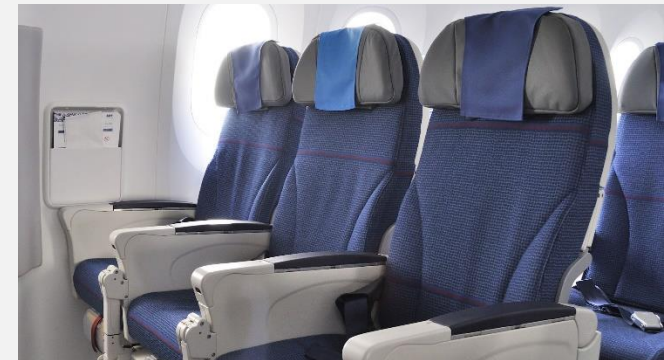
Email: John.Peluso@AvePoint.com

Twitter: www.twitter.com/johnconnected

LinkedIn: <https://www.linkedin.com/in/johnpeluso>

Blog: <https://www.avepoint.com/blog/author/john-pelusoavepoint-com/>

If all else fails: <http://johnpeluso.me>



Today's Agenda

The reality...

Why we're having this discussion

Why you may be confused...

And you *should* be! Understanding the fundamentals of Guest Access in Teams

The plot thickens...

What's with external sharing in SPO and ODFB?

Managing guests at scale...

Operationalizing external sharing for your organization with AvePoint





The Landscape of Office 365 External Sharing

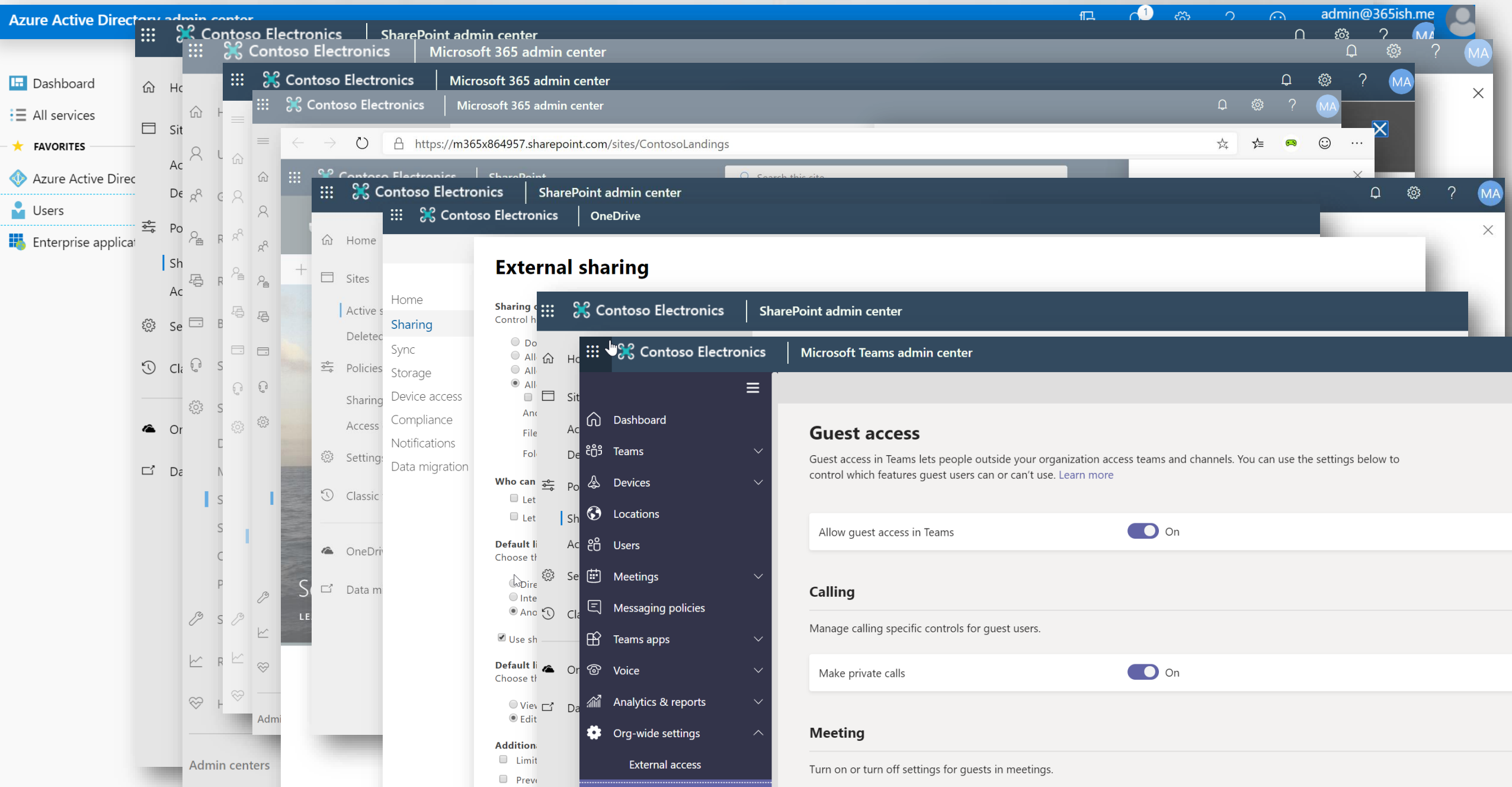
External collaboration in O365 is like an onion...

There are many layers to deal with

And...

If you do it wrong, it can make you tear up!



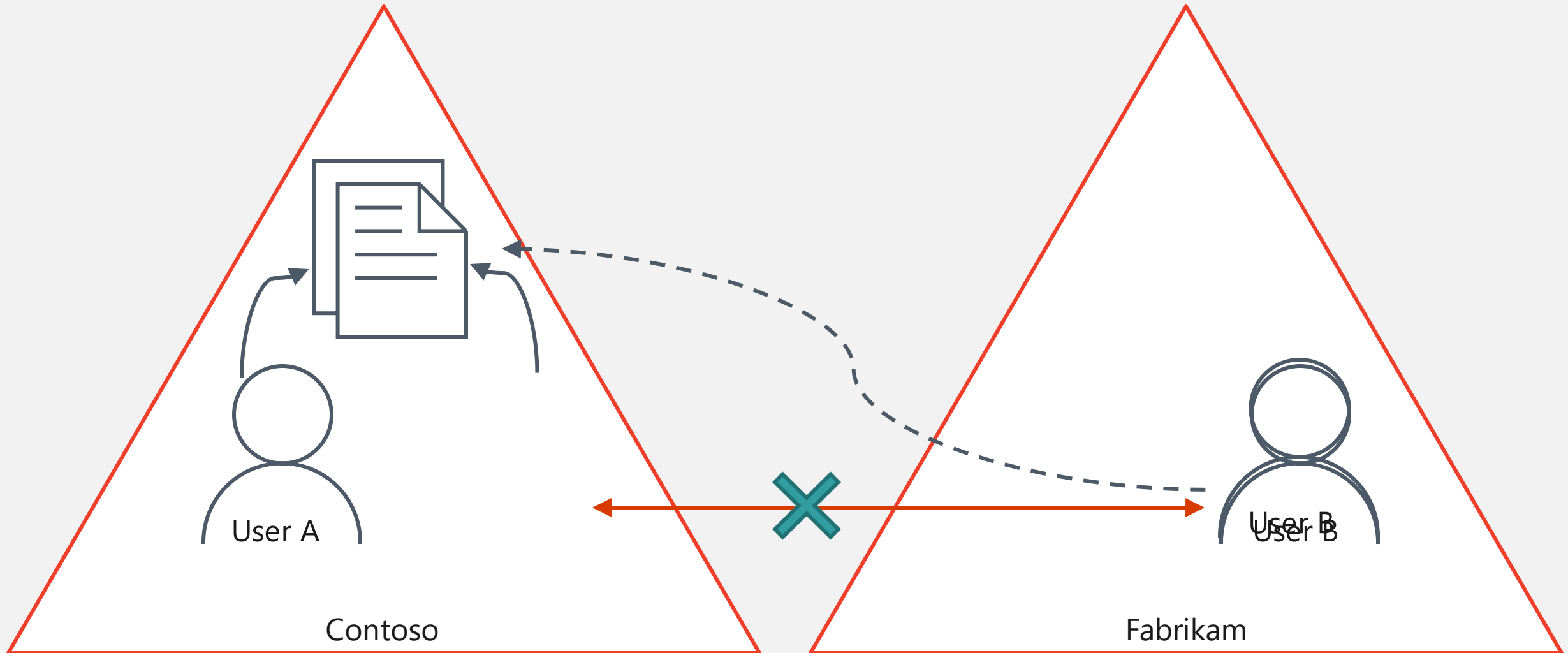




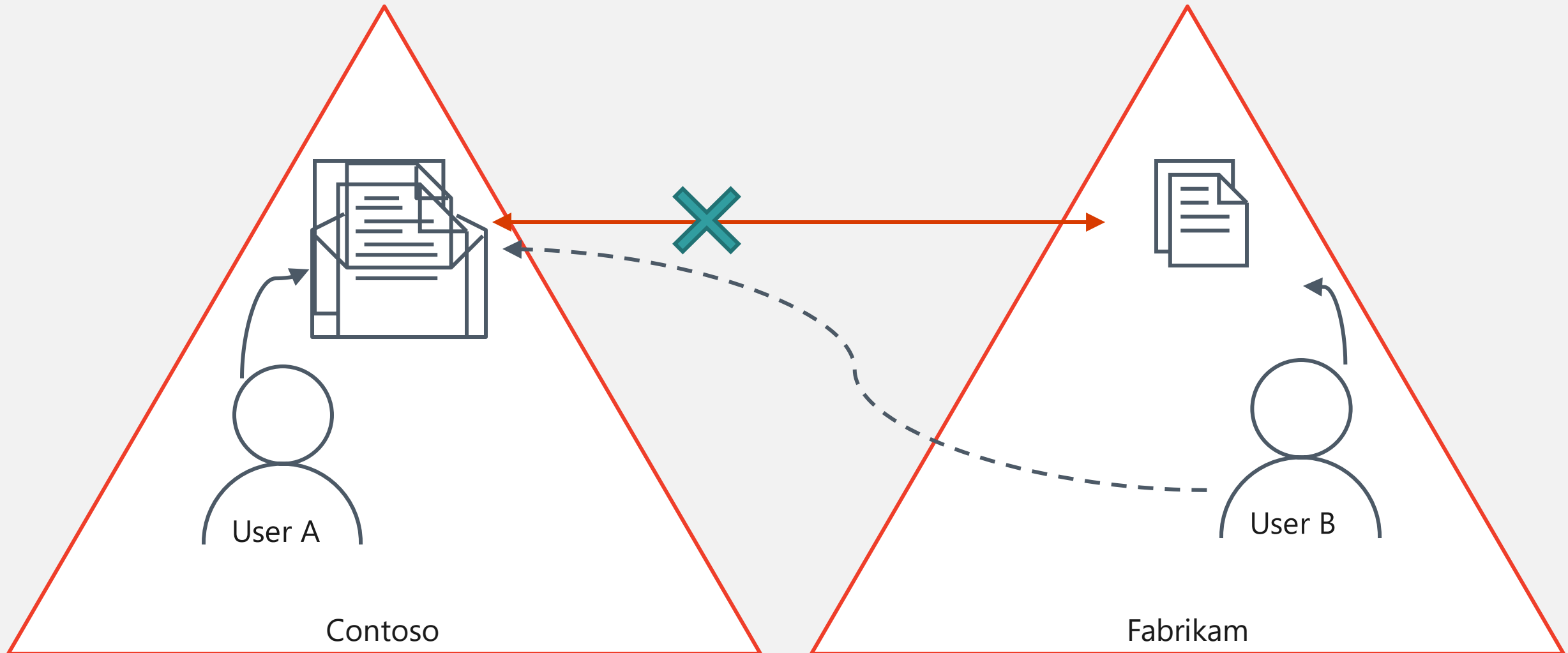


The Core: Azure
AD B2B

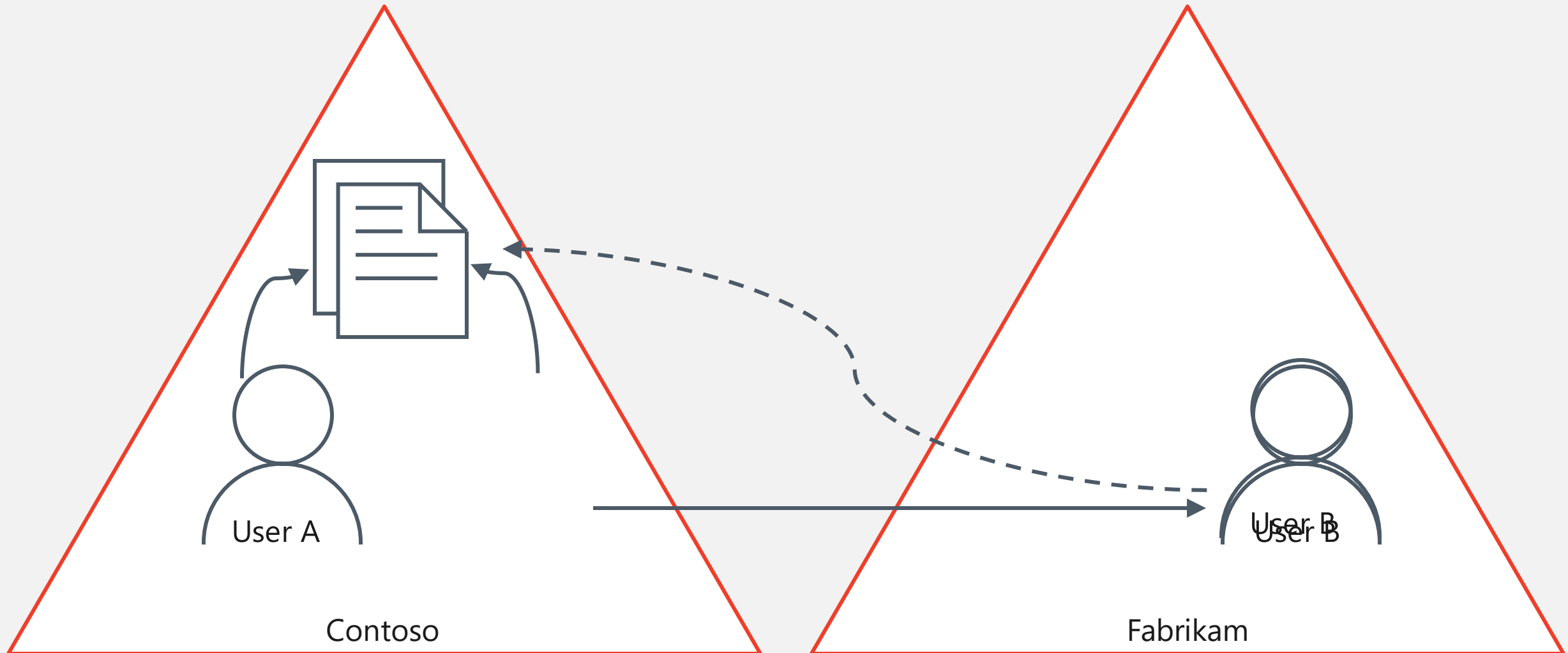
How we've shared externally in the past...



And this is even more common...



"Guest Users" in Azure Active Directory



Conditional access for guest users

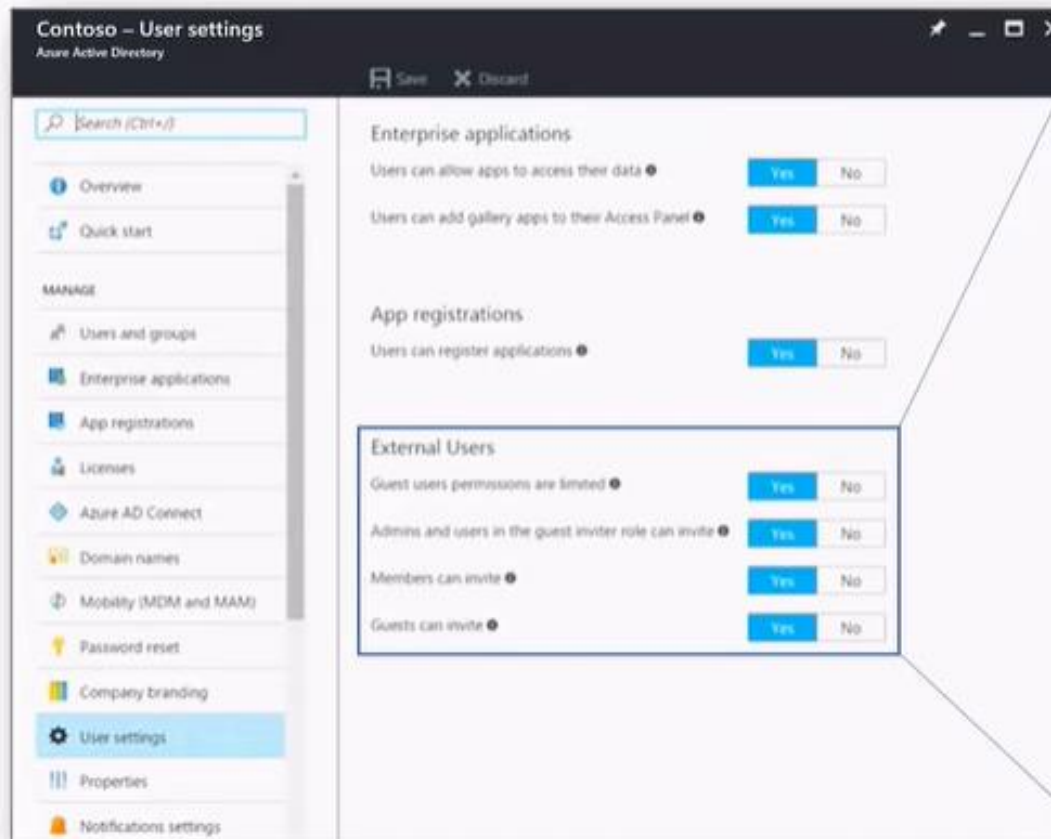
You can enforce conditional access policies on guests just like you would for any other user

Can also have policies *specific* to guests

The screenshot shows the 'New' conditional access policy configuration window in the Azure AD portal. The breadcrumb navigation at the top reads: Home > Contoso > Conditional access - Policies > New > Users and groups. The window is split into two panes. The left pane, titled 'New', contains an 'Info' section with a red asterisk and the label 'Name', followed by a text box containing 'Require guests to be on Network' with a green checkmark. Below this is an 'Assignments' section with three expandable options: 'Users and groups' (selected and highlighted in blue), 'Specific users included', and 'Cloud apps'. The right pane, titled 'Users and groups', shows two tabs: 'Include' (active, outlined in blue) and 'Exclude'. Under the 'Include' tab, there are three radio button options: 'None', 'All users', and 'Select users and groups' (selected). Below these are three checked checkboxes: 'All guest users (preview)', 'Directory roles (preview)', and 'Users and groups'. Each checkbox has an information icon to its right.

Configuring B2B settings in AAD...

Lever 1: Tenant level settings on Azure Active Directory



Guest users permission limited: No means guests and members have same access to directory data. **Yes** limits permission. Some Guests can be added to special access roles.

Admins and users in the guest inviter role can invite: Yes means users in the role can invite guests. **No** means admins or users can't.

Members can invite: No means that only admins can invite guests to your directory.

Guests can invite: No means guests can't invite other guests.
Default value is set to **Yes** for tenants.



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>

Demo:

Configuring Azure AD for "Guest" access



The Outer Layers

Things to know...

Guests are

- Anyone outside your organization/tenant
- Anyone with a work or consumer email account
- Added by Team owners or IT Admins



Guest license is

- Included as part of O365 subscriptions at no additional cost; up to 5 guests per one user on your tenant
- Subjected to Azure AD and O365 Service Limits

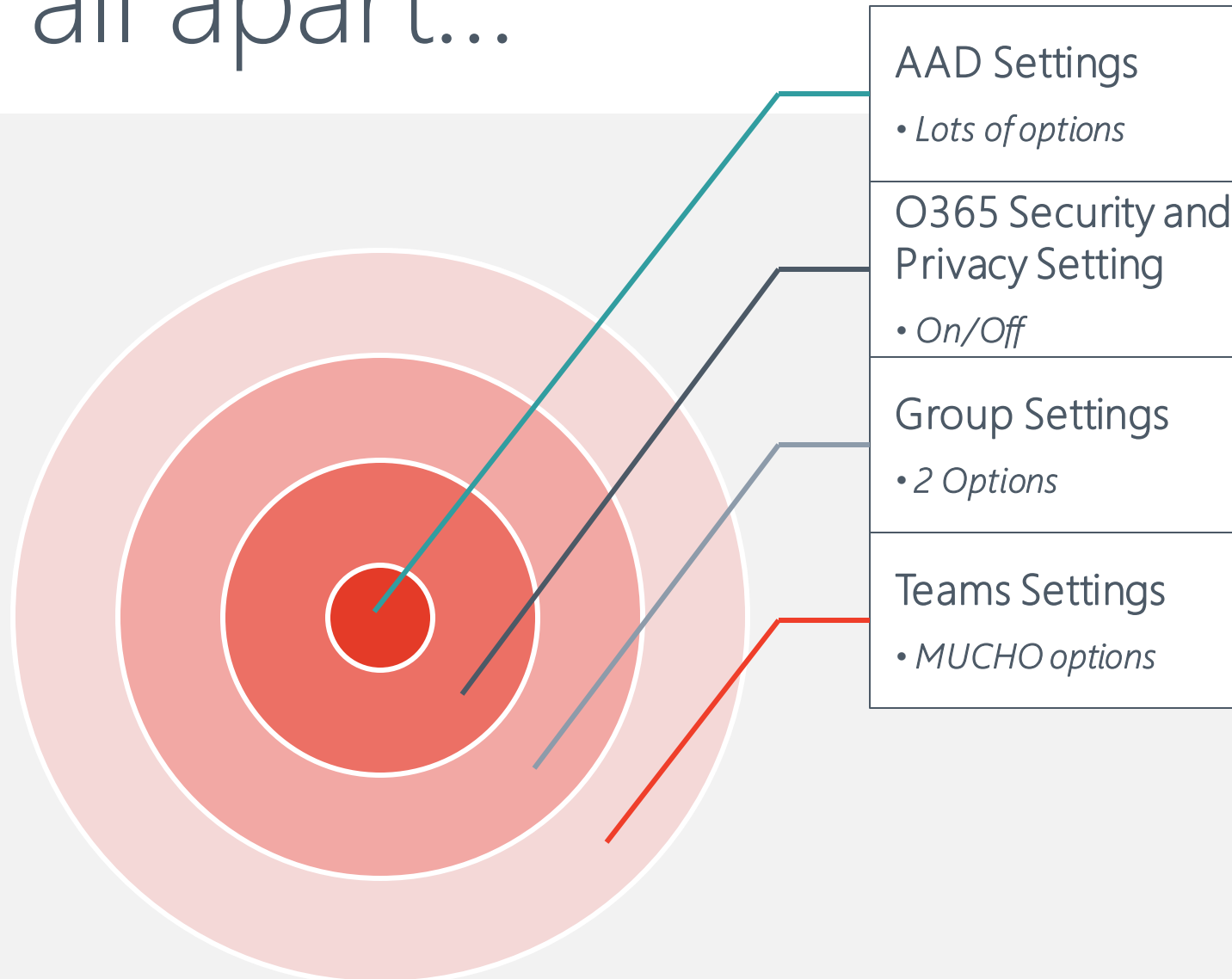


Guest are managed

- As users within the inviting tenant's Azure AD
- By the inviting tenant with Multi-Factor Auth, Mobile Device or Application Management, and Conditional Access Policies as applicable



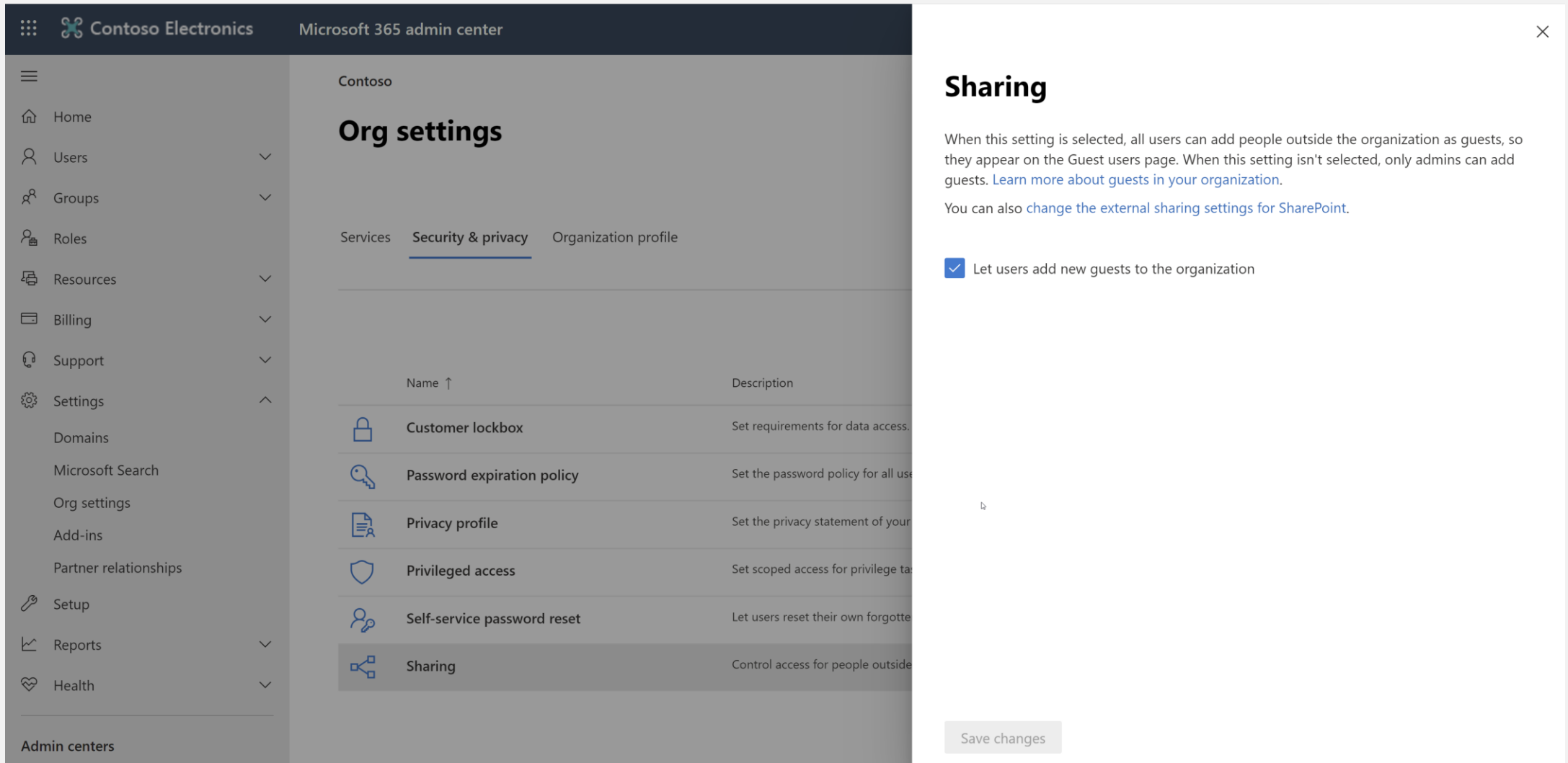
Peeling it all apart...



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



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



The screenshot displays the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar contains navigation links: Home, Users, Groups, Roles, Resources, Billing, Support, Settings (expanded), Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is titled 'Org settings' and includes tabs for Services, Security & privacy (selected), and Organization profile. A table lists various settings, with 'Sharing' highlighted at the bottom. An overlay window titled 'Sharing' is open on the right, providing details about the 'Let users add new guests to the organization' setting.

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

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



O365 Groups: Owners can *add* and/or *invite* 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 Microsc
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 C
Office software download settings	Choose whether your users can in
Office What's New management	Manage What's New content for c
Reports	Show anonymous IDs instead of r

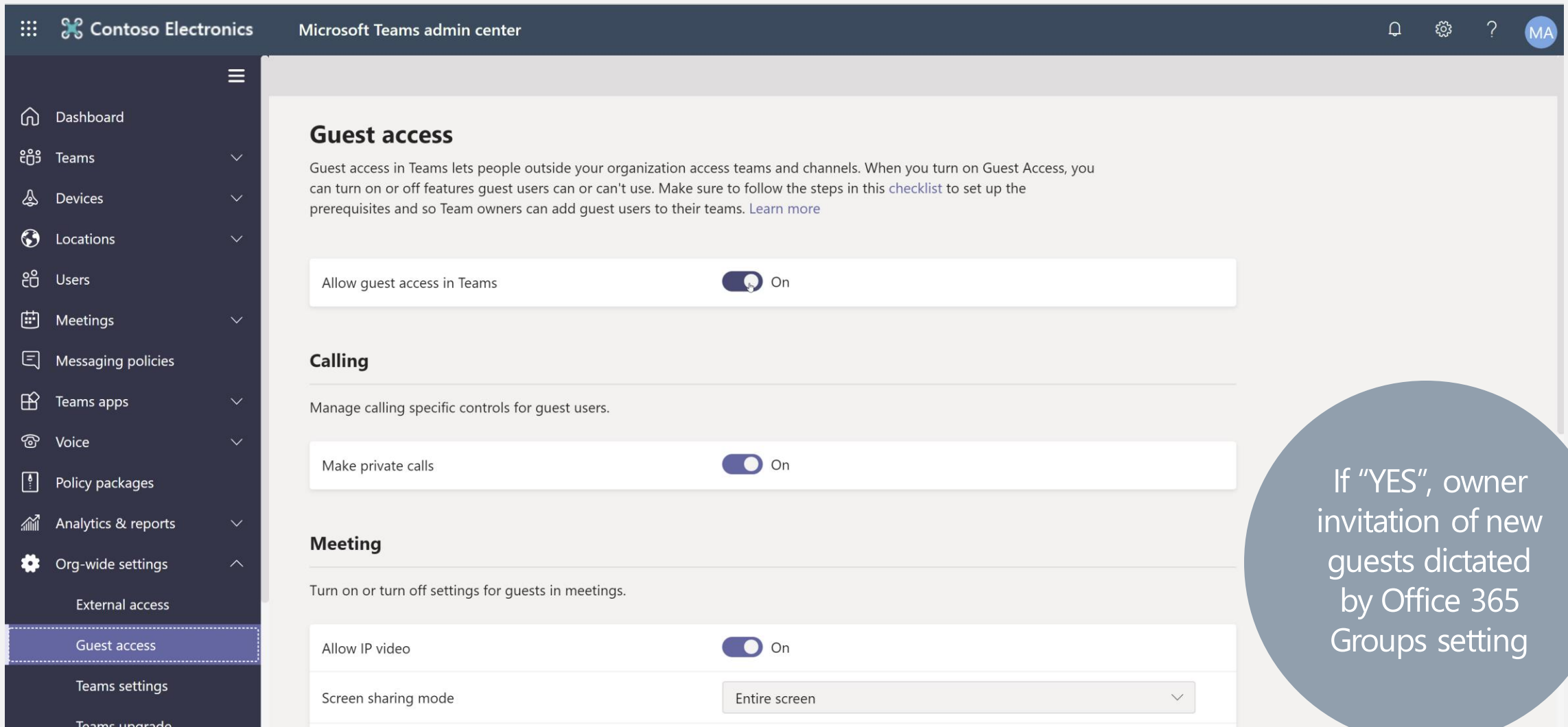
Microsoft 365 Groups

- ☒ 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



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 links to 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 set to 'On'. Below this, a text block explains that guest access allows external users to join teams and channels, and provides a link to a 'checklist' for setup prerequisites.
- Calling:** A section header followed by the instruction 'Manage calling specific controls for guest users.' and a toggle switch for 'Make private calls' set to 'On'.
- Meeting:** A section header followed by the instruction 'Turn on or turn off settings for guests in meetings.' and two settings:
 - 'Allow IP video' toggle switch set to 'On'.
 - 'Screen sharing mode' dropdown menu set to 'Entire screen'.

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



Teams+Groups: Should *this one* be more restrictive?

The screenshot shows the Microsoft Docs interface for the article "Use PowerShell to control guest access to a team". The page has a dark theme. At the top, there's a navigation bar with the Microsoft logo, "Docs", "Documentation", "Learn", "Q&A", and "Code Samples". A search bar and a "Sign in" link are on the right. Below this is a breadcrumb trail: "Microsoft Teams / Chat, teams, channels, and apps / Communicate with external users / Guest access / Use PowerShell to control guest access". On the right side of the breadcrumb trail are links for "Bookmark", "Feedback", "Edit", and "Share".

The left sidebar contains a "Filter by title" search box and a list of navigation items: "Add a guest to a team", "View guest users in a team", "Edit guest user information", "Use PowerShell to control guest access" (which is highlighted), and "Troubleshoot guest access". Below these are expandable sections: "Manage Teams", "Meetings and conferencing", "Cloud voice", "Adopt", "Upgrade to Teams", "Hybrid connectivity", "Microsoft 365 Business Voice", "Industries and government guidance", "Security, privacy, and compliance", "Monitor, maintain, and troubleshoot", and "Reference". At the bottom of the sidebar is a "Download PDF" link.

The main content area has the article title "Use PowerShell to control guest access to a team" in large white text. Below the title is the metadata: "06/24/2020 • 2 minutes to read • [author icons] +13 • Applies to: Microsoft Teams". The article text begins with "In addition to using the Microsoft 365 admin center and the Azure Active Directory (Azure AD) portal, you can use Windows PowerShell to control guest access. With PowerShell, you can do the following:" followed by a bulleted list:

- Allow or block guest access to all teams and Microsoft 365 Groups
- Allow guests to be added to all teams and Microsoft 365 Groups
- Allow or block guest users from a specific team or Microsoft 365 group

Below the list, the text says: "For details, see 'Use PowerShell to control guest access' in [Manage guest access in Microsoft 365 Groups](#)." The next paragraph states: "You can also use PowerShell to allow or block a guest user based on their domain. For example, let's say your business (Contoso) has a partnership with another business (Fabrikam). You can add Fabrikam to your Allow list so your users can add those guests to their groups. For more information, see [Allow/Block guest access to Microsoft 365 Groups](#)." The final paragraph reads: "If you want to block guests in Teams and still want to allow them to access SharePoint sites, you can use Azure AD Powershell cmdlets to disable the AllowGuestsToAccessGroups parameter on the Company object, assuming external sharing is turned on for SharePoint sites."

On the right side of the article, there's a section "Is this page helpful?" with "Yes" and "No" buttons. Below that is "In this article" with two links: "Use PowerShell to turn guest access on or off" and "Guest access vs. external access".

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



What guests in Teams can do...

Guests can

- Participate in private chat with other users in the team(s) to which they're invited
- Participate in a channel conversation in the invited Team
- Post, delete, and edit messages
- Share a channel file



Guests might

- Create a channel
- Invite a user outside the Office 365 tenant's domain

Only if Team owner allows



Guests cannot

- Create teams or meetings
- Discover and join public teams
- Share files over chat
- Add apps (tabs/bot/connectors)
- Access OneDrive for Business
- Change guest access policies
- Search for users outside the team(s) to which they're invited



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>



SharePoint Online
and ODFB...
a.k.a "the shallots"

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

Managing external sharing

- Control WHO can share to external users

Everyone

Only specific people

No one

- Control WHICH external users can be shared with

Anyone

Only authenticated users

Only authenticated users except specific domains

Only authenticated users in specific domains

No one

- Control WHAT can be shared externally

Anything

Only specific libraries

Only files without sensitive content

- Control HOW externally shareable links can be used

Default

Enabled, but not default

Mandatory expiration date

Block externally-shareable edit links

Disabled

SharePoint: Is "External Sharing" allowed?

Contoso Electronics Microsoft 365 admin center

Services Security & privacy Organization profile

Home Users Groups Roles Resources Billing Support Settings Domains Microsoft Search Org settings Add-ins Partner relationships Setup Reports Health Admin centers

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 apps.
Office software download settings	Choose whether your users can install Office software.
Office What's New management	Manage What's New content for Office apps.
Reports	Show anonymous IDs instead of real user IDs in reports.
SharePoint	Control external sharing.
Sway	Manage sharing and content sources for Sway.
User consent to apps	Choose whether users can consent to 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



SharePoint: What are the *global* settings?

The screenshot shows the SharePoint admin center interface. 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 has two sliders for 'SharePoint' and 'OneDrive'. The 'SharePoint' slider is set to 'Most permissive' (top), and the 'OneDrive' slider is set to 'Least permissive' (bottom). To the right of the sliders are four sharing options: '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, there is a link: 'You can further restrict sharing for each individual site and OneDrive. [Learn how](#)'. At the bottom, there is a section titled 'More external sharing settings' with a dropdown arrow. This section contains 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 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 site information. 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
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. The top navigation bar includes the 'Contoso Electronics' logo, the site name, and a search bar. The left sidebar shows the site structure with options like Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area is divided into sections: 'Most unique viewers' (Last 7 days), 'Most viewed' (Last 7 days), and 'Shared with external users'. The 'Shared with external users' section contains a 'Run report' button and a table of shared documents.

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

A 'Documents' dialog box is open, prompting the user to 'Choose a destination to save this report'. It shows a list of folders: 'General' and 'Presentation Prep'. The 'Save' button is highlighted.

Settings

- SharePoint
 - Add a page
 - Add an app
 - Site contents
 - Site information
 - Site permissions
 - Site usage
 - Change the look
 - Site designs
- Office 365

Quick links

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

with news on your

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

Most unique viewers

This folder is empty

Shared with external users

Run report

Documents

Choose a destination to save this report

Name

- General
- Presentation Prep

Save Cancel

@JohnConr

So...

Key take-aways...

- Yes, there are many interfaces, but it makes sense when you understand the layers
- Don't get duped by the duplication of settings in SPO/ODFB... they are redundant because they're a different kind of onion
- There should be plenty of options and flexibility to support most orgs
- Remember, some settings may take a while to apply
- Consider "users already in the directory" for SPO/ODFB to keep things centralized

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?

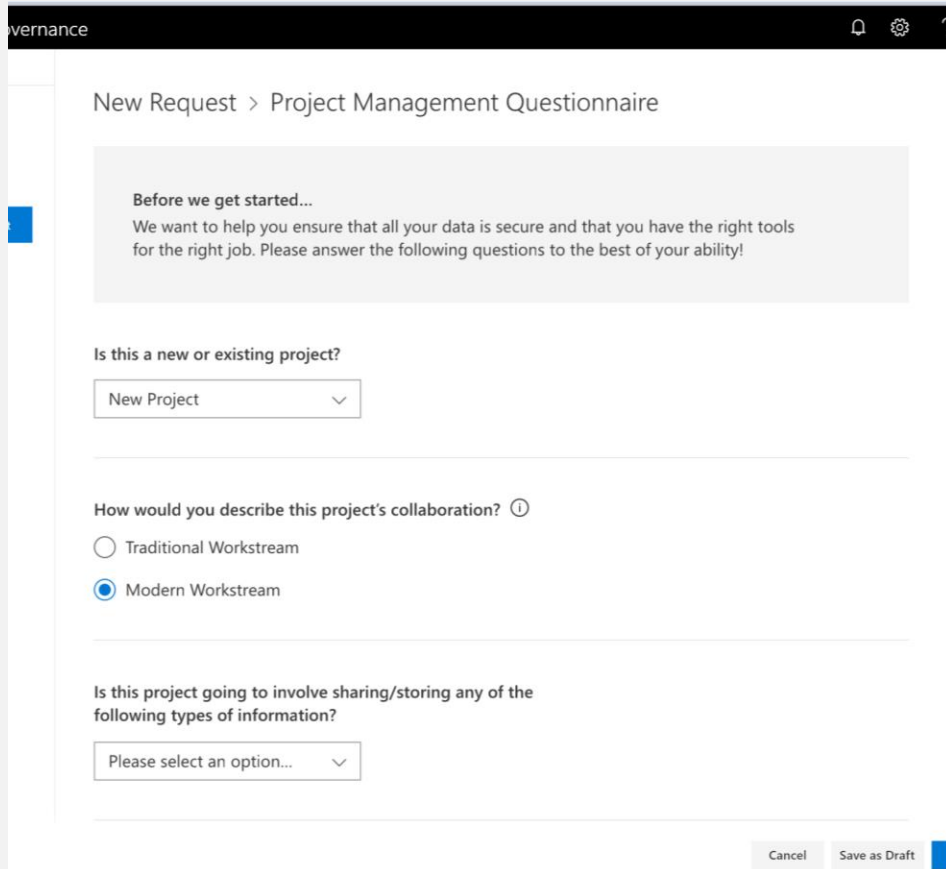
Monitoring, reporting, need for access, off-boarding.... How will this happen?

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



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 'New Request > Project Management Questionnaire'. It includes a header bar with 'Governance' and navigation icons. The main content area has a grey box with 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, there are three questions: 'Is this a new or existing project?' with a dropdown menu showing 'New Project'; 'How would you describe this project's collaboration?' with radio buttons for 'Traditional Workstream' and 'Modern Workstream' (selected); and '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, there 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



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



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?

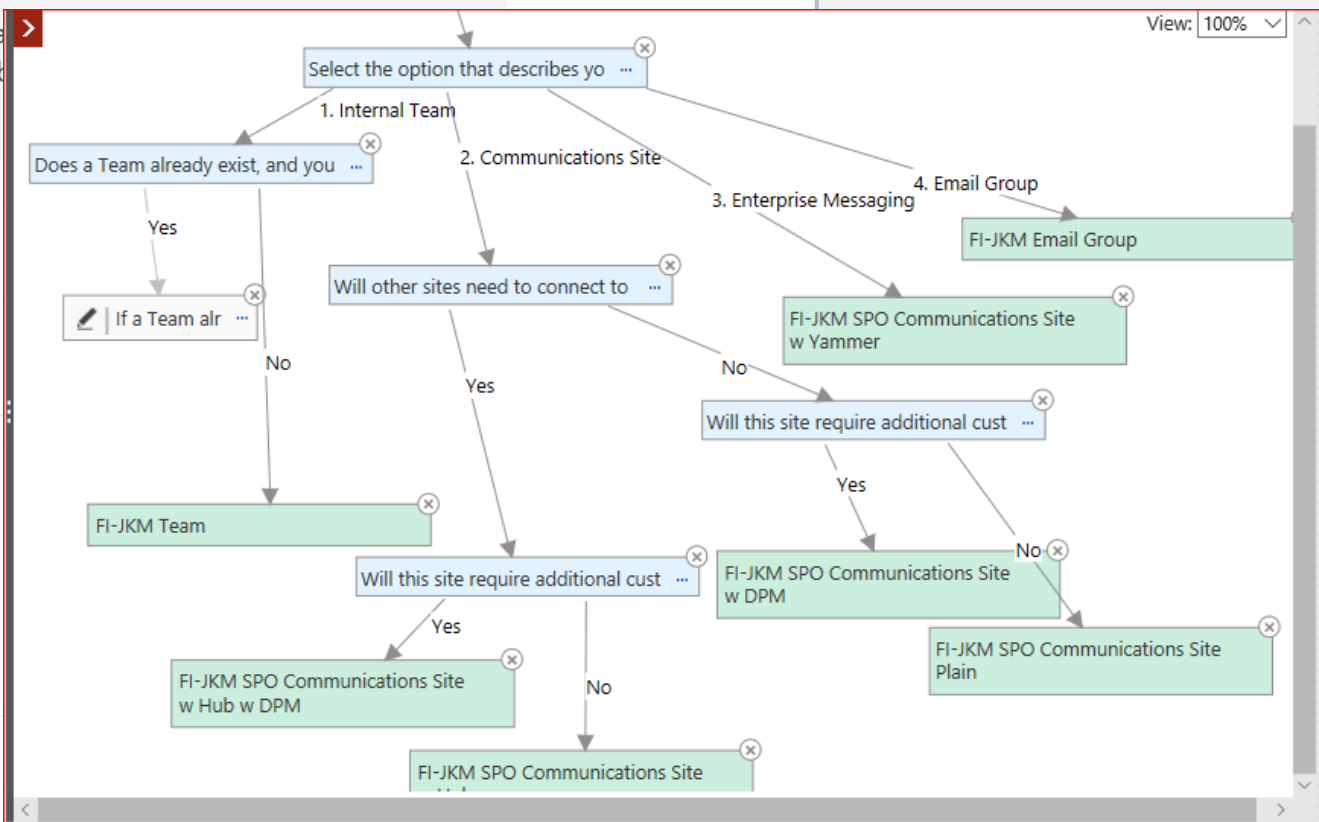
New Project

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
 -



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

Preview the approval process



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 'To-do list' on the left and a 'Group renewal: Q2 Outing' modal window in the center. The modal window contains a 'Renewal steps' section with four items: Contact renewal, Permission renewal, Membership renewal, and Metadata renewal. To the right of these steps is a table listing group members with columns for Username, User role, Change action, and Access type. The 'Access type' column is highlighted with a red box, showing 'Internal' for most users and 'External' for two others. In the background, a 'To-do list' shows a task 'Delete Office 365 Group/Microsoft Team Ext...' and a 'Confirmations' section lists 'PM Extranet' and 'Q2 Outing' with 'Renewal Pending' status.

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.

Group renewal: Q2 Outing

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

To-do list

Approvals Due date ▾

Delete Office 365 Group/Microsoft Team Ext...
Group/Team Lifecycle Management

AT Auto-generated task ✓ ✗ 🔄

Confirmations

PM Extranet
Renew Site Collection

Renewal Pending 🔄

Q2 Outing
Renew Office 365 Group

Renewal Pending 🔄



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 links: Home, Management, Services (selected), Settings, and Directory. Under 'Services', 'Guest renewal profil...' is visible. The main content area is titled 'Services > Invite New Guest User > Edit' and has three tabs: '1. Basic info', '2. Settings' (active), and '3. Advanced settings'. The 'Settings' tab contains several configuration options: 'Microsoft 365 tenant *' (AvePoint ATS Dev), 'Primary contact *' (\$Requester), 'Secondary contact' (\$Manager of Requester), and a toggle for 'Allow requesters to add guest users to groups or teams' (enabled). Below these are checkboxes for 'The requester is the owner of the group or team' and 'The requester is the primary/secondary contact of the group or team' (both checked). A 'Renewal profile' dropdown is set to 'Guest User Renewal'. The right panel, titled 'Create guest user renewal profile', contains fields for 'Profile name *' (Renew guests every 30d), 'Description', 'Microsoft 365 tenant *' (AvePoint ATS Dev), 'Category *' (Lifecycle Management), and a 'Renewal process' section. The 'Renewal process' section includes radio buttons for 'Daily' (selected), 'Weekly', and 'Monthly', and a checkbox for 'Specify the time to generate the first renewal task'. Below this is a field for '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 *' dropdown is set to 'Built-in Guest User Renewal Process Assignment E-mail Template'. At the bottom of the right panel is a checkbox for 'Allow renewal task assignees to reassign tasks to other users'.

AvePoint Cloud Governance

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), Directory (Workspace report, Guest user report), and the 'Guest user report' is currently selected. The main area shows a 'Guest user report' table with columns for Username, E-mail address, and Primary contact. Two users are listed: 'Gawczynski.Tom' and 'Tom.Gawczynski'. The latter is selected, and a 'View details' panel is open on the right. This panel shows the user's profile information, including contact details and workspace access. A red text overlay is positioned over the lower part of the interface.

Existing guests can be imported for management as well!

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



Demo:

End user self-service guest
request and renewal

Ongoing compliance for external access in SPO and ODFB with Policy Enforcer

Controlling External Sharing

Policy enforcer received a few crucial updates this month for external sharing in Office 365 SharePoint Sites and OneDrives for your customers:

- How do I find and report on sites that have external sharing enabled?
- How can I restrict external sharing to *only* specific groups or OneDrives?
- How can I reach back to existing sites to disable external sharing for external users?

Control Where and How External Sharing is Enabled

When customers apply policies for external sharing, Microsoft gives you "circuit-breaker" level controls for external sharing. You can set external sharing as a global setting for all SharePoint Sites and OneDrives in Office 365, which gives every site collection the option to enable external sharing or not. All sites and objects below a site collection that has external sharing enabled will allow external sharing as well. If you have tight controls over how site collections are provisioned and have external sharing as an approval workflow in Governance Automation, this may not be the best option.

For all other customers, Policy Enforcer is that vigilant control over where external sharing is permitted. Policy Enforcer adds controls for:

- Where external sharing is permitted based on site collection filters (titles, etc.)
- Types of external sharing options if it has been allowed (such as allowing anonymous access vs. authenticated users)
- What types of documents that can have guest links enabled
- What sites and documents can be shared through white-lists and black-lists, creating ethical walls internally (such as Engineering not being able to see "highly sensitive")
- How sites can be shared outside the organization with white-lists and black-lists of domains (such as preventing external sharing with competitors)

In addition, now that you have governance standards defined in policy enforcer, you can generate reports on areas where external sharing has been enabled out of compliance via the health dashboard.

<input type="checkbox"/>	Copy	Restrict or allow individual users or groups to copy SharePoint objec...	Copy
<input type="checkbox"/>	Custom Script Settings	Control custom script settings on SharePoint sites (except for OneDr...	Scan Site Collection Le...
<input type="checkbox"/>	Delete	Restrict or allow individual users or groups to delete items, files, list...	Delete
<input checked="" type="checkbox"/>	External Sharing Settings	Control the sharing settings of SharePoint sites.	Scan Site Collection Le...
<input type="checkbox"/>	Grant, Revoke and/or Modify Pe...	Restrict or allow individual users or groups to modify User and Grou...	Add Group Member;De...
<input type="checkbox"/>	Information Rights Management...	Control IRM settings for lists/libraries with a SharePoint 2013 experi...	Scan List Level Condition

Custom Action

If selected, any out of policy settings, objects and/or permissions will be reverted, restored or deleted based on the settings defined in this Policy Enforcer rule.

- ☒ Remove external users from the site collections where external sharing is disabled



DocAve


Management


Configuration


Security


Policy Enforcer


Plan Manager


 Add Rule


 Remove Rule


 Configure Rule


 Activate


 Deactivate

 Inherit

 Stop Inheriting

 Remove Profile

 Apply

 Cancel

Commit

Rule Management

Manage

 No profile is defined for the selected nodes. Choose a desired option to create a new profile.

Profile Name

Specify a name for the profile you are about to create. You can choose to reuse an existing profile and retain the rules and settings, copy from an existing profile and then customize it, or configure new rules and settings for the selected nodes.

- ☐ Reuse an existing profile
- ☐ Configure new rules and settings based on an existing profile
- ☒ Create my own rules and settings

* Name:

Off by Default Policy

Description:

These are default settings for Office 365 collaboration workspaces.

<input type="checkbox"/>	Rule Name	Status	Custom Action Settings	Notification Recipient	Parameter Status		
<input type="checkbox"/>	External Sharing Settings	✔	On		Default values	✗	
<input type="checkbox"/>	Information Rights Management (IRM) SharePoint...	✔	On		Default values	✗	
<input type="checkbox"/>	Site Collection Audit Settings	✔	On		Default values	✗	
<input type="checkbox"/>	User/Group Restriction	✔	On		Configured values	✗	
0 of 4 selected							
Show rows 15 Go to 1 of 1							



DocAve


Management


Configuration


Security


Policy Enforcer


Plan Manager


 Fix

 Manual Operation Required

 Hide

 Hidden List

 Export



 Close


Action




















Manage

Commit

 **Generate Report**

 Within policy  Out of Policy  Fixed automatically  Can be fixed  Requires manual operation  Error

input keywords to match url 

Scope 	URL	Status	Action	Profile
 https://m365x483549.sharepoint.com	https://m365x483549.sharepoint.com			Off by Default Policy
 https://m365x483549.sharepoint.com/portals/hub	https://m365x483549.sharepoint.com/portals/hub			Off by Default Policy
 https://m365x483549.sharepoint.com/search	https://m365x483549.sharepoint.com/search			Off by Default Policy
 https://m365x483549.sharepoint.com/sites/AdvancedeDiscovery	https://m365x483549.sharepoint.com/sites/AdvancedeDiscovery			Off by Default Policy
 https://m365x483549.sharepoint.com/sites/Analytics	https://m365x483549.sharepoint.com/sites/Analytics			Off by Default Policy
 https://m365x483549.sharepoint.com/sites/ContosoInsider	https://m365x483549.sharepoint.com/sites/ContosoInsider			Off by Default Policy
 https://m365x483549.sharepoint.com/sites/ContosoMarketingCen...	https://m365x483549.sharepoint.com/sites/ContosoMarketingCentral			Off by Default Policy
 https://m365x483549.sharepoint.com/sites/ProductMarketing	https://m365x483549.sharepoint.com/sites/ProductMarketing			Off by Default Policy
 https://m365x483549-my.sharepoint.com	https://m365x483549-my.sharepoint.com			Off by Default Policy


<


1


of 1

>


DocAveManagementSecurityPlan ManagerPolicy Enforcer

Fix

Manual Operation Required

Hide

Hidden ListExport

















Close

ActionManageCommit

Generate Report

 Within policy  Out of Policy  Fixed automatically  Can be fixed  Requires manual operation  Error

input keywords to match url

Scope	URL	Status	Action	Profile
▶  https://m365x483549.sharepoint.com	https://m365x483549.sharepoint.com	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/portals/hub	https://m365x483549.sharepoint.com/portals/hub	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/search	https://m365x483549.sharepoint.com/search	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/sites/AdvancedeDiscovery	https://m365x483549.sharepoint.com/sites/AdvancedeDiscovery	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/sites/Analytics	https://m365x483549.sharepoint.com/sites/Analytics	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/sites/ContosoInsider	https://m365x483549.sharepoint.com/sites/ContosoInsider	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/sites/ContosoMarketingCen...	https://m365x483549.sharepoint.com/sites/ContosoMarketingCentral	✓		Off by Default Policy
▶  https://m365x483549.sharepoint.com/sites/ProductMarketing	https://m365x483549.sharepoint.com/sites/ProductMarketing	✓		Off by Default Policy
▶  https://m365x483549-my.sharepoint.com	https://m365x483549-my.sharepoint.com	✓		Off by Default Policy
▶  User/Group Restriction ⓘ				
 /	https://m365x483549-my.sharepoint.com			
▶  Information Rights Management (IRM) SharePoint 2013 ⓘ				
▶  External Sharing Settings ⓘ				
 /	https://m365x483549-my.sharepoint.com			

<1of1>

Key Policy Enforcer Updates

The moment *Microsoft's activity feed* for Office 365 or Azure AD publishes changes, our tools can take corrective actions!

No "*full scans*" needed anymore, offline cache (after the initial sync) will always stay up to date from Microsoft's own reports!

Reusable filters help fill in where policies apply that can read Cloud Governance metadata, native classifications, etc.

First Release Rules	Value
Classification Protection	Keep Group / Team owners from modifying native classifications
External Sharing Settings	Govern Guest Access for individual Teams and Groups
Membership / Ownership Restriction	Whitelist / Blacklist users by name or AD properties (role, title, geography, dept, etc.)
Outlook Group Visibility	Controlling visibility of Groups / Teams upon creation to flag violations
Membership / Ownership Size	Cap the size of Members / Owners by a specific number, preventing top-heavy groups
Privacy Restriction	Prevent Groups / Teams from switching from Private to Public teams, affecting visibility
Access Request Settings	For SharePoint / OneDrive to enforce how permissions are processed
Deletion Restriction	Control SharePoint (libraries, sites) deletions to create a safer work environment
Permission Inheritance	Monitor for broken inheritance and standardize how information is shared
External User Scans	Identify external user access to SharePoint and OneDrive content
Site External Sharing Settings	Control the SharePoint and OneDrive external sharing settings for each site

Report on external users across SPO and ODFB with Security Search

Administrator > Security > Security Search Form Mode User: admin@odemo.me

DocAve Management Security Plan Manager Policy Enforcer

Security Search Deactivated Account Cleaner Job Monitor

Contribute Account Statistics

Scope

Input Keyword

My Registered Sites

- ☒ Default Office 365 Group Team Site Container
- ☐ Default OneDrive for Business Container
- ☐ Default Site Collection Container
- ☐ Group Team Sites
- ☐ Modern Sites
- ☐ Personal Sites

Security Search Form Mode

Change settings for: Logical Group{Default Office 365 Group Sites Group}

Create a new plan.

Plan Name
Choose a name and description for the plan you are about to create.

* Plan Name: Security Search 09:55:45 2019-09-24 Check

Description:

User Type
Choose what user types to search.

User and Group
Choose users and/or groups to search for.
Separate each username or group name with a semicolon.
Choose whether or not to include Active Directory group-membership details in the report or group names only.

Permission Settings
Limit search users or contents using permissions assigned to them.
Has Permissions -- base upon the permission which you select to limit the search result.
There are two options based on Has Permissions field:
Exact permission -- exactly meet the permission you have selected.

Select All

- ☒ Select All
- ☒ External User
- ☒ Users with Guest Links
- ☒ SharePoint User and Group

OK Cancel

SharePoint Groups:

☐ Include members of Active Directory groups in the search results

Has Permissions: Search for any Permission

☒ Exact permission

☐ Exact permission or better



Report on external sharing settings across SPO and ODFB with Report Center

Report Center > Administration Reports > Configuration Reports

User: admin@od

DocAve Administration Reports Compliance Reports DocAve Reports Settings

Configuration Reports Save Profile and Run Report Job Monitor

Administration Report Actions Statistics

* Report Profile Input/Select

1. Scope

Input Keyword

My Registered Sites

- Select All
- Default Office 365 Group Team Site Container
- Default OneDrive for Business Container
- Default Site Collection Container
- Group Team Sites
- Modern Sites
- Personal Sites

Report Settings:

Select All

Site Collection

- Site
- List

General Settings

- Site Collection Administration
- Statistics
- SharePoint Storage Report

- Size
- Administrators Information
- Description
- Created Time
- Owners Information
- Quota
- Primary Site Collection Administrator
- Site Collection Administrator Contact
- Sharing Outside Your Company
- External Sharing Domain Settings

Generated Report:

- Include summary report
- Include detailed report



Key Takeaways

Automation can help IT scale and guide end users to do the right thing.

IT stay in control when policy enforcement is in place

AvePoint have a number of ways to help scale delegated administration



Customer Location
Minnesota, United States

Industry
Public Sector

Platform
Office 365

- Critical Needs**
- Multiple Teams provisioning approaches within a single tenant
 - Secure, compliant and auditable collaboration within Teams
 - Ability to support surge in remote work

- Solution**
- Cloud Governance

"We went live with AvePoint Cloud Governance on March 15, 2020 via a schedule crash to allow the organization to make Teams since the Governor of Minnesota closed schools [in response to COVID]. We have some backlog, but the process has been working beautifully. Within one week we had a 20 percent increase in Teams created."

-Jeff Godderz, ECM Architect,
Metropolitan Council

Metropolitan Council Responds To COVID-19 Work-from-Home Orders By Deploying Cloud Governance and Microsoft Teams

Success Highlights

- Supported an influx of about 2,000 remote workers
- 20 percent increase of Teams creation within one week; 400 percent increase in Teams daily active usage; 21 percent decrease in emails
- Automated provisioning and lifecycle of Teams in compliance with regulations

Customer Profile

The Metropolitan Council is the regional policy-making body, planning agency, and provider of essential services for the Twin Cities metropolitan region. The Met Council and its 5,000 employees provide essential services and infrastructure – Metro Transit's bus and rail system, Metro Mobility, Transit Link, wastewater treatment services, regional parks, planning, affordable housing to support communities and businesses to ensure a high quality of life for its residents.

The Challenge

Metropolitan Council started to roll out Microsoft Teams in July 2019 following its SharePoint 2010 to SharePoint Online migration with AvePoint.

"Our move to Teams made sense as we were re-organizing and re-architecting SharePoint sites and our collaboration needs. From that point, we have been slowly rolling out features available in Teams," said Jeff Godderz, ECM Architect Metropolitan Council.

Metropolitan Council decided to leverage AvePoint's Cloud Governance to support its Microsoft Teams deployment because of its functionality to automatically enforce critical governance components of a Team or SharePoint site such as naming conventions, lifecycle, permissions, and ownership. The organization also needed to have a more tailored provisioning process for each of its council departments.

"We have five council departments, with five different cultures and it seems like all of them had different ideas for managing Teams self-provisioning," said Godderz. "One wanted self-service creation enabled, one wanted to route to IT for approval, and all want more control over getting resources as quickly as possible."

Metropolitan Council Teams Governance Needs:

- ❖ **Automation** - provisioning to support influx of user requests for Microsoft Teams
- ❖ **Flexibility** - Multiple governance policies mapped to Teams creation during provisioning.

"We have five council departments, with five different cultures and it seems like all of them had different ideas for managing Teams self-provisioning," said Godderz. "One wanted self-service creation enabled, one wanted to route to IT for approval, and all want more control over getting resources as quickly as possible."

Free Download >

Read all about it!

<https://www.avepoint.com/uk/events/webinar/remote-work-microsoft-teams>

What does a Teams governance quickstart look like?



8 Unique Teams templates (includes both Public and Private team types)



Ready made Policies to be automatically applied during Teams creation to manage multiple lifecycles, classification, ownership, naming convention & guest access



Customisable questionnaire for end users to request a Team



Landscaping reporting & auditing

What's Next?



These virtual workspaces all contain critical business data of varying sensitivity levels and oversight is critical to long-term success. **Ask yourself will you (or do you):**

- Have a firm grasp on why all these Teams are being created?
- Be confident the content being stored and shared within them is appropriate for all Team members?
- Still need all these Teams a year from now?

Following a rapid, two week deployment, you will be able to:

- Move from IT service delivery to user self-service
- Automate internal & **external collaboration** across public sector agencies
- Combat Microsoft Teams sprawl
- Identify clear ownership of Microsoft Team owners assigned automatically
- Automatically classify Microsoft Teams depending on content sensitivity



Interested in knowing more? Contact us.



SCAN ME

<https://www.avepoint.com/uk/lp/jumpstart-microsoft-teams-governance>

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

ໂພນລຸ້ນລຸ້ນ

Dziękuję

谢谢

Tack

Mulțumesc

спасибо

תודה

多謝晒

дядкую

Ďakujem