



# Layers of the Onion: Configuring External collaboration in Office 365

*... and managing it with AvePoint*

Microsoft  
Partner



Gold Application Development  
Gold Cloud Platform  
Gold Cloud Productivity  
Gold Collaboration and Content

Accessible content is available upon request.

# OFF202 – Layers of the Onion

---

*Managing External Sharing in Office 365*

John Peluso, CTO AvePoint Public Sector  
@JohnConnected  
<http://johnpeluso.me>



# Introduction...



**John Peluso**

CTO, AvePoint Public Sector  
Microsoft Regional Director

Email: [John.Peluso@AvePoint.com](mailto:John.Peluso@AvePoint.com)

Twitter: [www.twitter.com/johnconnected](https://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>



@JohnConnected

# 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





Why are we  
here?

Discussion:

*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?





# 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!



- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Contoso Electronics | SharePoint admin center

Contoso Electronics | Microsoft 365 admin center

Contoso Electronics | Microsoft 365 admin center

Contoso Electronics | SharePoint admin center

Contoso Electronics | OneDrive

Contoso Electronics | SharePoint admin center

Contoso Electronics | Microsoft Teams admin center

Home

Sites

Active sites

Sharing

Deleted sites

Sync

Policies

Storage

Device access

Compliance

Notifications

Data migration

Classic

OneDrive

Data migration

Admin centers

External sharing

Sharing Control Panel

Who can share

Default location

Choose the default location for sharing files and folders.

Use sharing

Default location

Choose the default location for sharing files and folders.

Additional settings

Limit

Previous

Dashboard

Teams

Devices

Locations

Users

Meetings

Messaging policies

Teams apps

Voice

Analytics & reports

Org-wide settings

External access

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.





The Core: Azure  
AD B2B

---

# Watch this!



The image shows a YouTube video player interface. On the left, there is a small video thumbnail showing a woman in a green shirt at a Microsoft-branded podium. Below the thumbnail, the text reads "Microsoft Ignite" in red, followed by "Orlando, FL" and "September 24-28, 2018". The main video area displays a presentation slide with the Microsoft logo and "BRK3249" in the top right corner. The slide title is "Granting partners and suppliers access to resources using Azure Active Directory B2B collaboration". Below the title, the presenter's name and title are listed: "Elisabeth Olson, Senior Program Manager, Microsoft @elisol". The video player controls at the bottom show a play button, a progress bar at 0:00 / 1:03:01, and icons for closed captions, HD, and other video settings.

Microsoft BRK3249

## Granting partners and suppliers access to resources using Azure Active Directory B2B collaboration

Elisabeth Olson  
Senior Program Manager, Microsoft  
@elisol

Microsoft Ignite  
Orlando, FL  
September 24-28, 2018

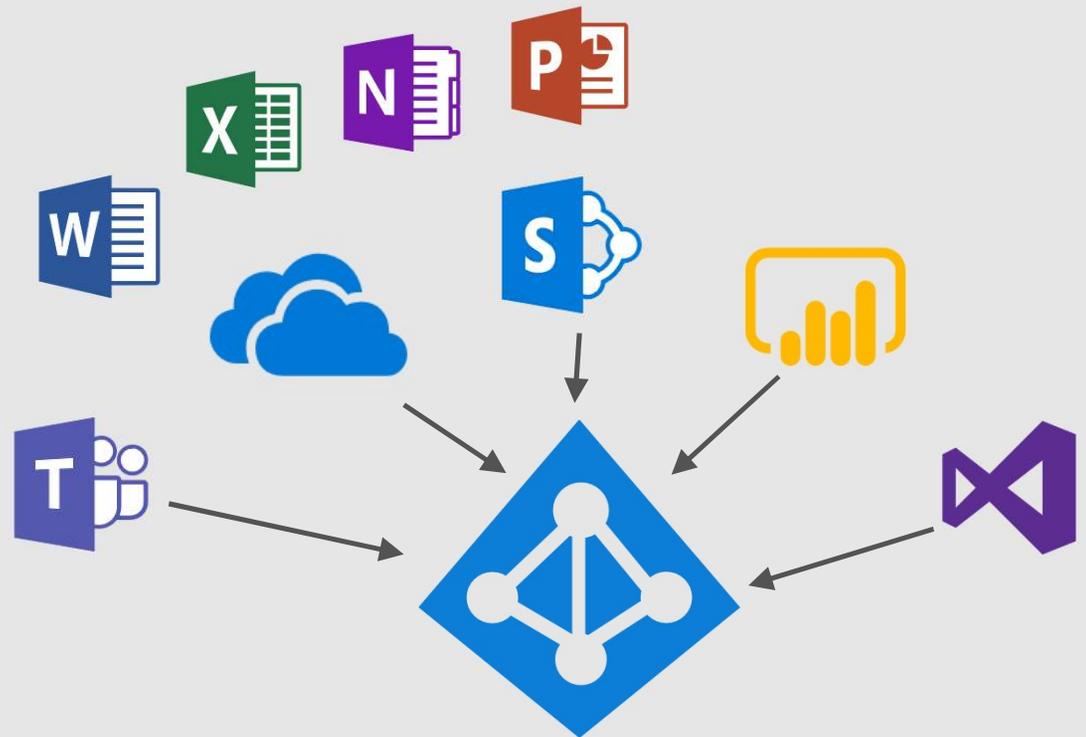
0:00 / 1:03:01

[https://www.youtube.com/watch?v=JN5u6w\\_gyic](https://www.youtube.com/watch?v=JN5u6w_gyic)

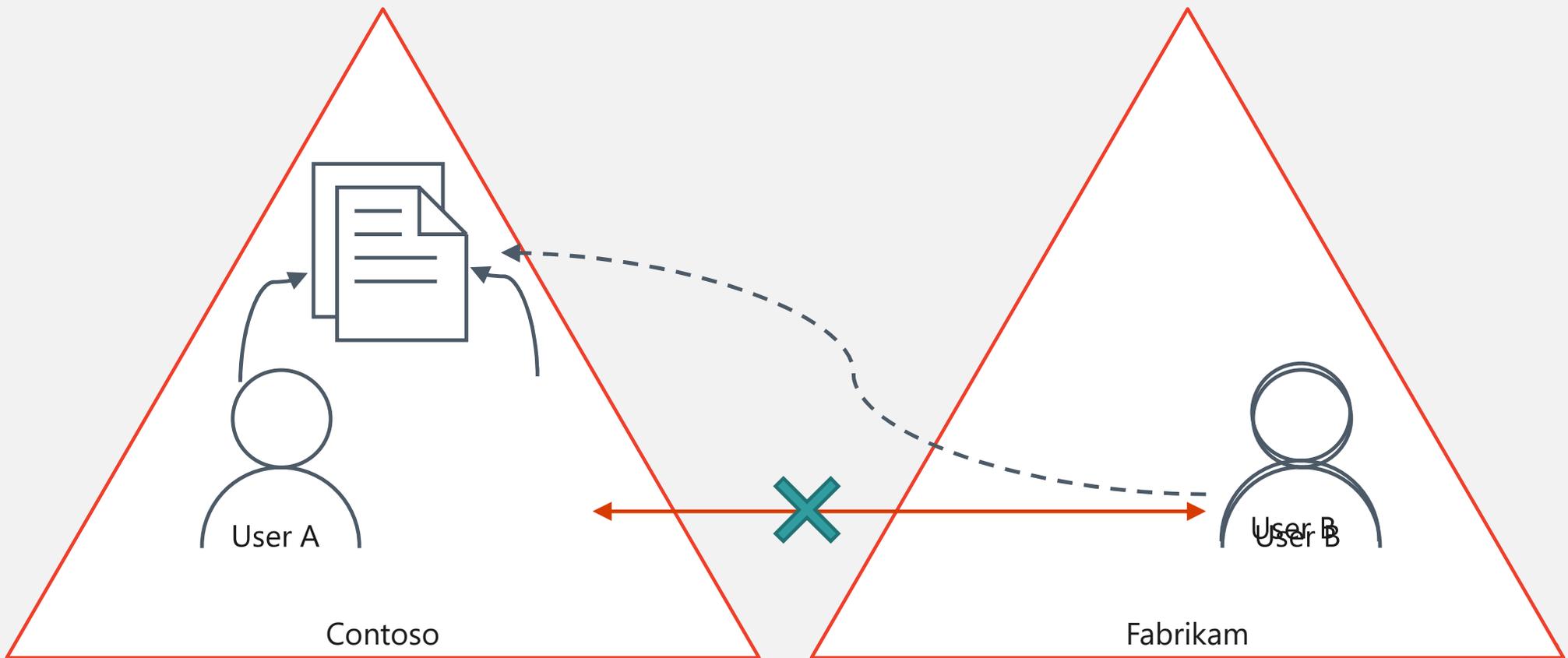
@JohnConnected

# Share and collaborate with guests in Microsoft products

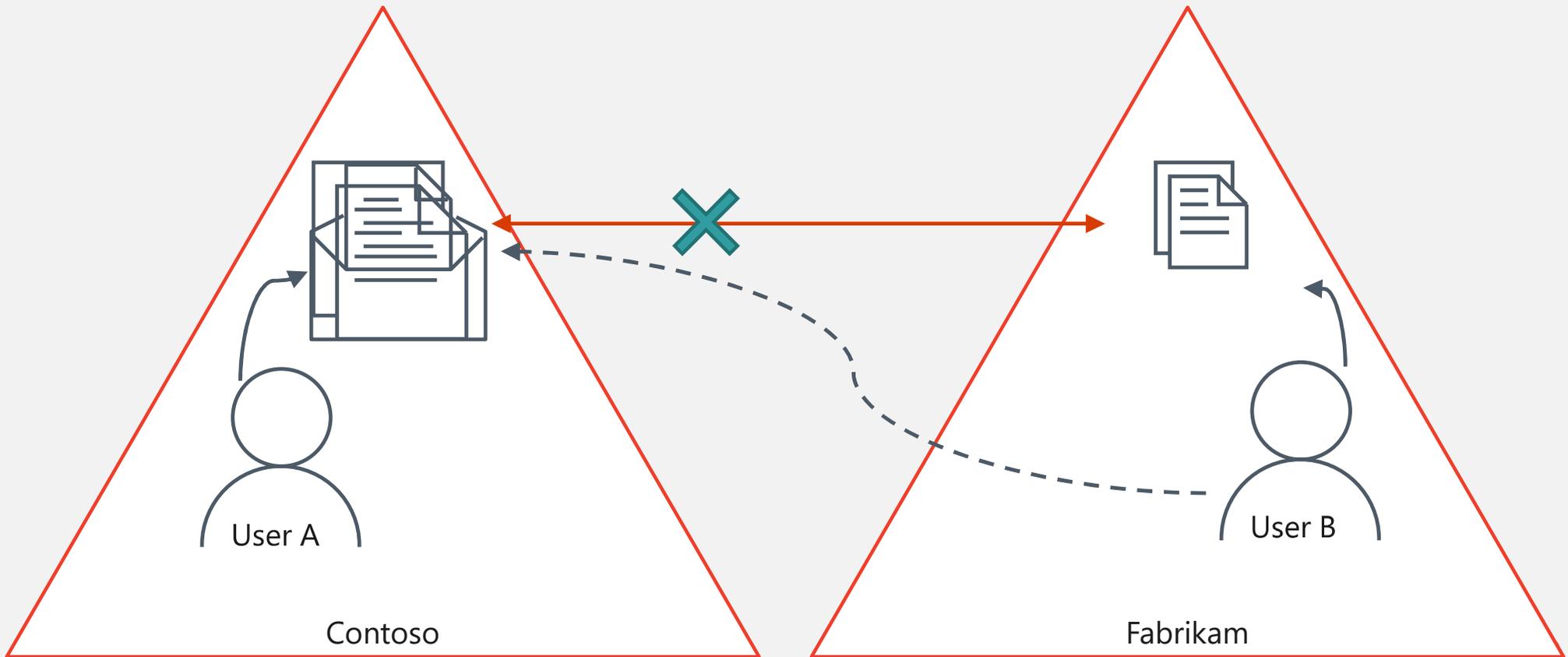
- Teams
- Office365 Groups
- SharePoint/Office client
- Power BI
- Visual Studio
- ...and more



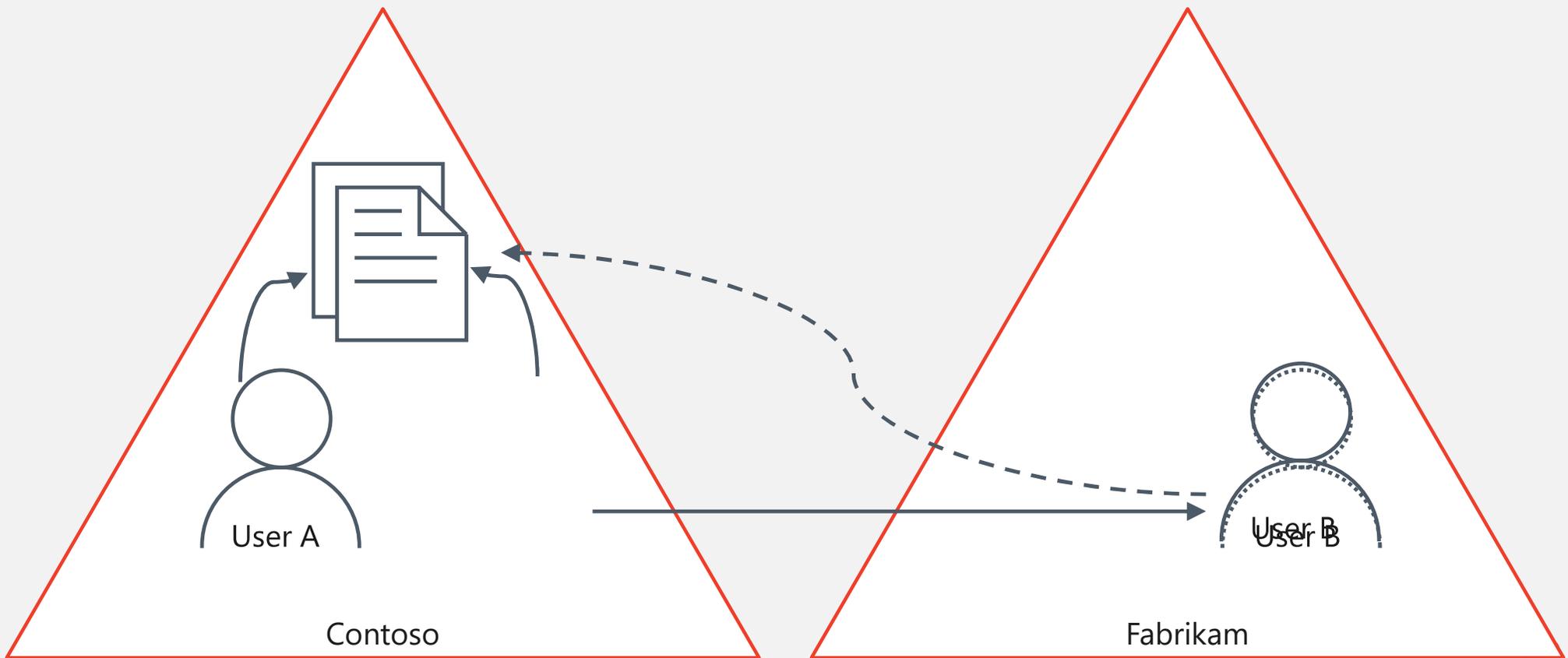
# How we've shared externally in the past...



# And this is even more common...



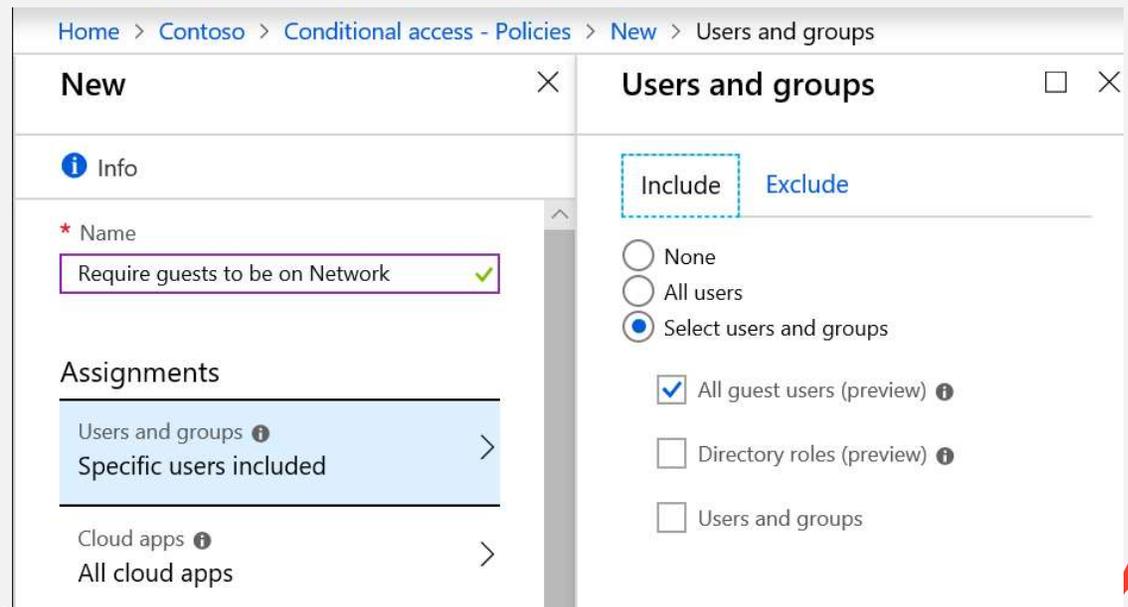
# "Guest Users" in Azure Active Directory



# Conditional access for guest users

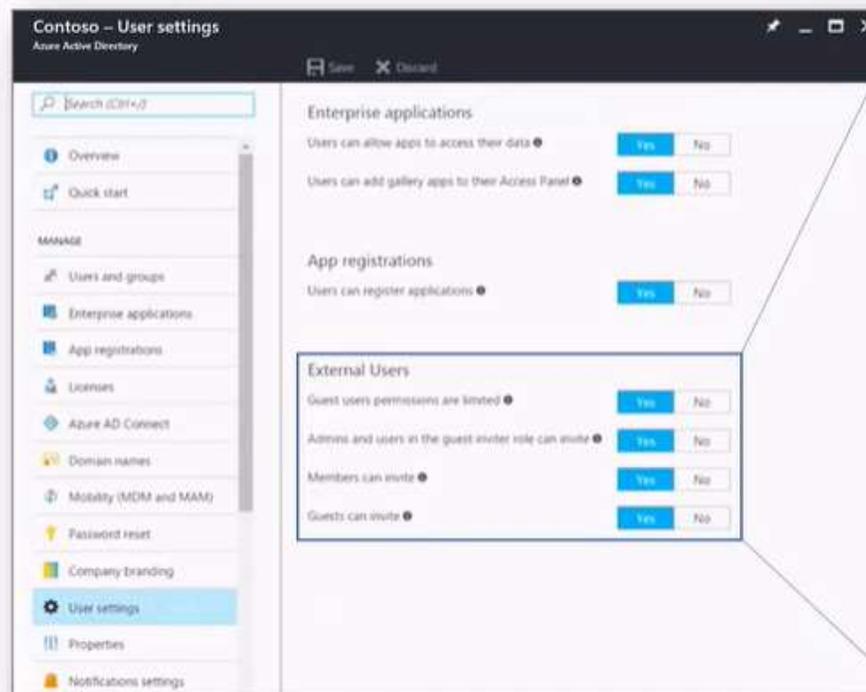
You can enforce conditional access policies on guests just like you would for any other user

Can also have policies *specific* to guests



# 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>

@JohnConnected

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

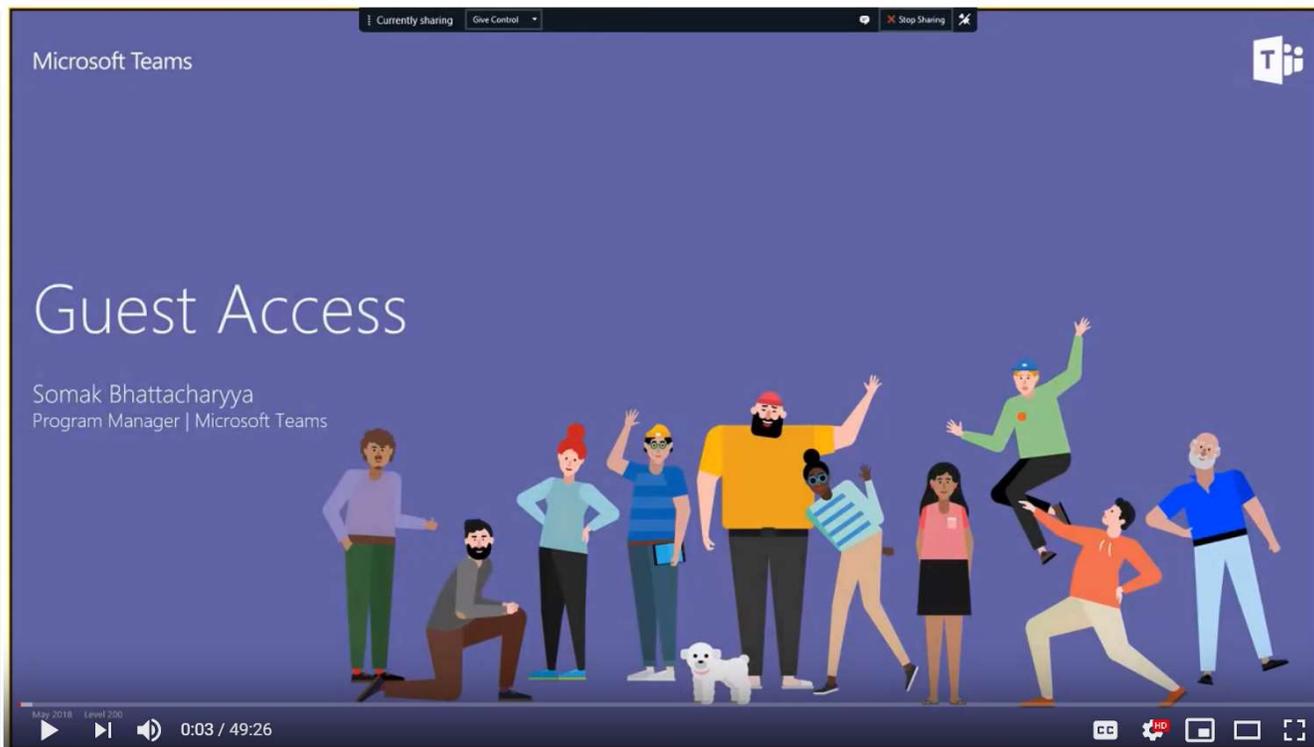


## Guest are managed

- 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



# And also watch this!

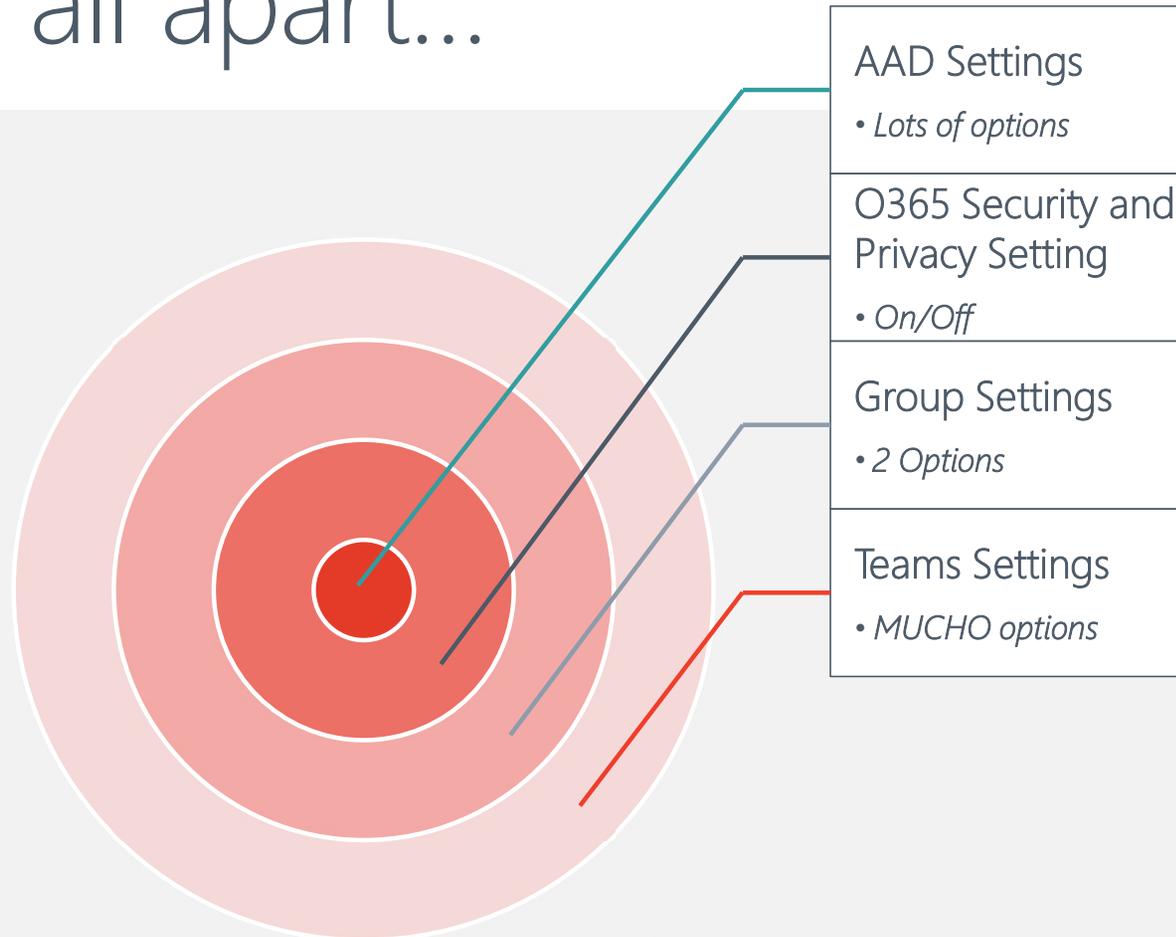


Microsoft Teams Best Practices for Managing Guest Access

<https://www.youtube.com/watch?v=vaJRRSjBxxY>

@JohnConnected

# Peeling it all apart...

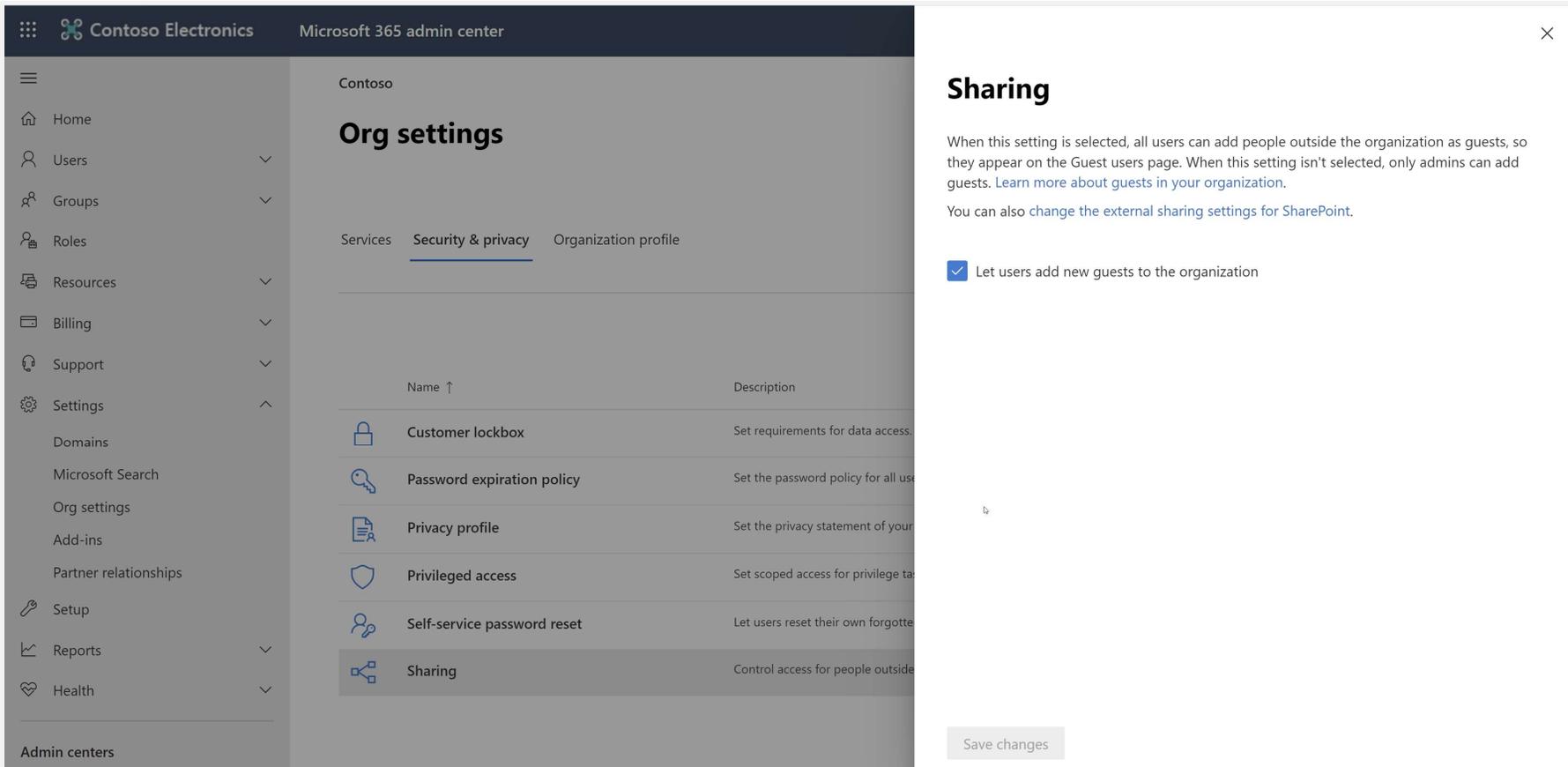


<https://docs.microsoft.com/en-us/microsoftteams/guest-access-checklist>

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



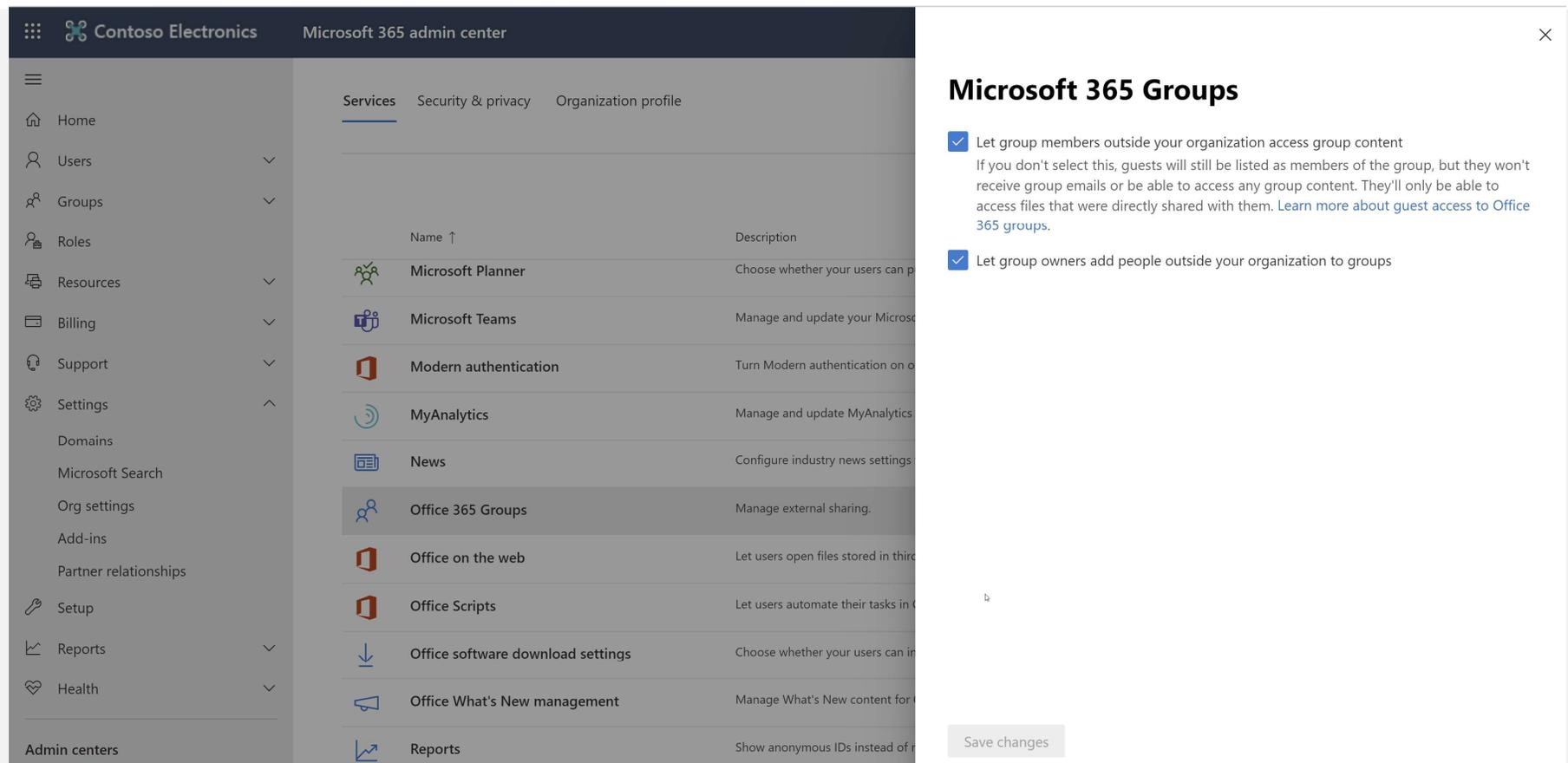
# O365 Tenant wide: Owners can invite *new* guests?



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



# O365 Groups: Owners can *add* and/or *invite* guests?



The screenshot shows the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar contains navigation options like Home, Users, Groups, Roles, Resources, Billing, Support, Settings, Domains, Microsoft Search, Org settings, Add-ins, Partner relationships, Setup, Reports, and Health. The main content area is titled 'Services' and lists various services. 'Office 365 Groups' is selected and highlighted. A settings panel on the right, titled 'Microsoft 365 Groups', contains two checked options:

- 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

A 'Save changes' button is visible at the bottom of the settings panel.



# Microsoft Teams: Are guests allowed in Teams?

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

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

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



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

The screenshot shows a Microsoft Docs page with a dark theme. The top navigation bar includes the Microsoft logo, 'Docs', 'Documentation', 'Learn', 'Q&A', and 'Code Samples'. A search bar and a 'Sign in' link are on the right. The breadcrumb trail reads: 'Microsoft Teams / Chat, teams, channels, and apps / Communicate with external users / Guest access / Use PowerShell to control guest access'. On the left, a sidebar menu is open, showing a search filter and a list of articles, with 'Use PowerShell to control guest access' selected. The main content area features the article title, a date (06/24/2020), a reading time (2 minutes), and a list of users. The article text discusses using PowerShell to control guest access in Teams, listing three bullet points: allowing/blocking guest access to all teams, allowing guests to be added to all teams, and allowing/blocking guest users from a specific team. It also provides links to 'Manage guest access in Microsoft 365 Groups' and 'Allow/Block guest access to Microsoft 365 Groups'. On the right, there are sections for 'Is this page helpful?' (Yes/No) and 'In this article' (Use PowerShell to turn guest access on or off, Guest access vs. external access). A 'Download PDF' link is at the bottom left of the article content.

<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

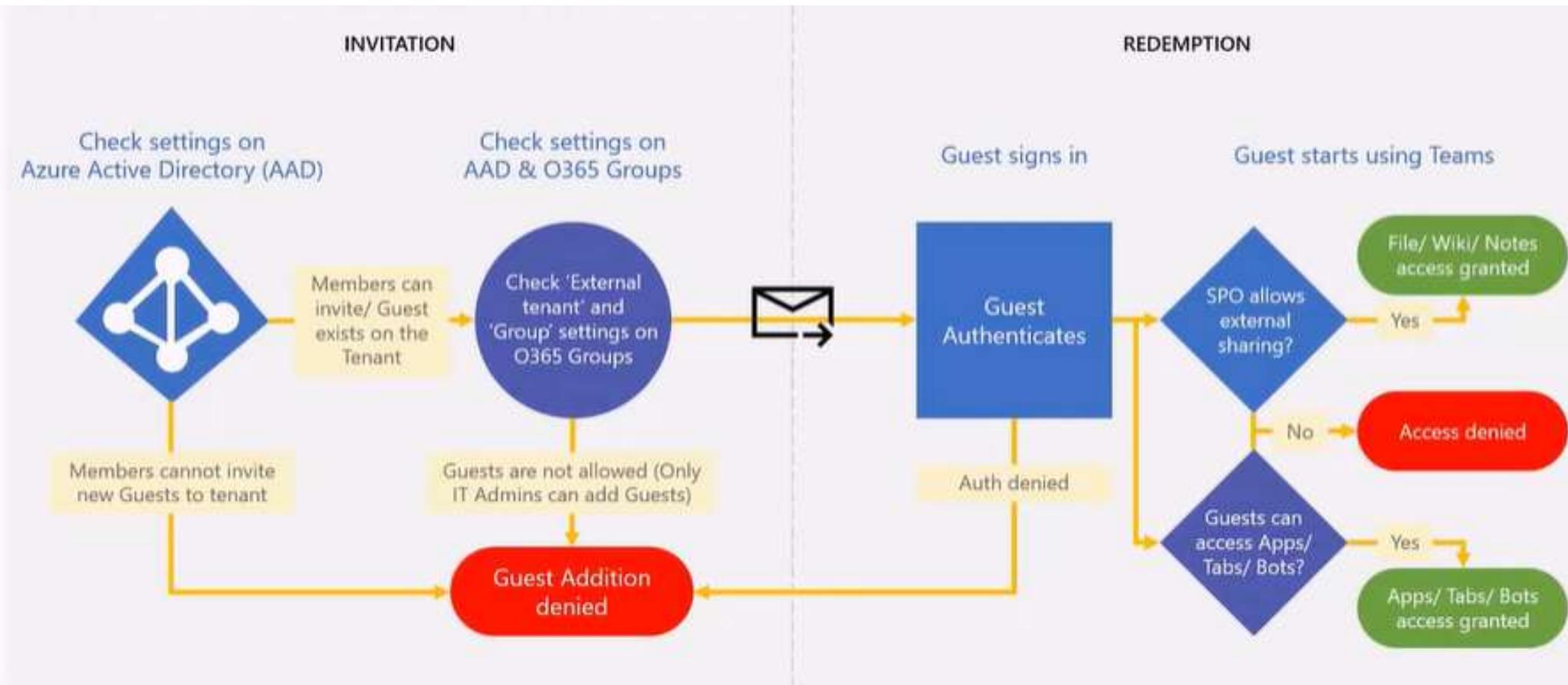


## Guests cannot

- 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



# How it all fits together..



@JohnConnected

# 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

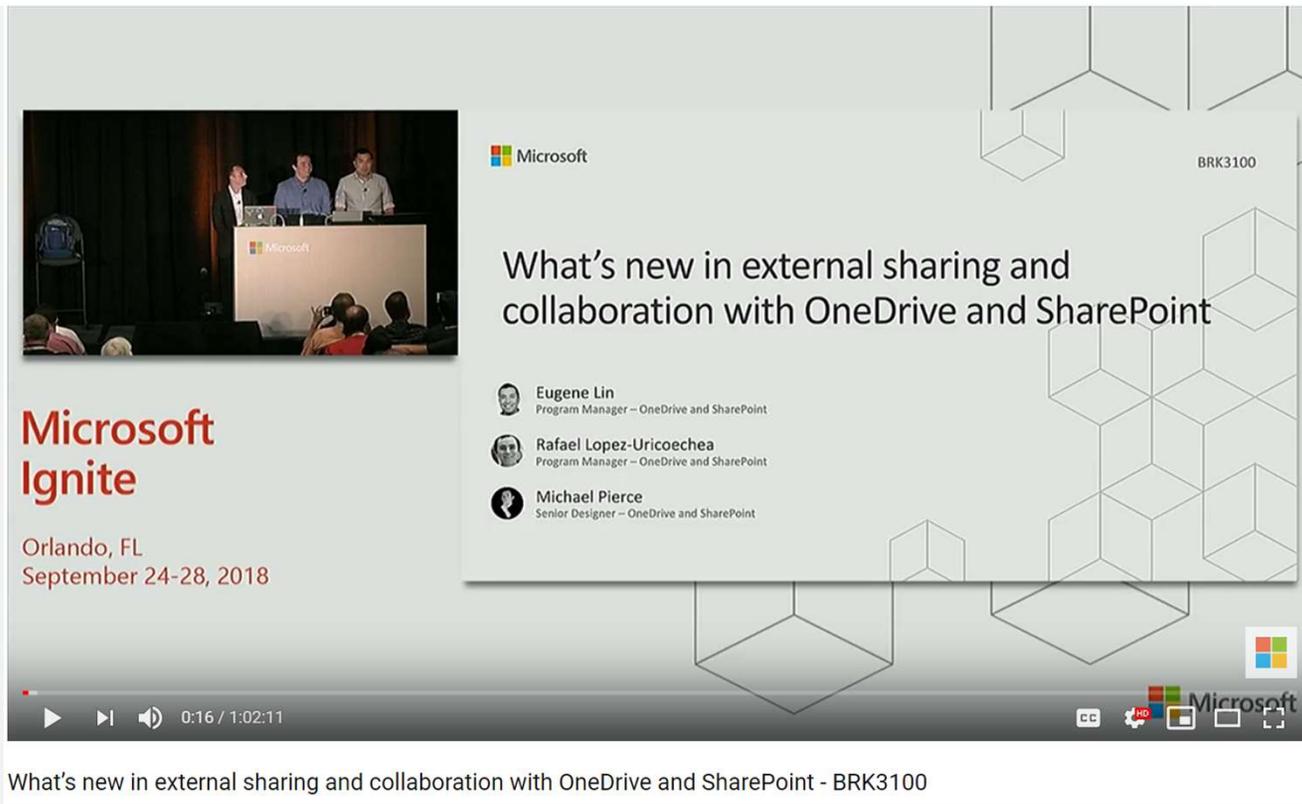
Demo:  
*Configuring Teams and Groups for Guest  
Access*





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

# And you should probably also watch this!



The image shows a screenshot of a YouTube video player. The video content is a presentation slide from Microsoft Ignite. The slide features the Microsoft logo in the top left corner and the session ID 'BRK3100' in the top right. The main title of the slide is 'What's new in external sharing and collaboration with OneDrive and SharePoint'. Below the title, there are three speaker profiles: Eugene Lin (Program Manager - OneDrive and SharePoint), Rafael Lopez-Uricoechea (Program Manager - OneDrive and SharePoint), and Michael Pierce (Senior Designer - OneDrive and SharePoint). The slide also includes the Microsoft Ignite logo and the event details: 'Orlando, FL September 24-28, 2018'. The video player interface at the bottom shows a progress bar at 0:16 / 1:02:11, a volume icon, and a Microsoft logo in the bottom right corner.

Microsoft

BRK3100

## What's new in external sharing and collaboration with OneDrive and SharePoint

**Eugene Lin**  
Program Manager - OneDrive and SharePoint

**Rafael Lopez-Uricoechea**  
Program Manager - OneDrive and SharePoint

**Michael Pierce**  
Senior Designer - OneDrive and SharePoint

**Microsoft Ignite**

Orlando, FL  
September 24-28, 2018

0:16 / 1:02:11

Microsoft

What's new in external sharing and collaboration with OneDrive and SharePoint - BRK3100

<https://www.youtube.com/watch?v=KvcYz3ERZSY>

@JohnConnected

# 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

# 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

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

## SharePoint

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

**Users can share with:**

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

Save changes Manage additional settings



# SharePoint: What are the *global* settings?

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

Contoso Electronics SharePoint admin center

## Sharing

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

### External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

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

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

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

**Only people in your organization**  
No external sharing allowed.

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

More external sharing settings

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



# SharePoint: Should *this site* be more restrictive?

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

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

**Sharing**

**External sharing**

Site content can be shared with:

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

**Advanced settings for external sharing**

- Limit sharing by domain

**Default sharing link type**

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

Save Cancel Reset to organization-level settings



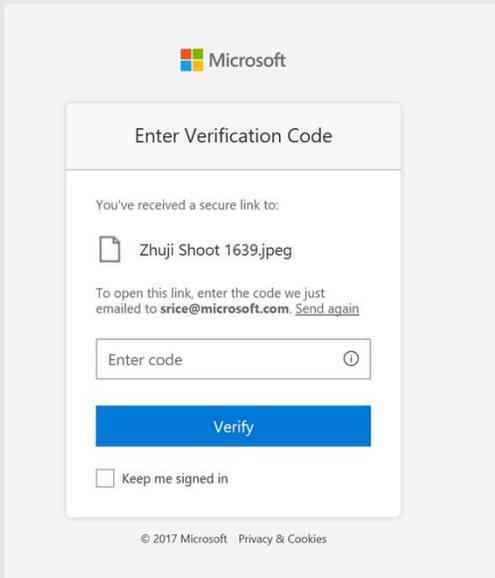
# External user reporting for SPO and ODFB is at the *site collection* level

The screenshot displays the SharePoint interface for the 'DTC Workshop Planning' site. A 'Run report' button is visible in the 'Shared with external users' section. A 'Documents' dialog box is open, prompting the user to 'Choose a destination to save this report' with options for 'General' and 'Presentation Prep' folders. The background shows a list of files and folders, including a 'Run report' file.

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

@JohnConr

# NEW! Azure AD B2B for one-time passcode users



Share securely with anyone in the world

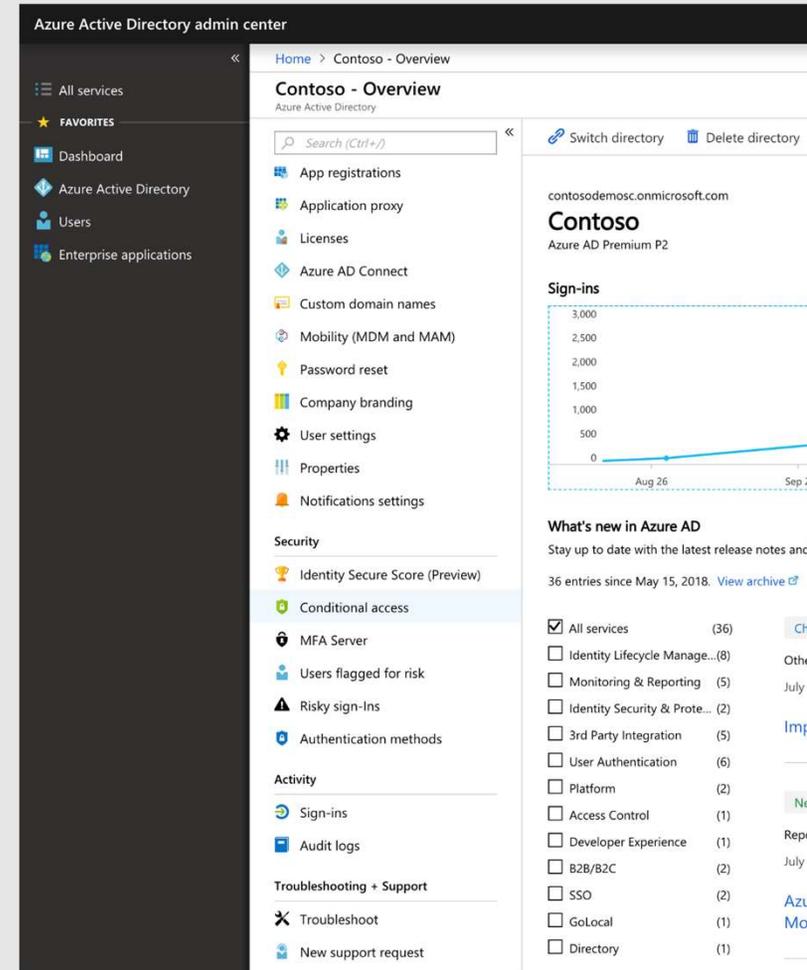
Simple verification with one-time passcode

AAD B2B guest management

Conditional access

Google auth federation

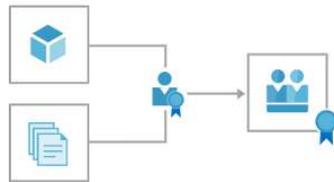
Guest do not require O365 licenses



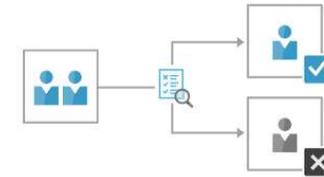
Demo:

*Configuring and exploring SPO/ODFB external sharing*

# Understanding Entitlement management & Access reviews



Entitlement management



Access reviews

- Manage access to “packages” of Groups/Teams, Applications and Sites
  - Request to access package can be subject to approval
  - Access to the package syncs membership to the resources in the package
  - Access review and revocation happens at the package level, and *named* reviewers
  - Workflow for intake of requests for guests not already in directory
  - Can remove guest from directly when access to last package is revoked
- Manage access to each group or application (*not standalone SharePoint Sites*)
  - Access review to the Group/application itself
  - Reviewers can be Group Owners or named users
  - No workflow for intake of requests for guests not already in directory (*standard B2B invitation process*)
  - No workflow to remove guest from directory when removing from group/application



Are You Ready?

# 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?

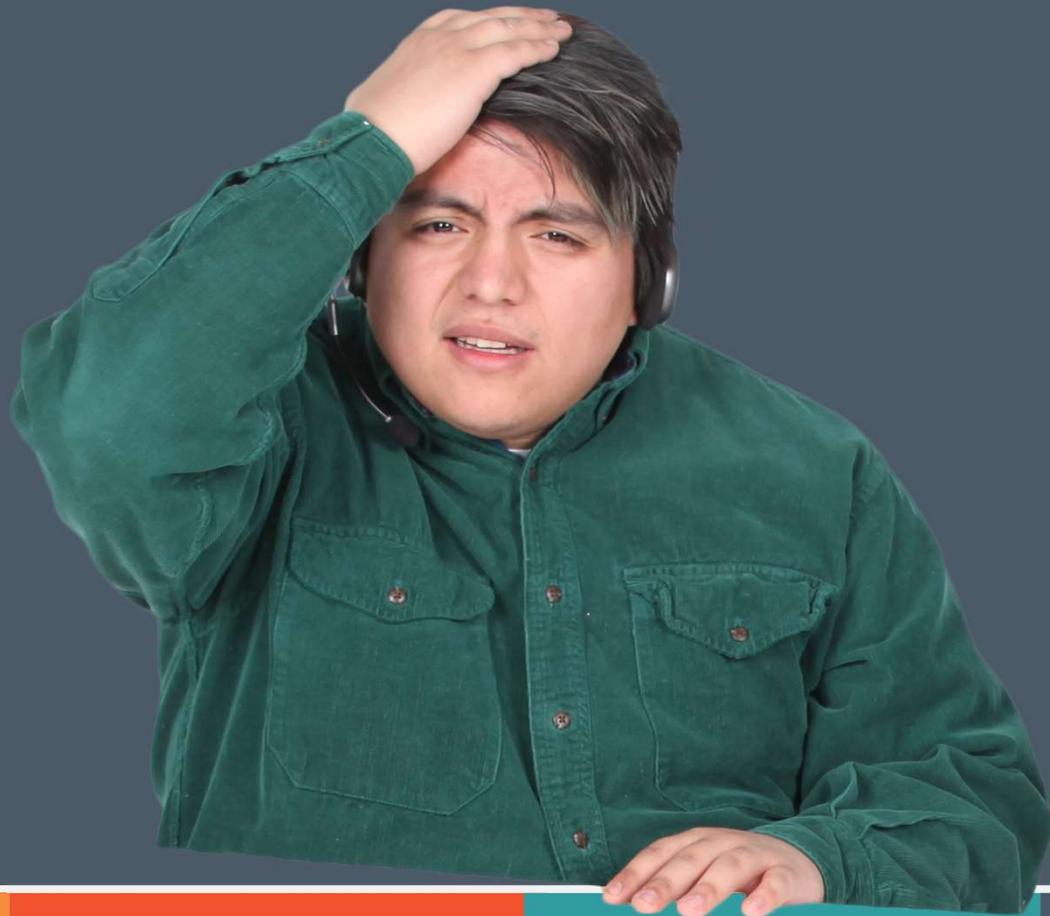
## How do you want to onboard *new* external collaborators?

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 a 'New Request' in the 'Governance' section, specifically for a 'Project Management Questionnaire'. The form includes a header with the title and navigation icons. Below the header is 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!'. The first question is 'Is this a new or existing project?' with a dropdown menu set to 'New Project'. The second question is 'How would you describe this project's collaboration?' with two radio button options: 'Traditional Workstream' and 'Modern Workstream', where 'Modern Workstream' 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 set to 'Please select an option...'. At the bottom right of the form are 'Cancel' and 'Save as Draft' buttons.

## Standardized Services

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

## Policy Enforcement

- Apply proactive monitoring/enforcement of permissions and configuration policies



**EXAMPLE**

DEPARTMENT



DEPARTMENT



DEPARTMENT



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



## New Request > Project Management Questionnaire

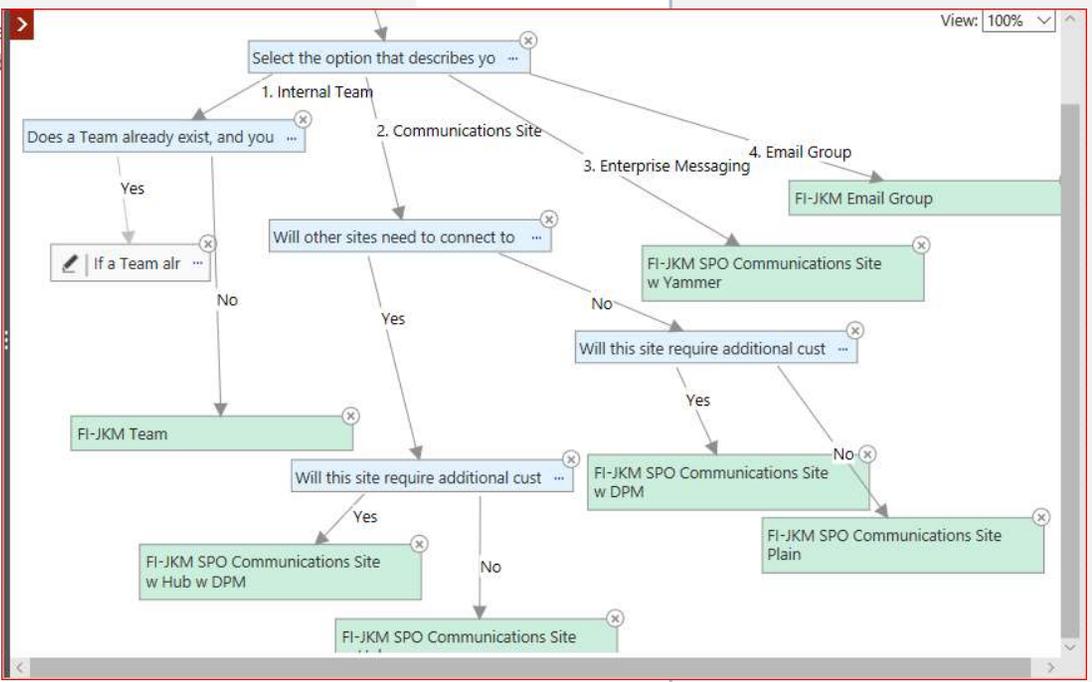
**Before we get started...**  
We want to help you ensure that all your data is secure and that you have the right tools for the right job. Please answer the following questions to the best of your ability.

Is this a new or existing project?

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?



# 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



# Targeting Services & Policies Across Divisions

## Tenant Wide General Services

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

**Core Services**  
(provisioning, lifecycle, policy, protection)

## Address Unique Needs of Specific Departments or Divisions

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

Division



Division



Division



## Specialized Services Smaller Groups

- Unique needs can be addressed
- Pilots of future services

**Team C-1**  
specialized Services



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

Service Management > Create Communicatio... ⓘ

Copy Save Save and Activate Cancel

### Service Initiation

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

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

### Service Permissions

Specify users that should have access to this service.

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

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

Conditions:

Local Users or Office 365 Users/Groups ▼

\*Allowed values:

Add to List Clear Settings

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

Clear Table



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

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

- To-do list:** Includes an 'Approvals' section with a task 'Delete Office 365 Group/Microsoft Team Ext...' and a 'Confirmations' section with a task 'PM Extranet Renew Site Collec...'. A red box highlights the 'Q2 Outing Renew Office 365 Group' task in the Confirmations section.
- Group renewal: Q2 Outing:** A central panel showing renewal steps and a user list. The steps include Contact, Permission, Membership, and Metadata renewal. The user list table is as follows:

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



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



# Designing the "Guest User Request" service

The screenshot displays the AvePoint Cloud Governance interface. The left sidebar contains navigation options: Home, Management, Services, Settings, and Directory. The main content area is titled 'Services > Invite New Guest User > Edit' and is divided into three tabs: '1. Basic info', '2. Settings', and '3. Advanced settings'. The 'Settings' tab is active, showing configuration for a 'Guest renewal profile'. The 'Basic info' section includes fields for 'Microsoft 365 tenant \*' (AvePoint ATS Dev), 'Primary contact \*' (\$Requester), and 'Secondary contact' (\$Manager of Requester). A toggle switch for 'Allow requesters to add guest users to groups or teams' is turned on. Below this are two checked checkboxes: 'The requester is the owner of the group or team' and 'The requester is the primary/secondary contact of the group or team'. The 'Renewal profile' dropdown is set to 'Guest User Renewal'. The right-hand pane, titled 'Create guest user renewal profile', contains the following fields: 'Profile name \*' (Renew guests every 30d), 'Description', 'Microsoft 365 tenant \*' (AvePoint ATS Dev), 'Category \*' (Lifecycle Management), 'Renewal process' (Daily selected, Every 30 days), '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), and 'Notification e-mail template for assigned renewal tasks \*' (Built-in Guest User Renewal Process Assignment E-mail Template). There are also 'Cancel', 'Back', and 'Next' buttons at the bottom of the main pane.



# Admin monitoring of Guests

The screenshot displays the AvePoint Cloud Governance interface. On the left is a navigation sidebar with options like Home, Management, Services, Guest renewal profil..., Settings, MyHub settings, System settings, Directory, Workspace report, and Guest user report. The main area shows a 'Guest user report' table with columns for Username, E-mail address, and Primary contact. Two rows are visible: 'Gawczynski.Tom' and 'Tom.Gawczynski'. The 'Tom.Gawczynski' row is selected, and a 'View details' panel is open on the right, showing user information such as Username, First name, Last name, E-mail address, Primary contact (Ray Hill), Secondary contact (Ian Anderson), Job title (Security Architect), Department (Collaboration), Renewal profile (Guest User Renewal), Invited by (Ray Hill), and Status (Renewal pending). Below this, a 'Workspace access' table lists three entries: Q2 Outing, Regional Hospital, and Project\_US, all of type 'Microsoft Team'.

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

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

*Existing guests can be imported for management as well!*



*Demo:*

End user self-service guest  
request and renewal

# Managing External Sharing for *SPO* and *ODFB*

# 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 customers who are looking to add control to external sharing in Office 365 SharePoint Sites and OneDrives. Example 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 (such as OneDrives)?
- How can I reach back to existing sites to disable external sharing for external users?

### Control Where and How External Sharing is Permitted

When customers apply policies for external sharing, Microsoft gives you 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 option that requires prior approval (such as an approval workflow in Governance Automation), this may not be an issue.

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

- Where external sharing is permitted based on site collection filters (such as properties, managed path, titles, etc.)
- Types of external sharing options if it has been allowed (such 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.

## Controlling External Sharing

Policy enforcer received a few crucial updates this month for customers who are looking to add control to external sharing in Office 365 SharePoint Sites and OneDrives. Example 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 (such as OneDrives)?
- How can I reach back to existing sites to disable external sharing for external users?

### Control Where and How External Sharing is Permitted

When customers apply policies for external sharing, Microsoft gives you 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 option that requires prior approval (such as an approval workflow in Governance Automation), this may not be an issue.

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

- Where external sharing is permitted based on site collection filters (such as properties, managed path, titles, etc.)
- Types of external sharing options if it has been allowed (such 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

Rule Management Manage Commit

**i** 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:

Description:

<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  Go to  of 1 < >



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/AdvancedDiscovery	https://m365x483549.sharepoint.com/sites/AdvancedDiscovery	✔		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 >



DocAve Management Security Plan Manager Policy Enforcer

Fix Manual Operation Required Hide

Hidden List Export Manage

Close 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
▶ 📁 User/Group Restriction ⓘ				
▶ 📁 /	https://m365x483549-my.sharepoint.com	⊕		
▶ 📁 Information Rights Management (IRM) SharePoint 2013 ⓘ				
▶ 📁 External Sharing Settings ⓘ				
▶ 📁 /	https://m365x483549-my.sharepoint.com	⊕		

< 1 of 1 >



# 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.

Select All

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

OK Cancel

**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.

SharePoint Groups:

Include members of Active Directory groups in the search results

**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.

Has Permissions:  
Search for any Permission

- Exact permission
- Exact permission or better



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

The screenshot displays the 'Report Center > Administration Reports > Configuration Reports' interface. The user is logged in as 'admin@od'. The main content area is titled 'Please configure report settings.' and contains the following sections:

- Report Profile:** A dropdown menu set to 'Input/Select'.
- Scope:** A search bar with 'Input Keyword' and a list of 'My Registered Sites' including 'Default Office 365 Group Team Site Container', 'Default OneDrive for Business Container', 'Default Site Collection Container', 'Group Team Sites', 'Modern Sites', and 'Personal Sites'.
- Report Settings:**
  - Select All:** A checkbox for selecting all items.
  - Site Collection:** A dropdown menu with 'Site' and 'List' options.
  - General Settings:** A list of checkboxes for 'Site Collection Administration', 'Statistics', and 'SharePoint Storage Report'.
  - Administrators Information:** A list of checkboxes for 'Size', 'Description', and 'Created Time'.
  - Owners Information:** A list of checkboxes for 'Quota', 'Primary Site Collection Administrator', 'Site Collection Administrator Contact', 'Sharing Outside Your Company', and 'External Sharing Domain Settings'. Red arrows point to the 'Sharing Outside Your Company' and 'External Sharing Domain Settings' options.
- Generated Report:** A section with checkboxes for 'Include summary report' and 'Include detailed report'.



# 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

# thank you

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



Sales@AvePoint.com | +1 800.661.6588



[www.AvePoint.com](http://www.AvePoint.com)



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