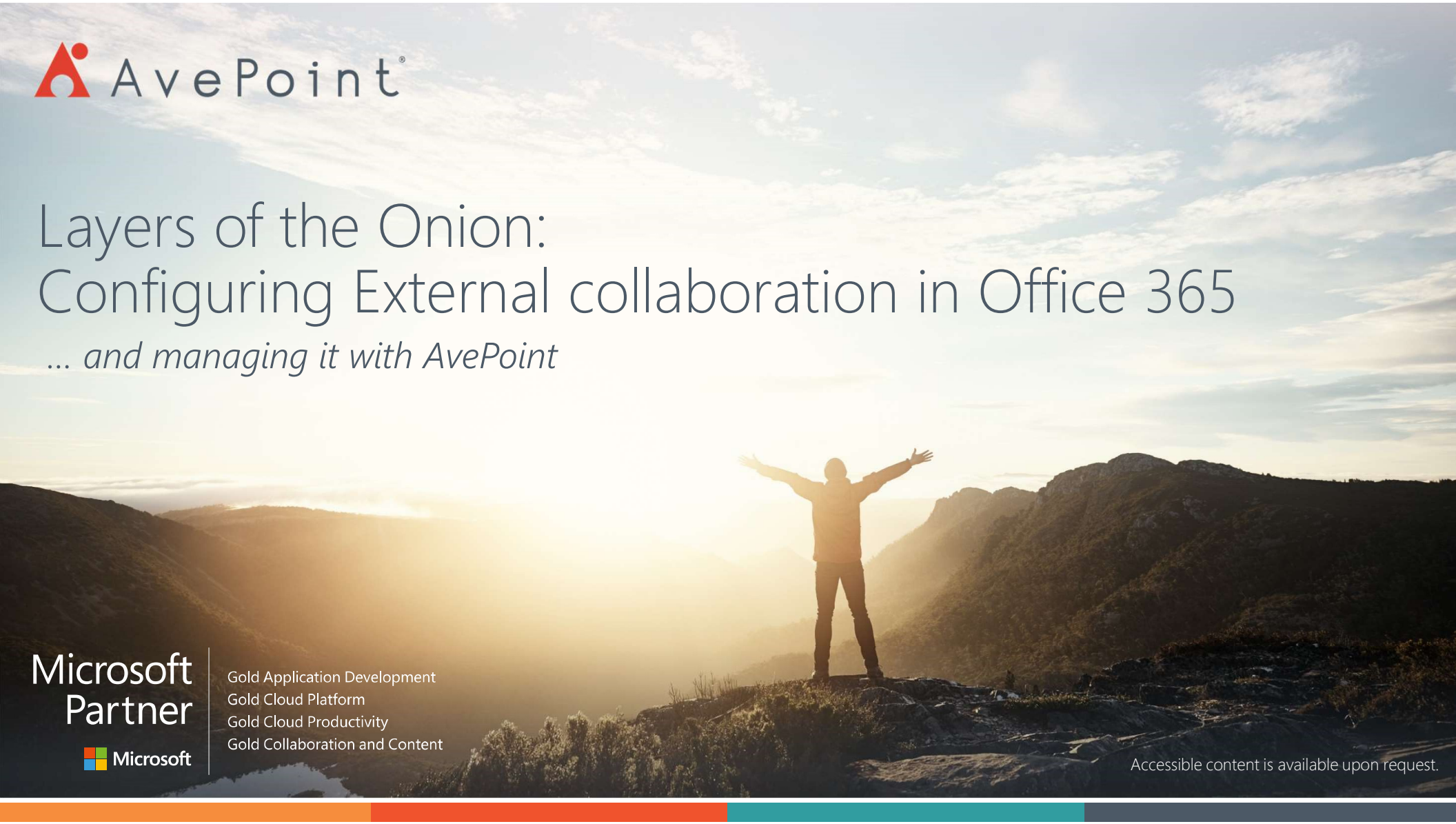

AvePoint
Layers of the Onion:
Configuring External collaboration in Office 365
... and managing it with AvePoint
Microsoft Partner
Microsoft
Gold Application Development
Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content
Accessible content is available upon request.

OFF202 – Layers of the Onion

Managing External Sharing in Office 365

John Peluso, CTO AvePoint Public Sector
@JohnConnnected
http://johnpeluso.me

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

@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?

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

The Landscape of Office 365 External Sharing

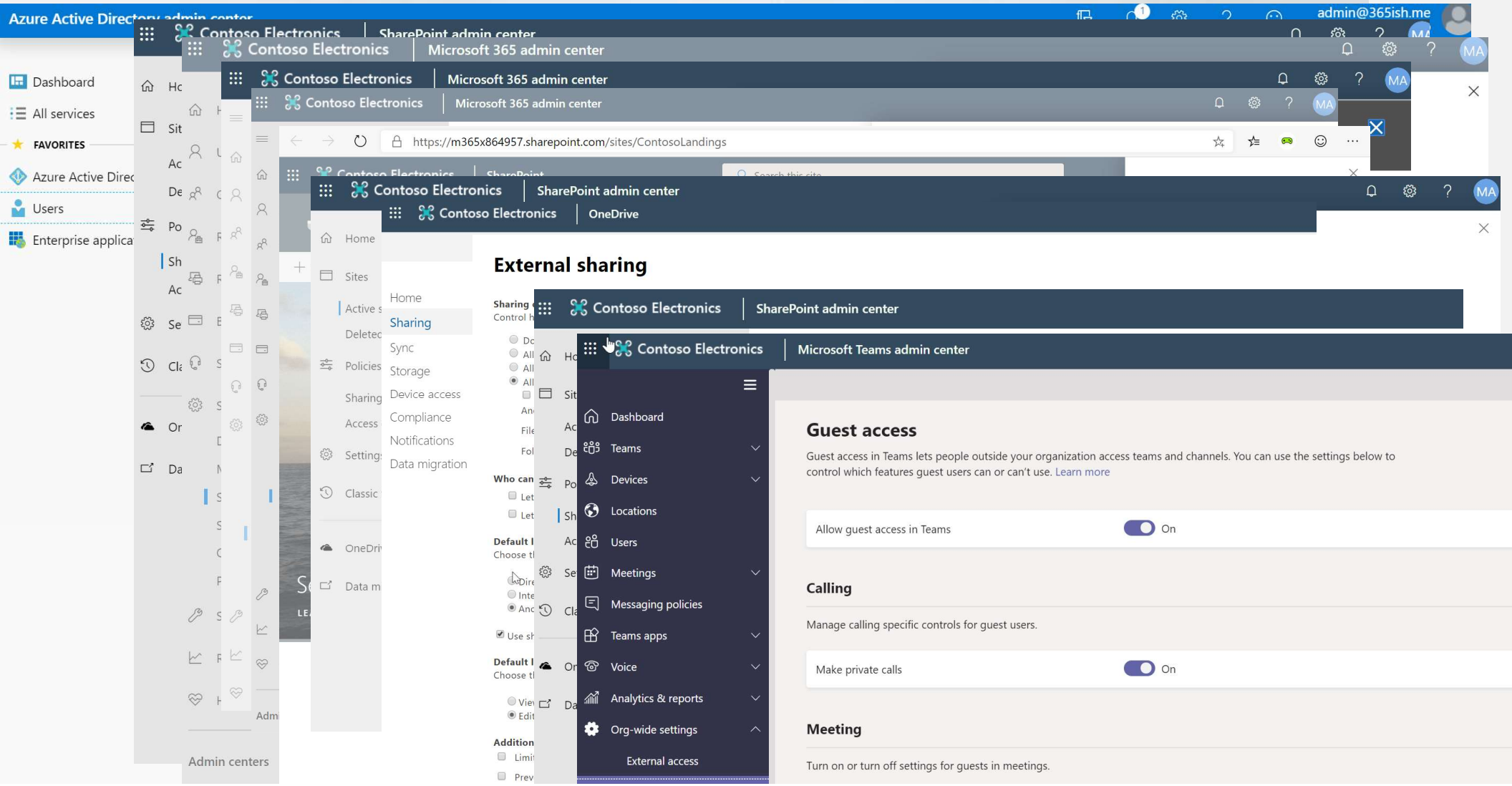
External collaboration in O365 is like an onion…

There are many layers to deal with

And…

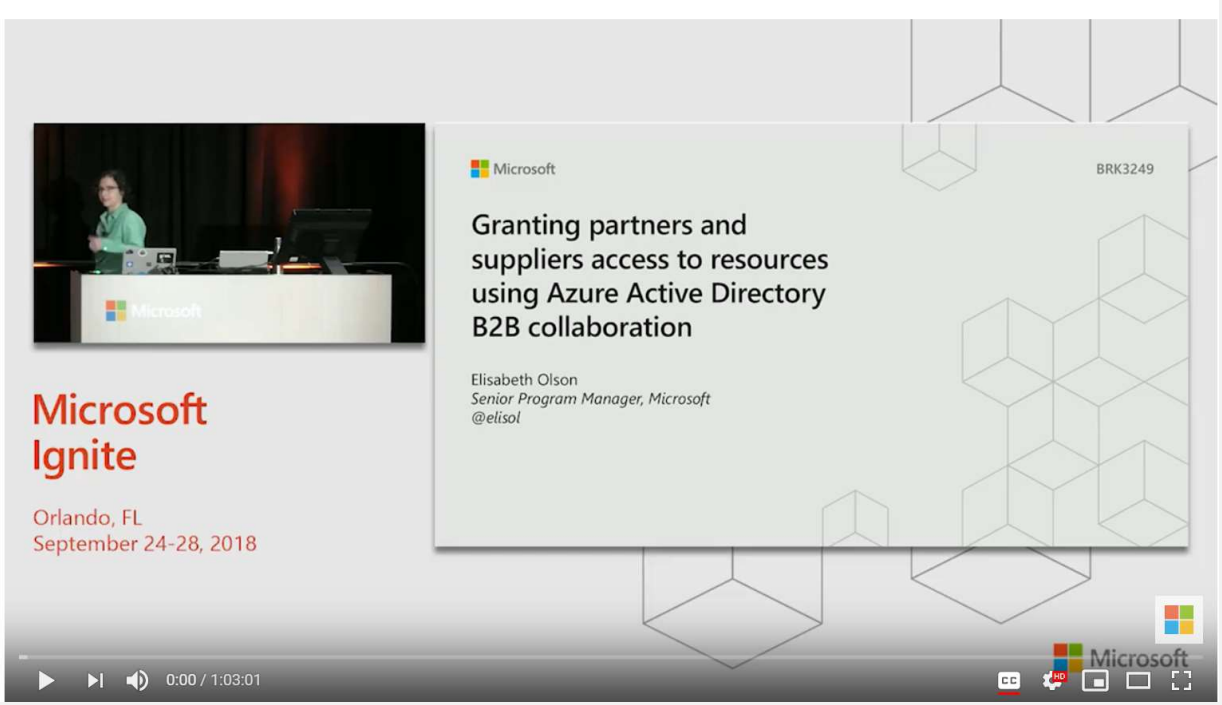
If you do it wrong, it can make you tear up!

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


Azure Active Directory admin center
admin@365ish.me
Dashboard
All services
FAVORITES
Azure Active Direc
Users
Enterprise applica
Contoso Electronics
SharePoint admin center
Microsoft 365 admin center
https://m365x864957.sharepoint.com/sites/ContosoLandings
OneDrive
Home
Sites
Sharing
Sync
Storage
Device access
Compliance
Notifications
Data migration
External sharing
Microsoft Teams admin center
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.
Admin centers

The Core: Azure AD B2B

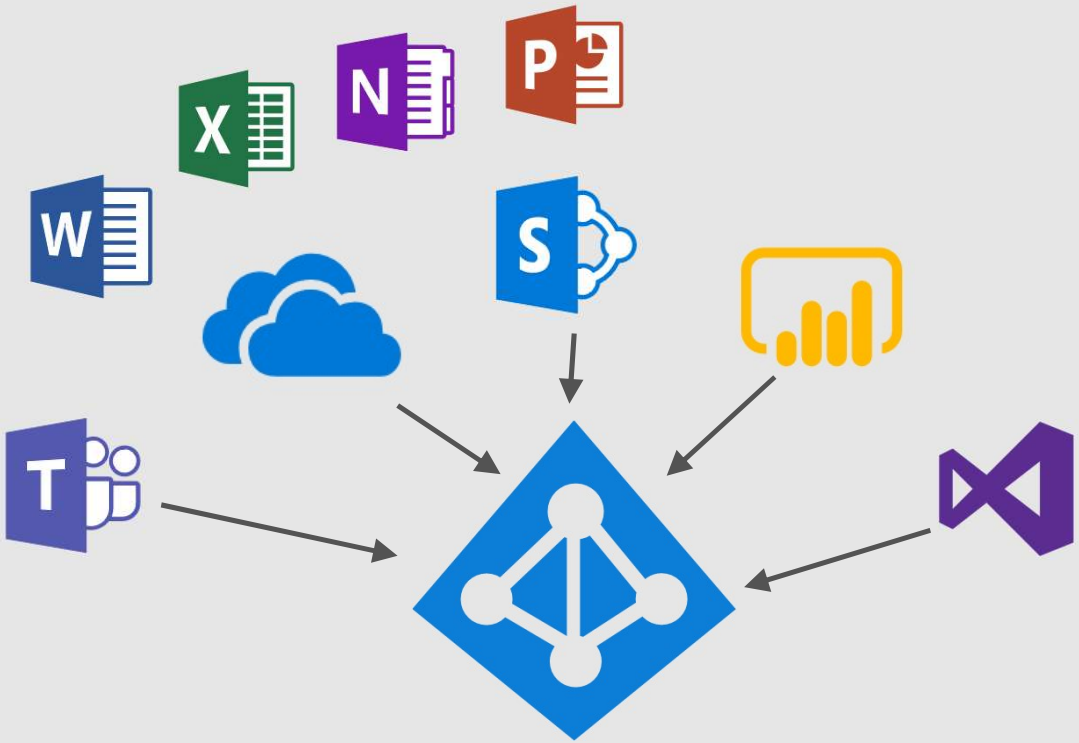
Watch this!



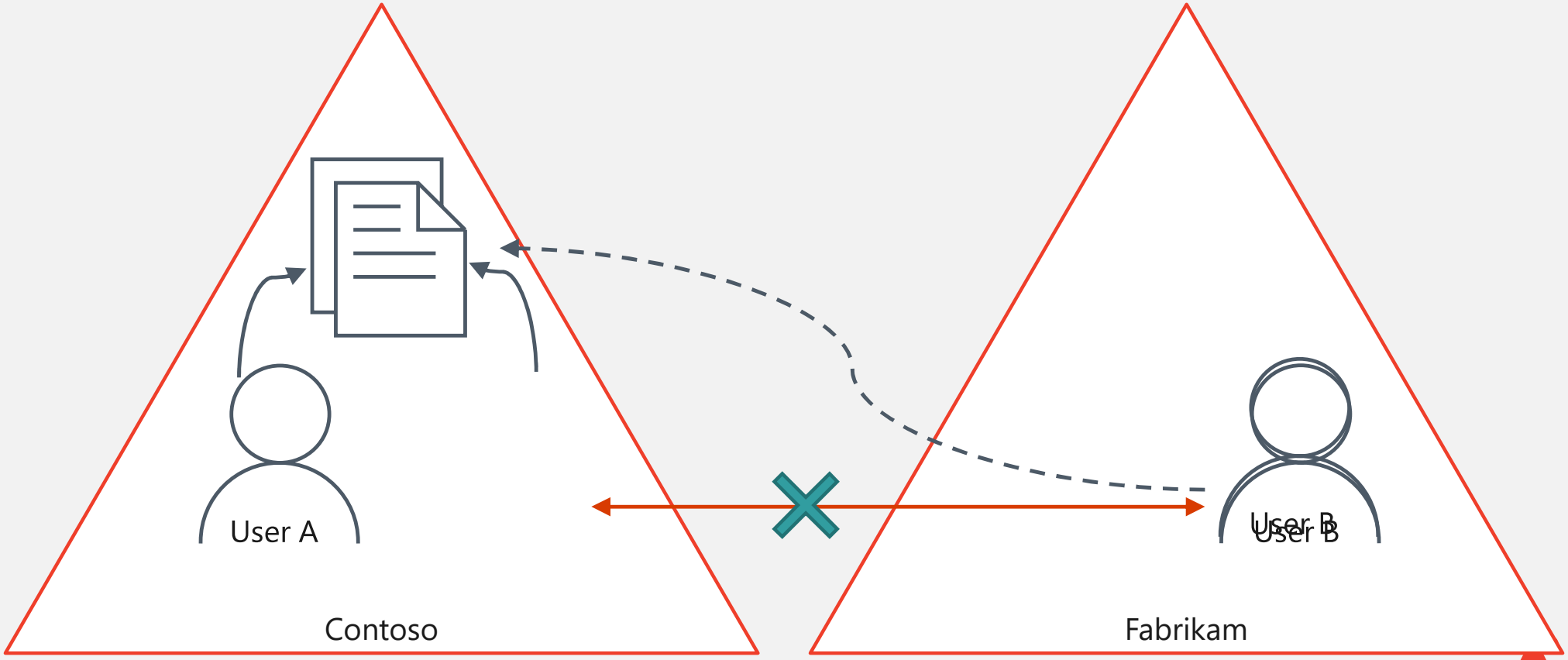
https://www.youtube.com/watch?v=JN5u6w_gyic

Share and collaborate with guests in Microsoft products

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

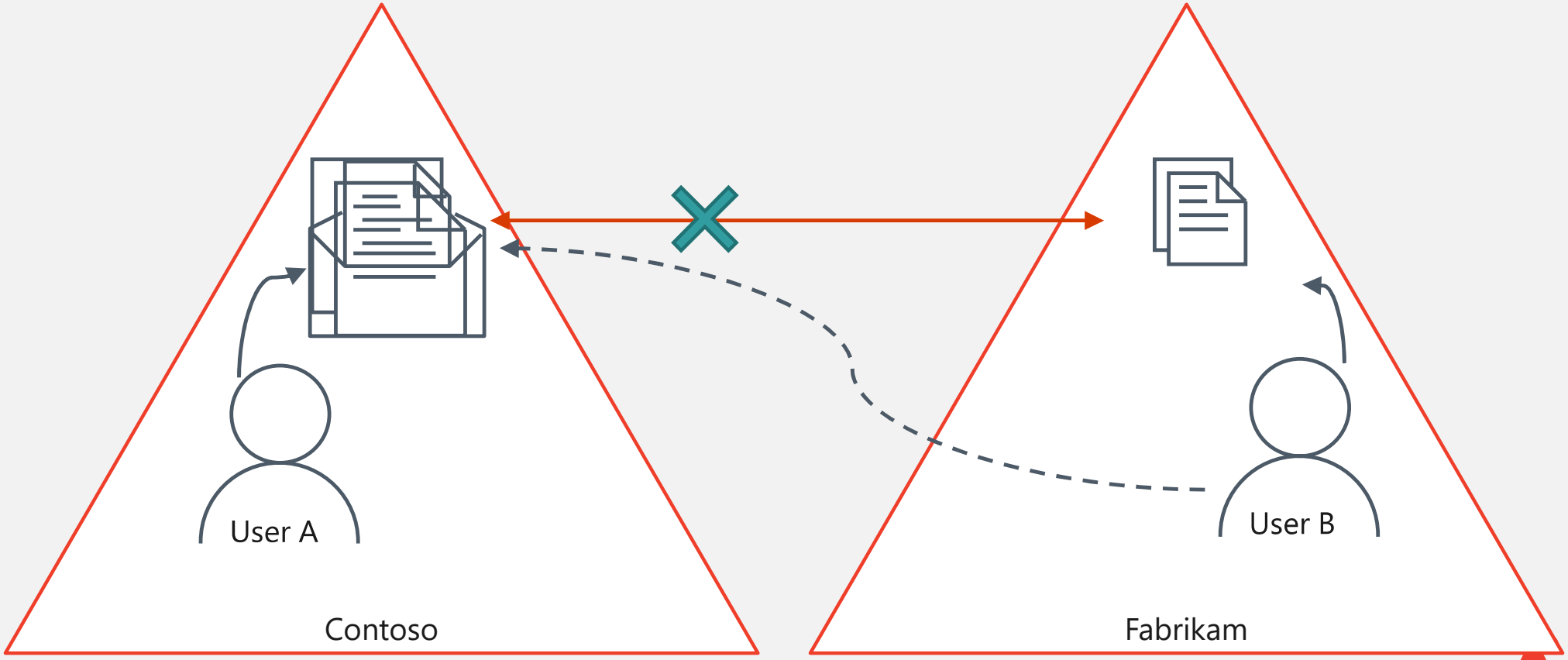


How we've shared externally in the past…



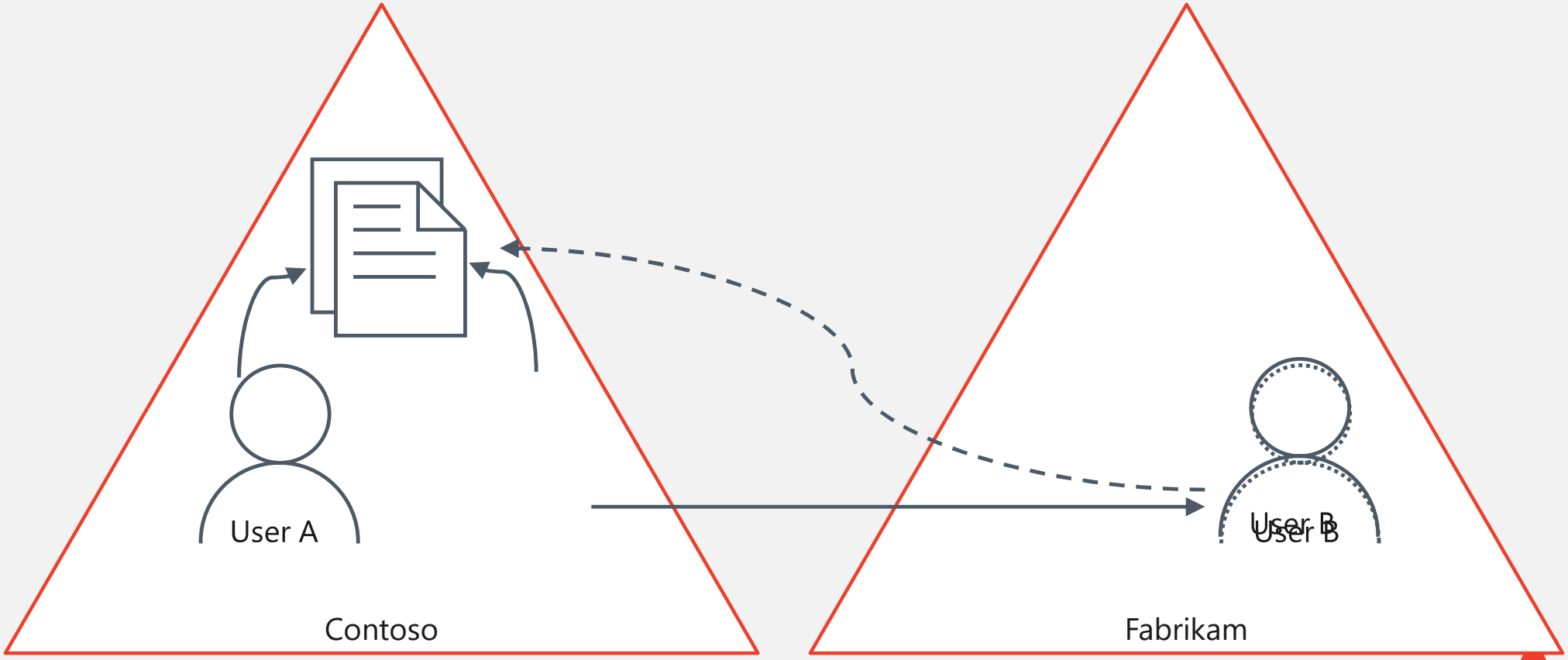
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

And this is even more common…



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

“Guest Users” in Azure Active Directory

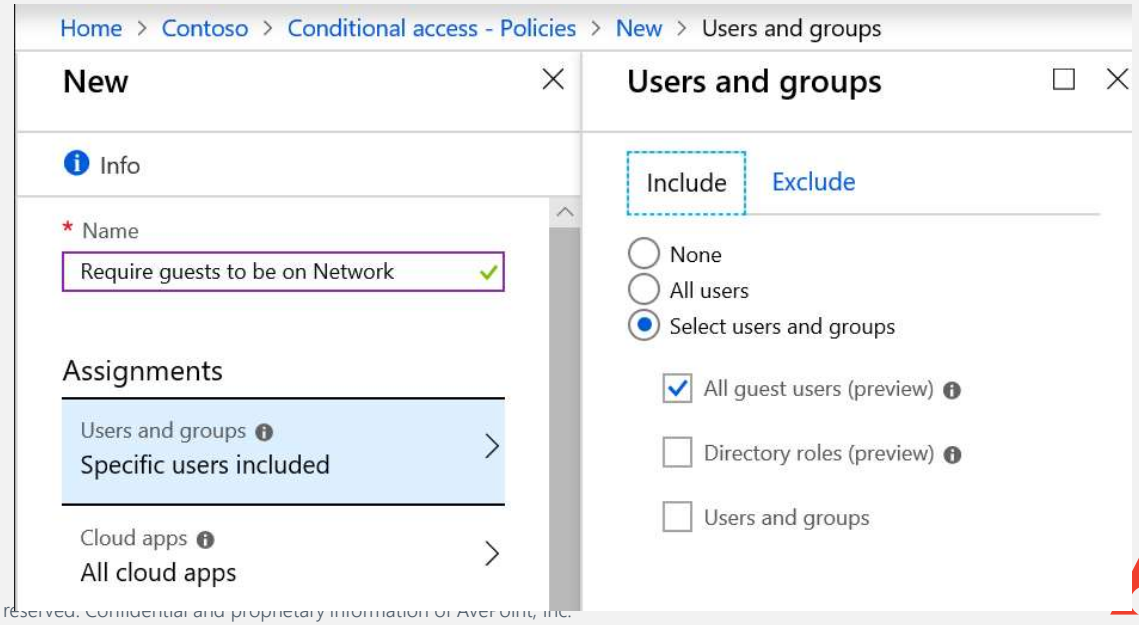


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Conditional access for guest users

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

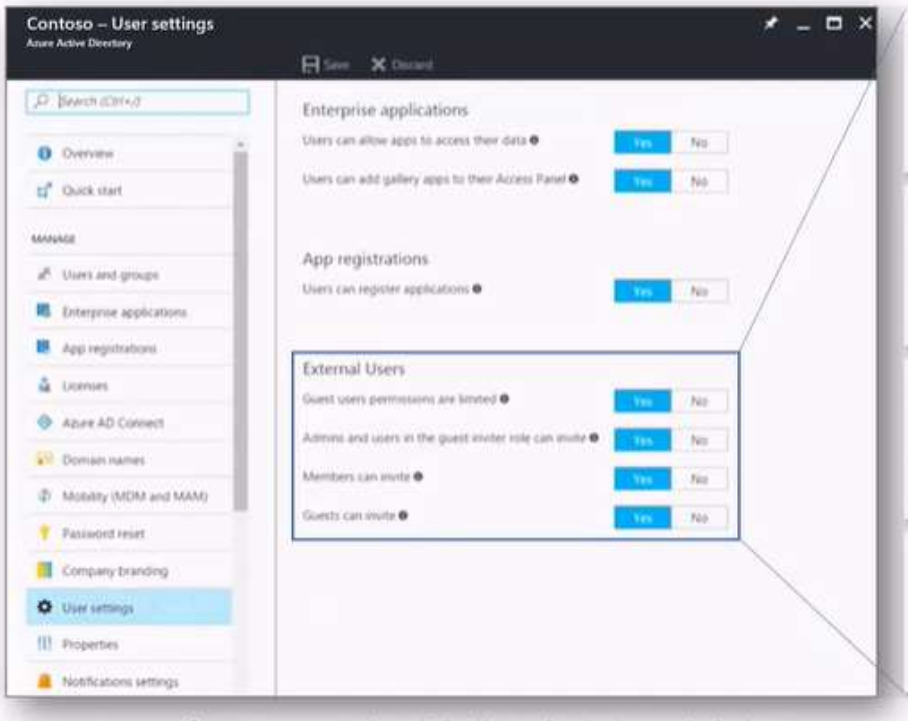
Can also have policies *specific* to guests



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

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.

May 2018 Level 200

Learn more about B2B delegated invitations and roles here:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations | https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-guest-to-role

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

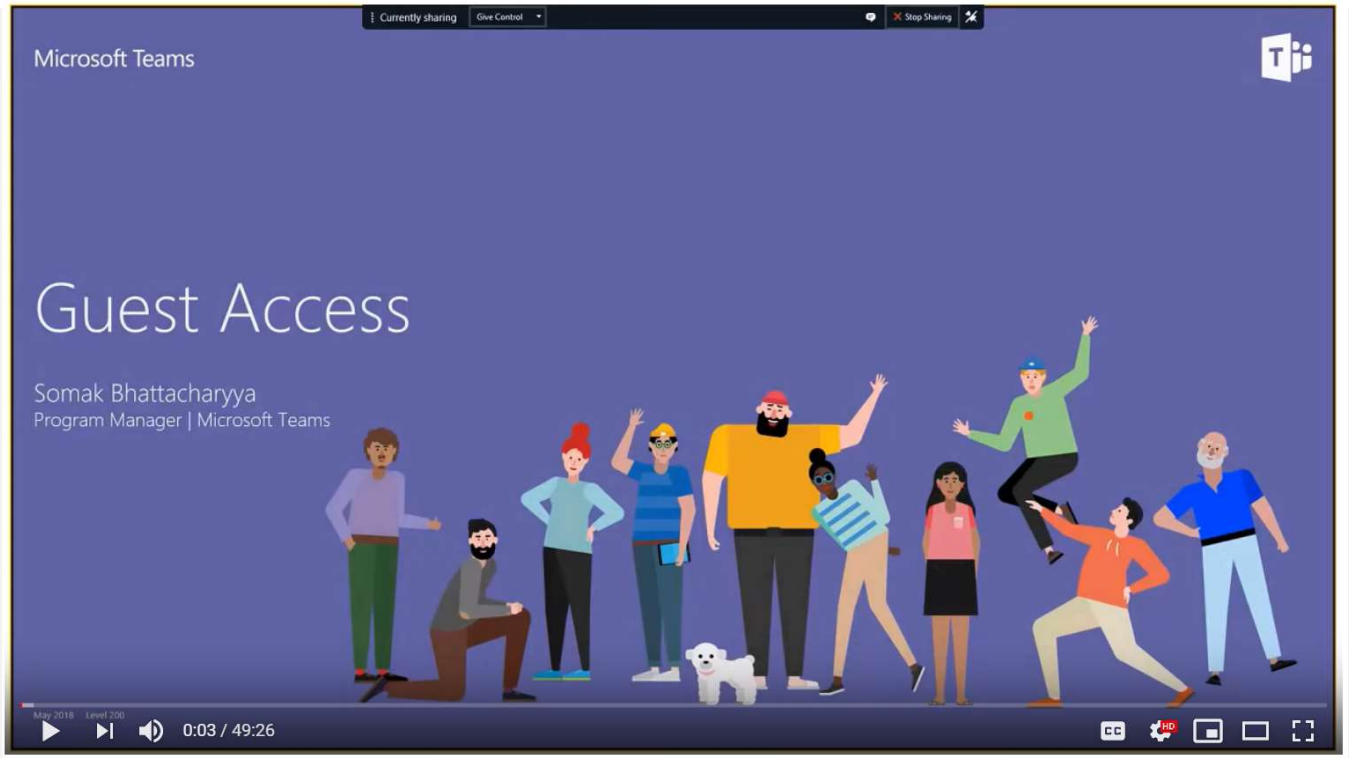
- Included as part of O365 subscriptions at no additional cost; up to 5 guests per one user on your tenant
- Subjected to Azure AD and O365 Service Limits

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

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

And also watch this!

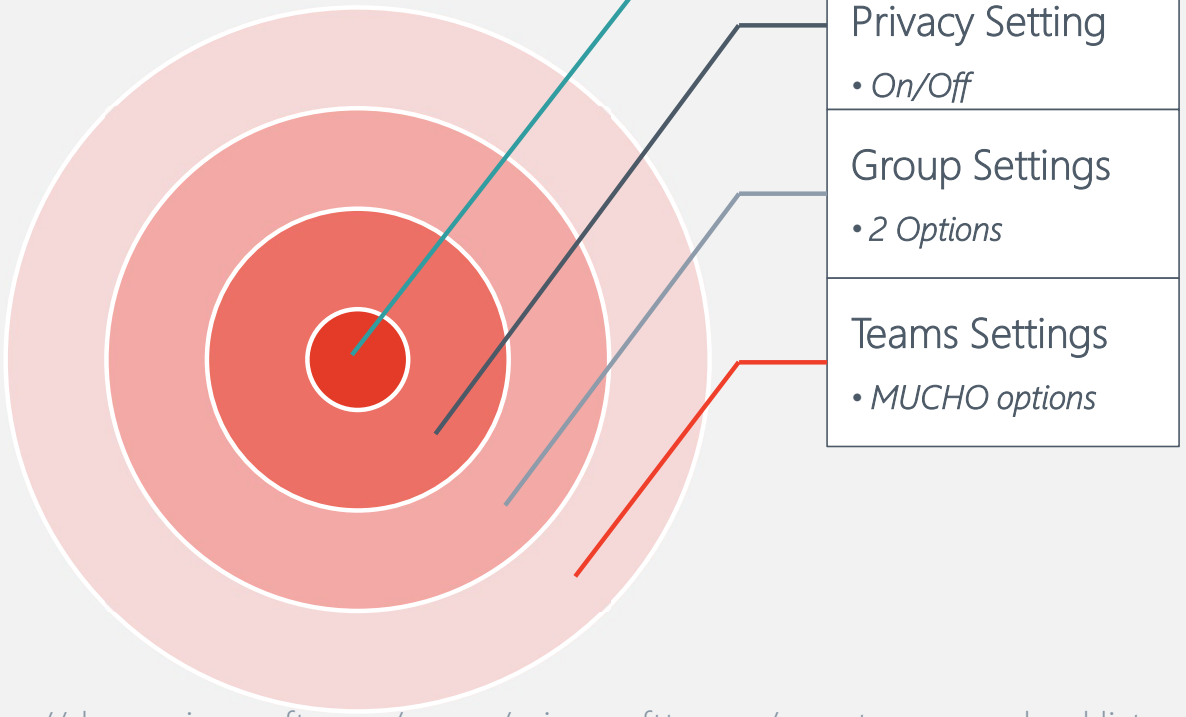


Microsoft Teams Best Practices for Managing Guest Access

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

@JohnConnected

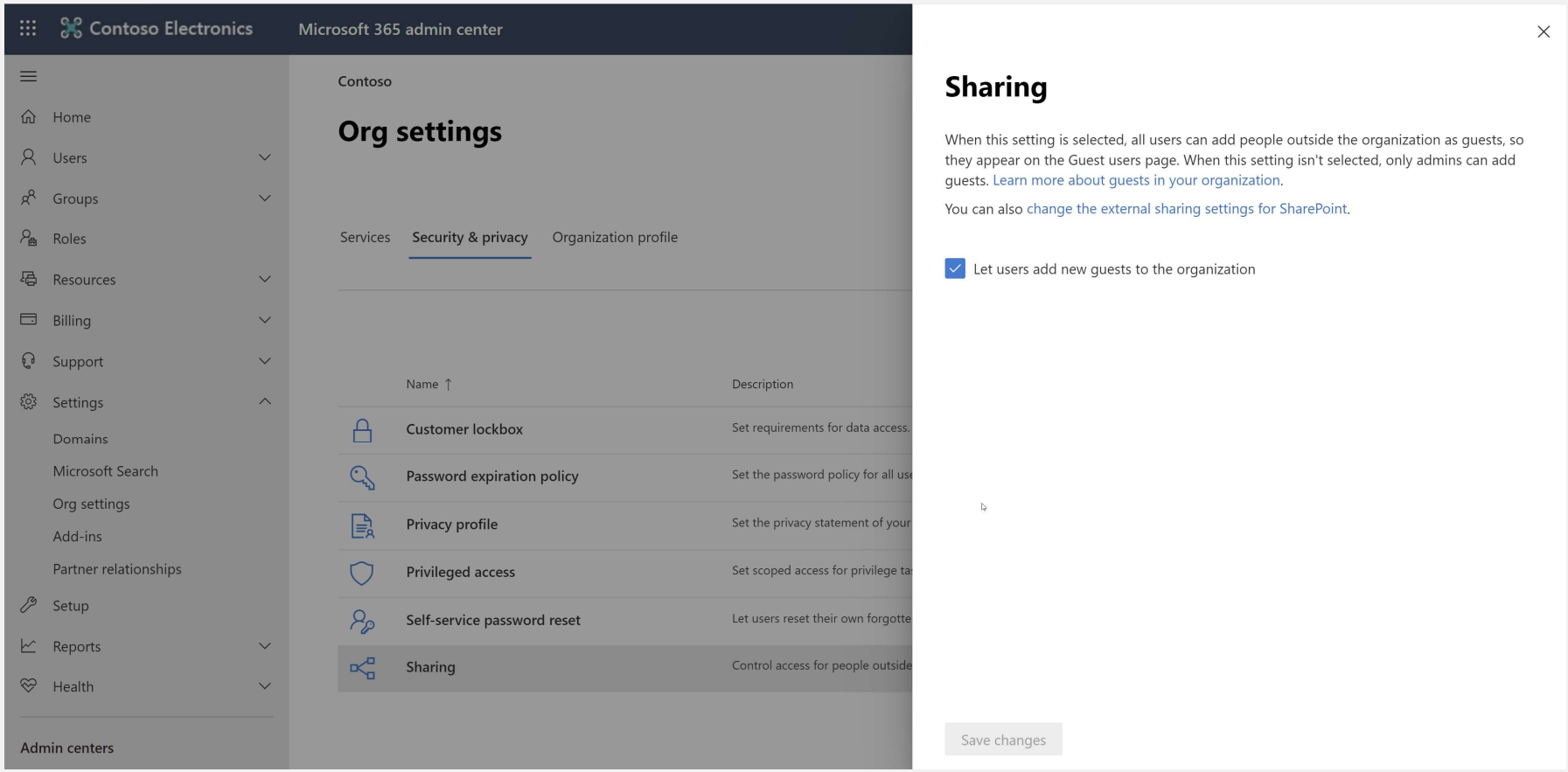
Peeling it all apart…



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

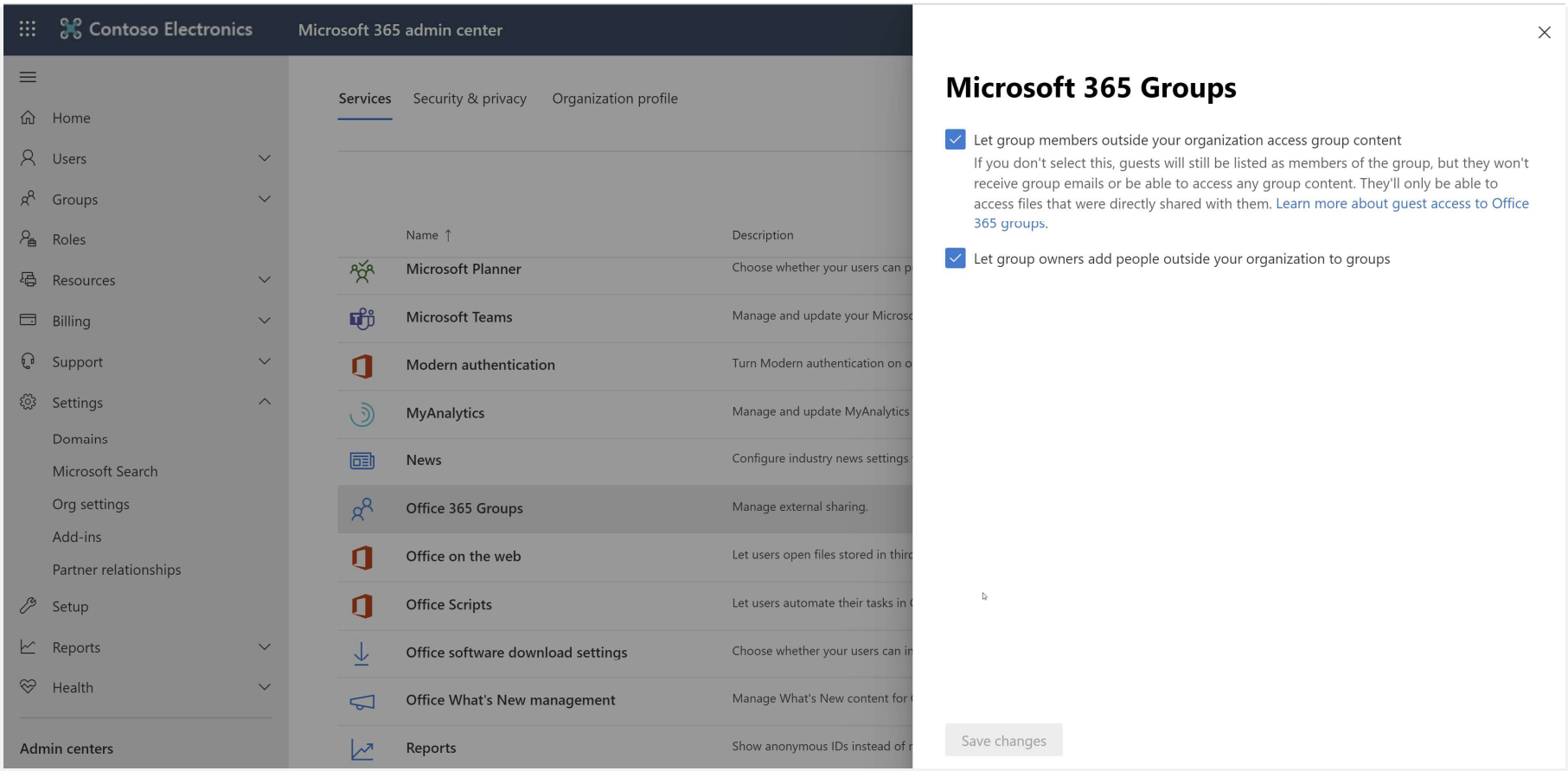
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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



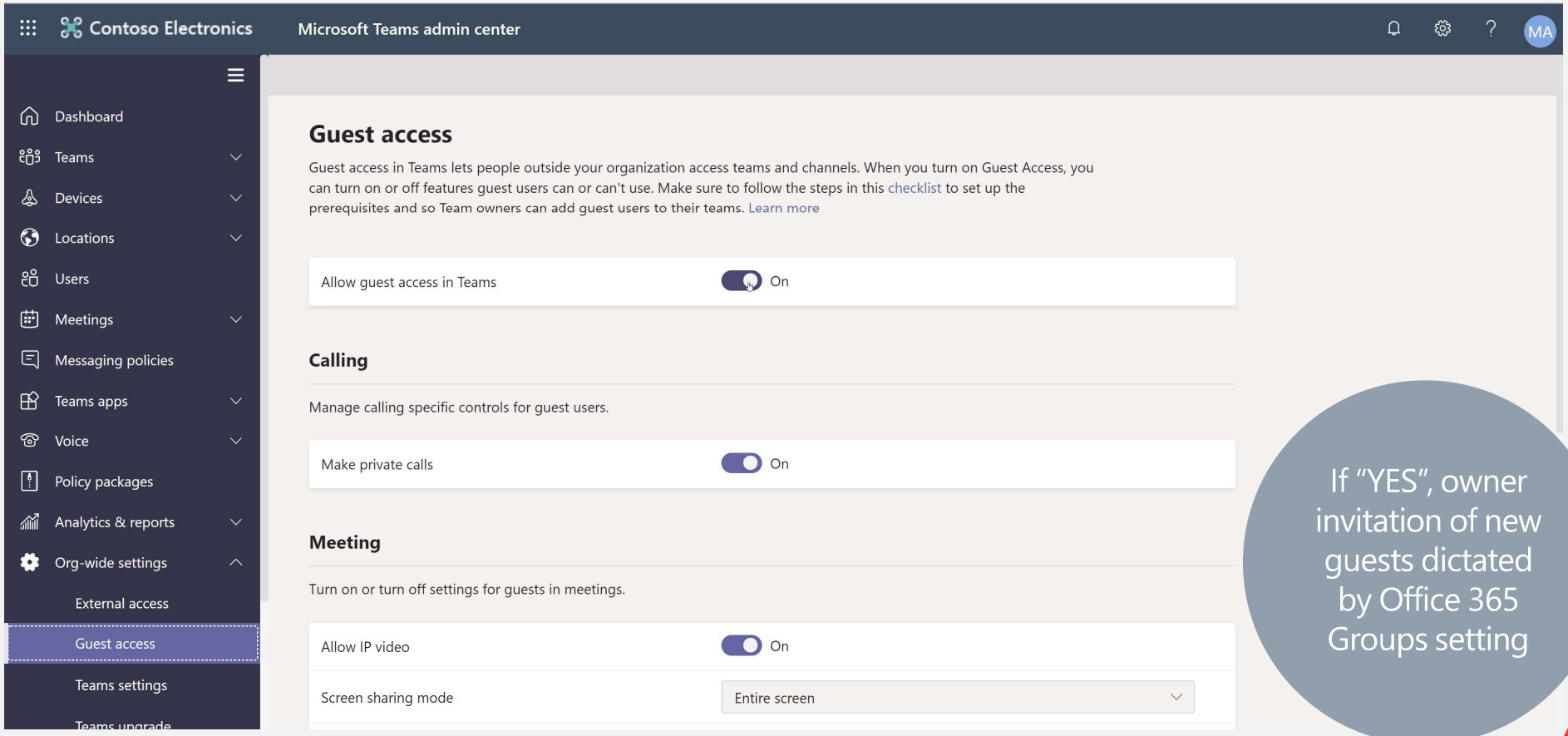
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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



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

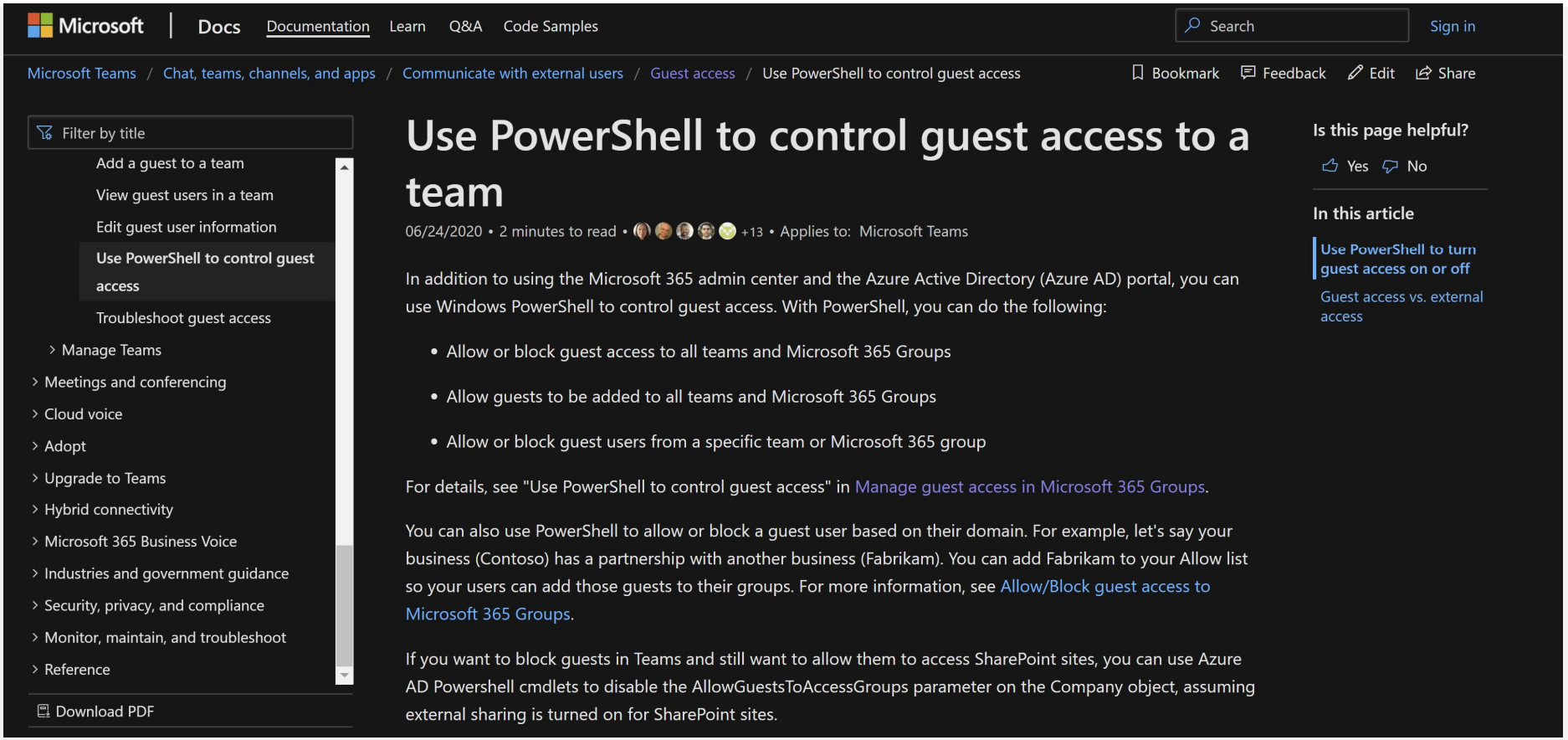
Microsoft Teams: Are *guests* allowed in Teams?



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

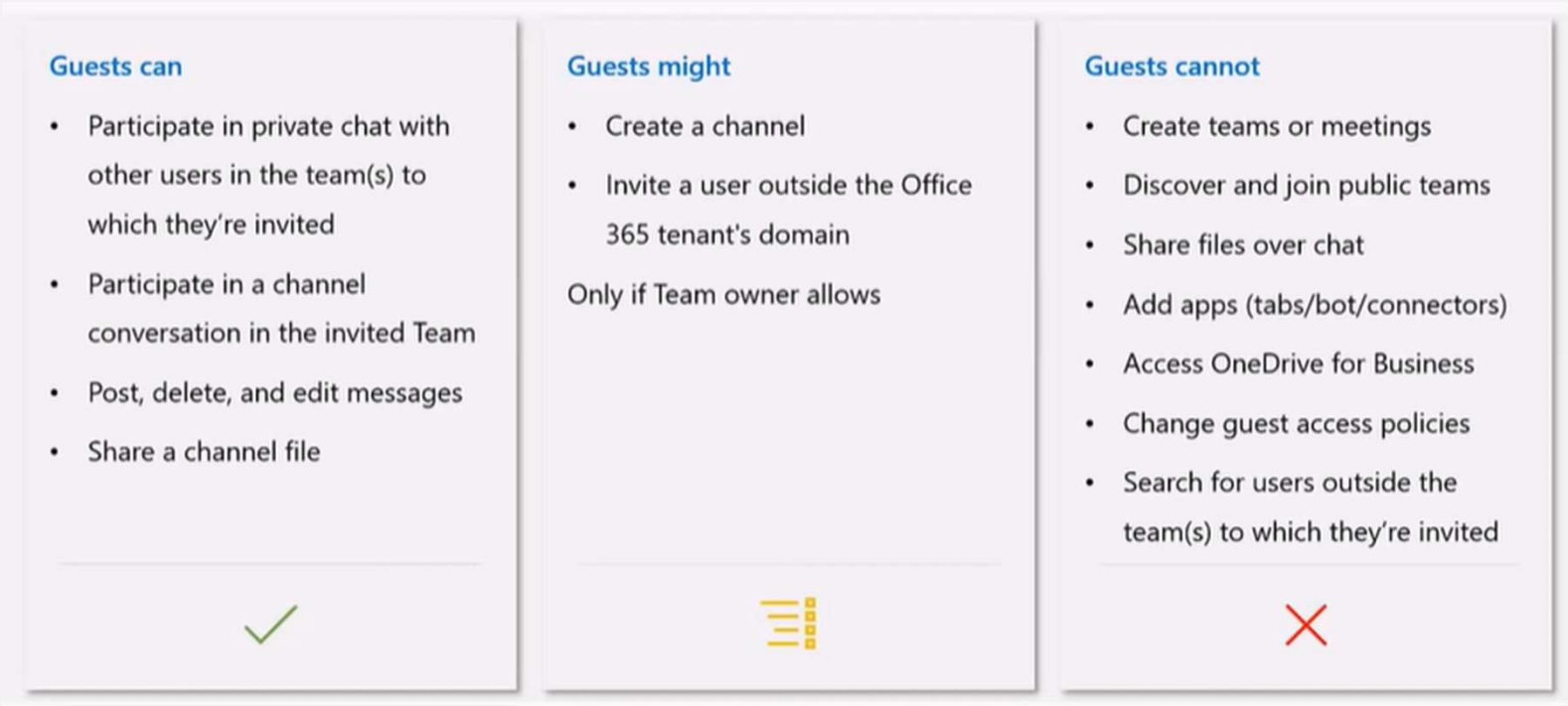
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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



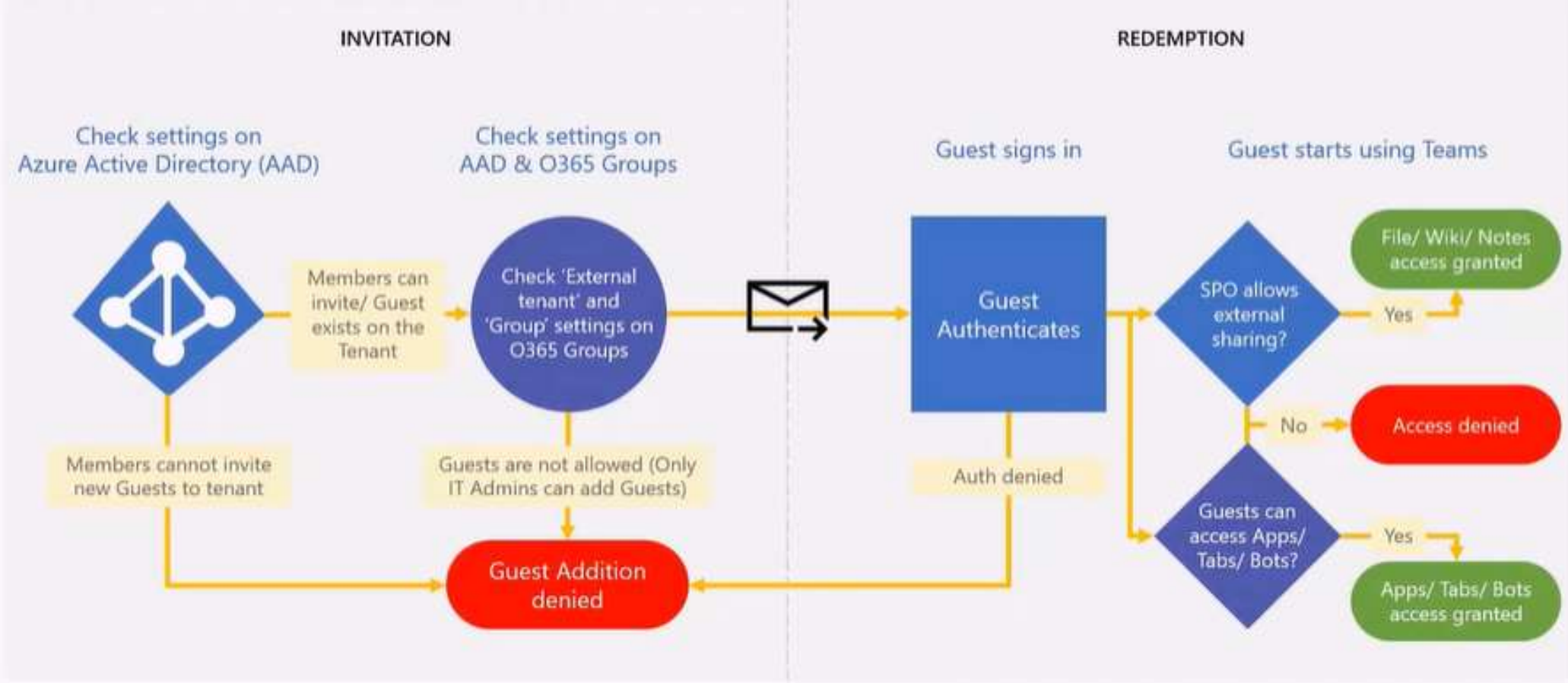
https://docs.microsoft.com/en-us/microsoftteams/guest-access-powershell

What guests in Teams can do...



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

How it all fits together…



Be careful with your "guest" and "external" terminology

Guest access vs. external access (federation)

External access (federation) and guest access are different:

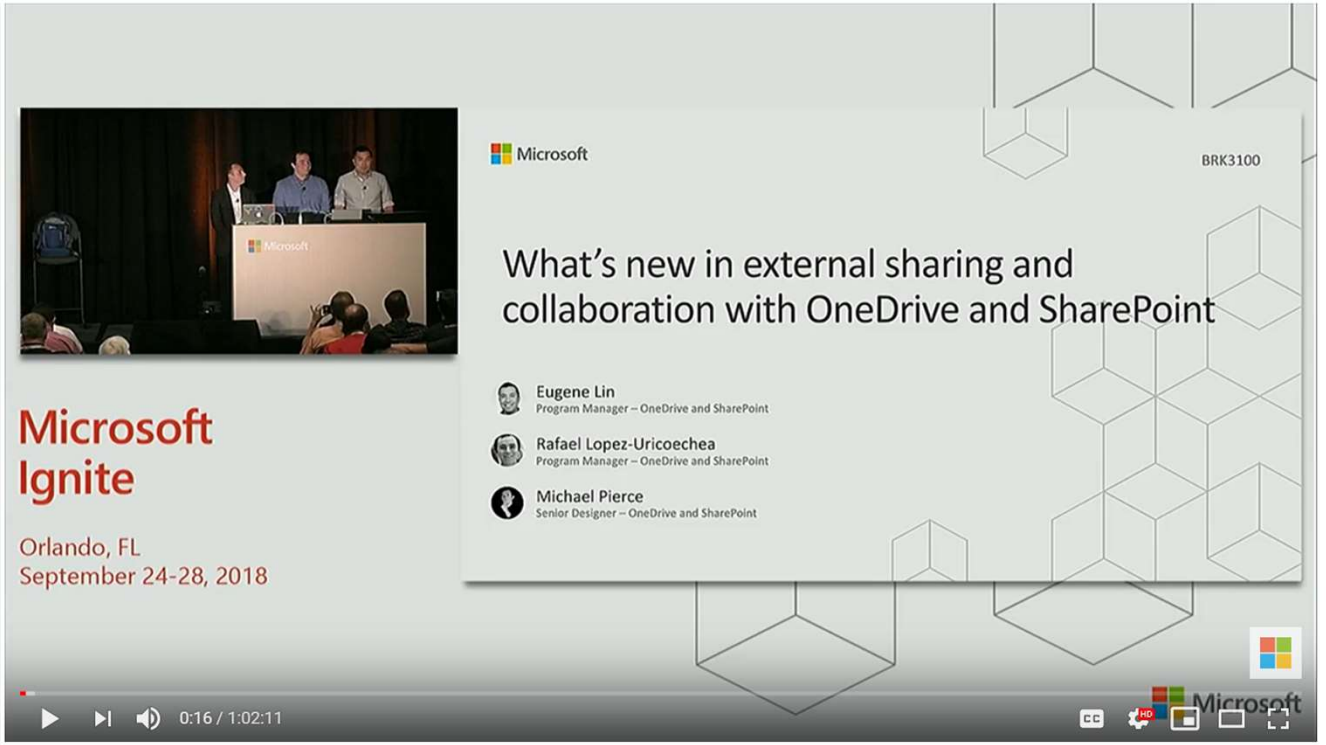
- Guest access gives access permission to an individual. External access gives access permission to an entire domain.
- Guest access, once granted by a team owner, allows a guest to access resources, such as channel discussions and files, for a specific team, and chat with other users in the team they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

Demo:
Configuring Teams and Groups for Guest Access

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

And you should probably also watch this!



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

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

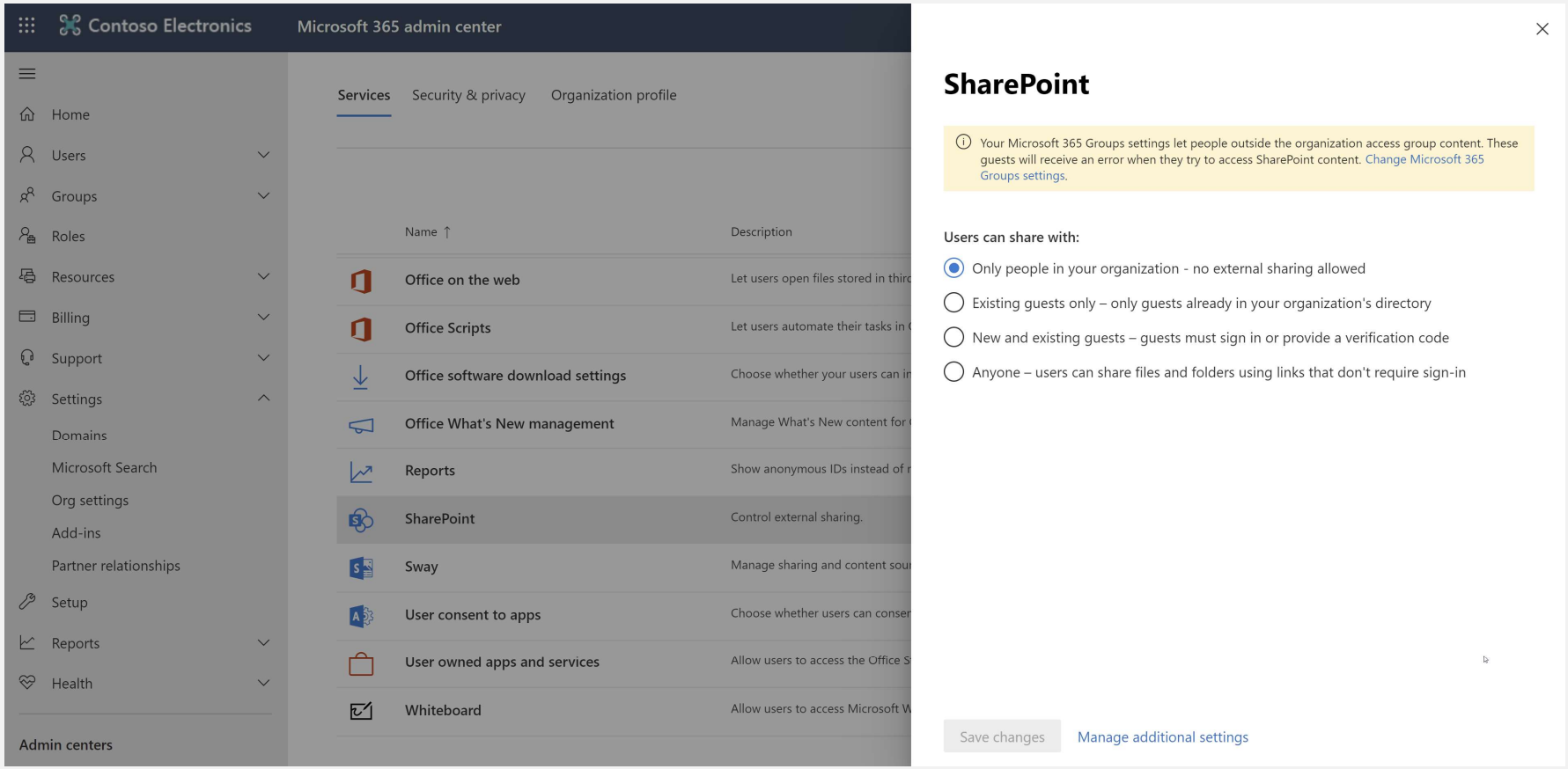
Enabled, but not default

Mandatory expiration date

Block externally-shareable edit links

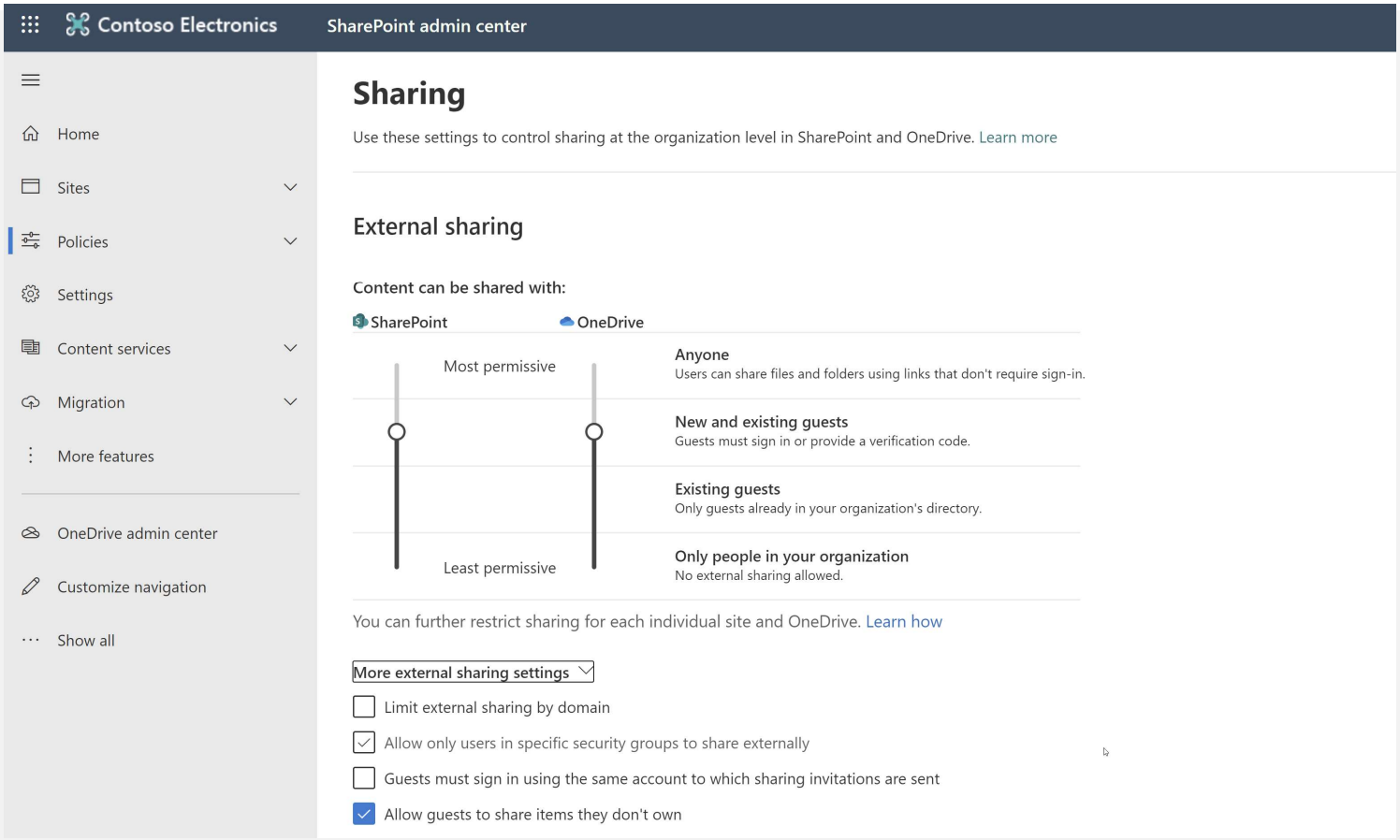
Disabled

SharePoint: Is *"External Sharing"* allowed?



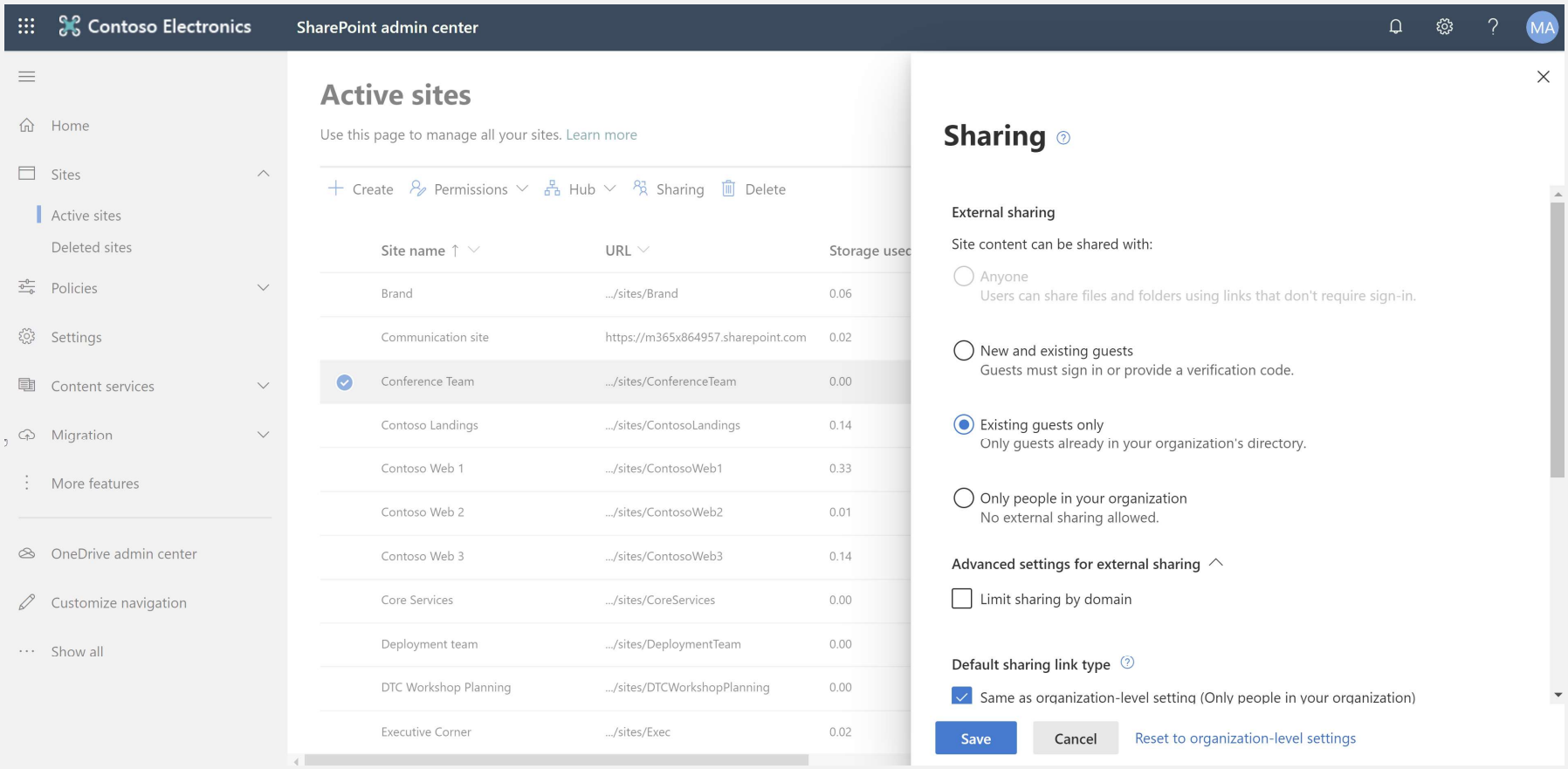
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

SharePoint: What are the *global* settings?



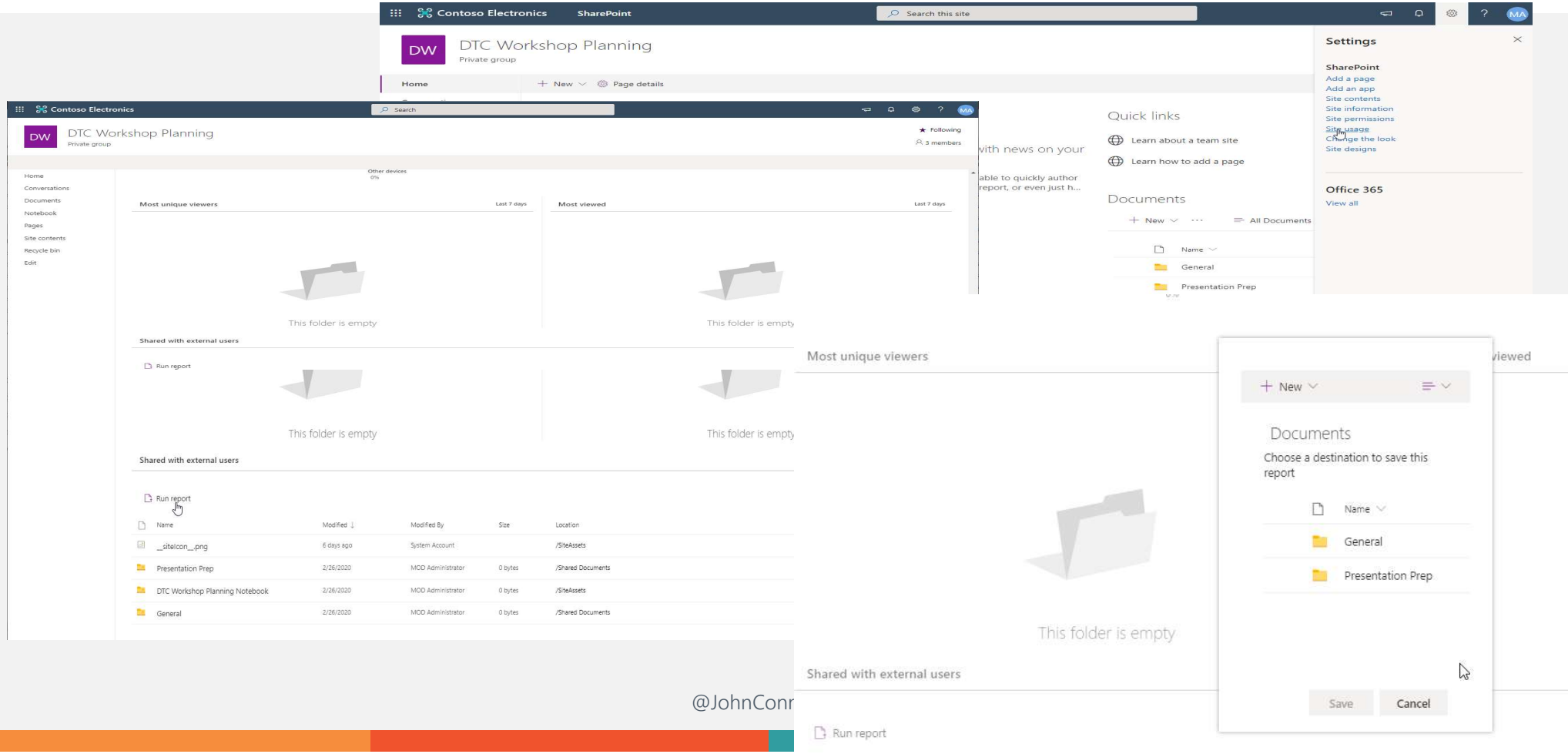
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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

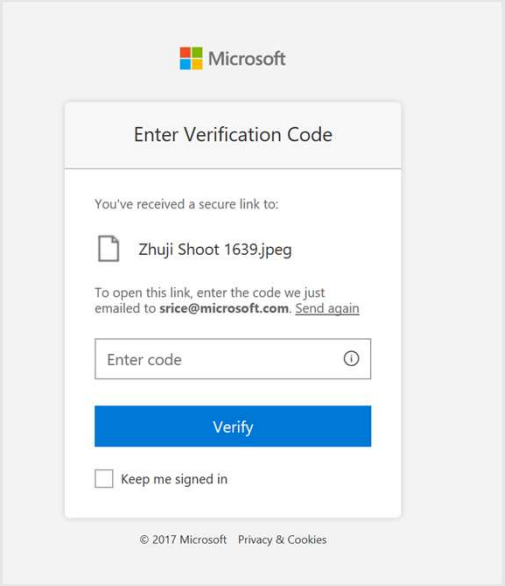


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

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



NEW! Azure AD B2B for one-time passcode users



Share securely with anyone in the world

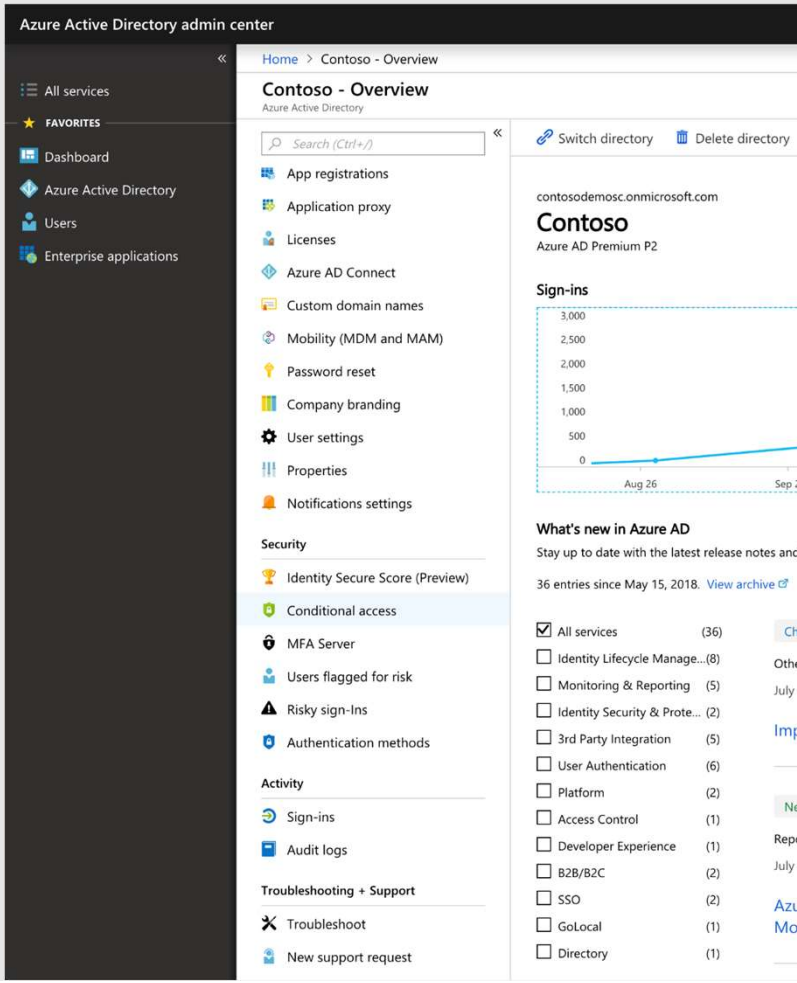
Simple verification with one-time passcode

AAD B2B guest management

Conditional access

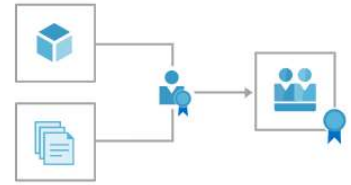
Google auth federation

Guest do not require O365 licenses



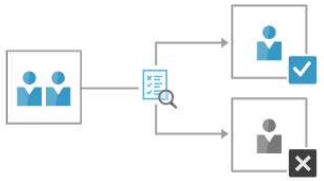
Demo:
Configuring and exploring SPO/ODFB external sharing

Understanding Entitlement management & Access reviews



Entitlement management

- 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



Access reviews

- Manage access to each group or application *(not stand-alone 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?

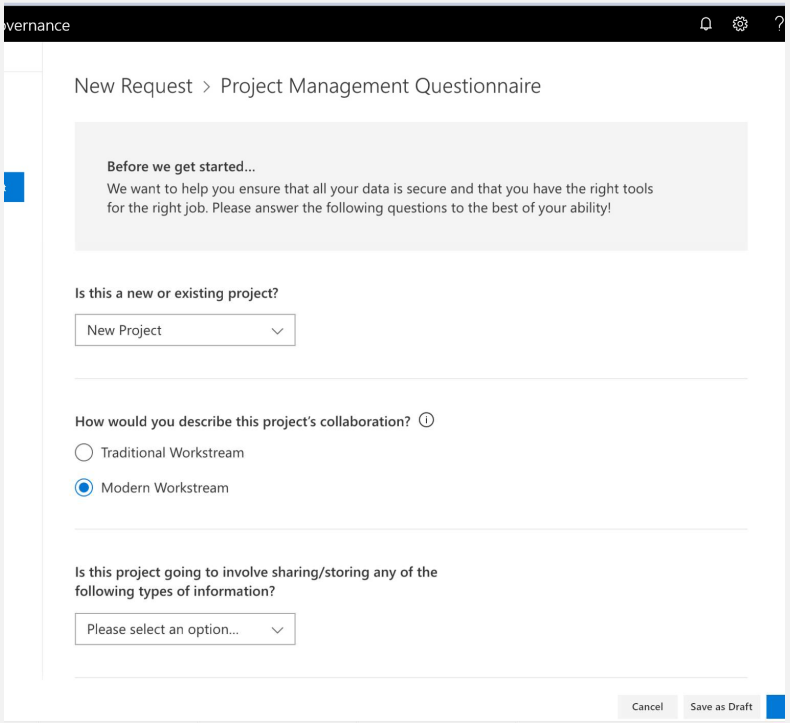
How will you handle the lifecycle of guests?

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



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

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

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

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

Cloud Governance

Kat Larsson

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 tha
for the right job. Please answer the following questions to the b

Is this a new or existing project?

New Project

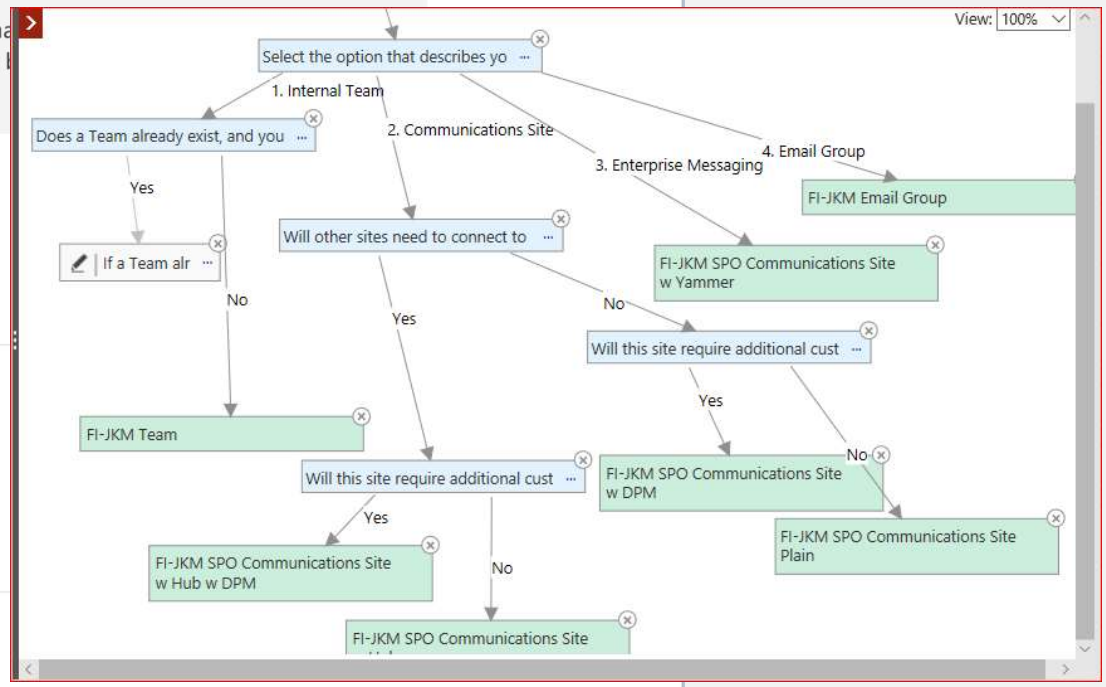
How would you describe this project's collaboration?

- ○ Traditional Workstream
- ◉ Modern Workstream

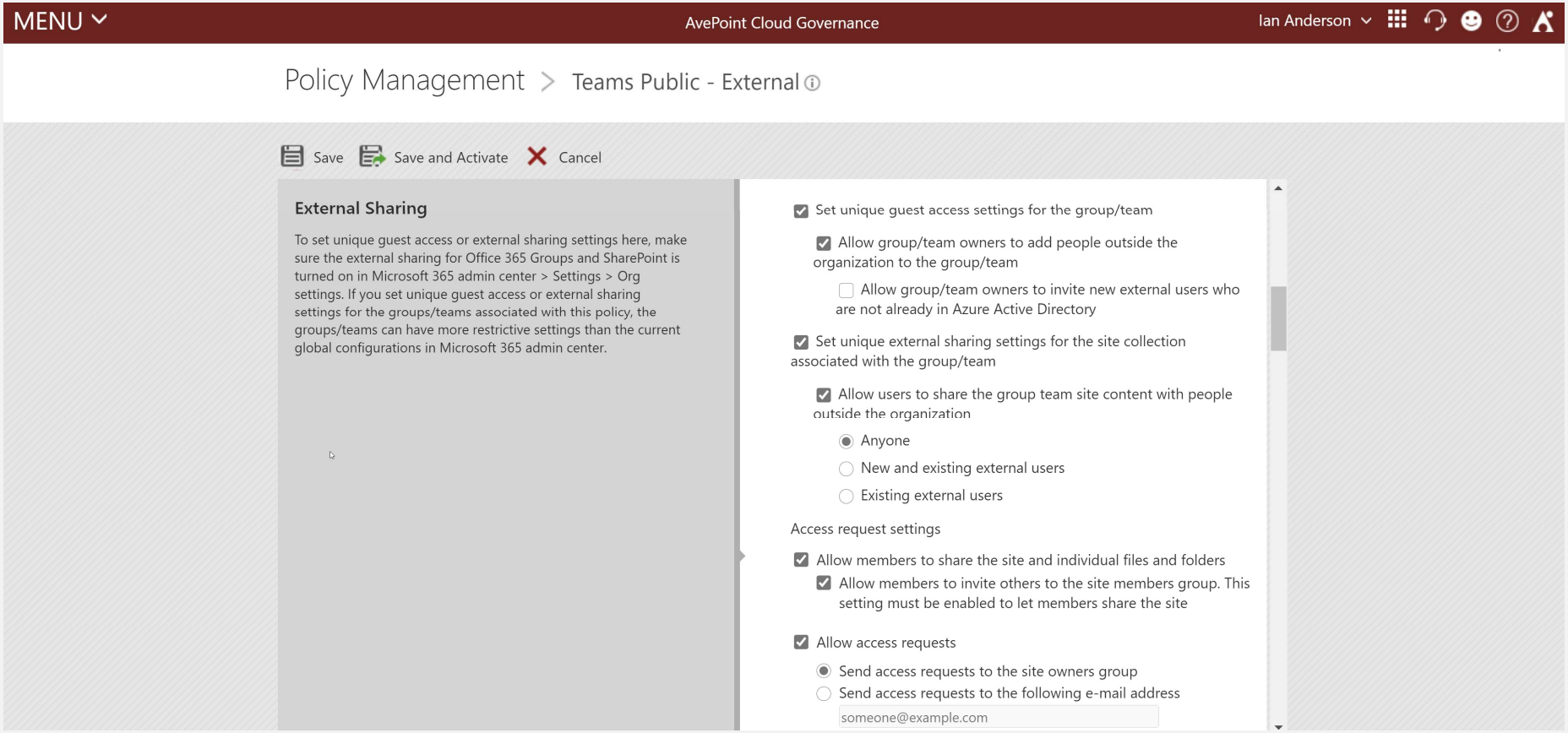
Is this project going to involve sharing/storing any of the following types of information?

Please select an option...

Cancel | Save as Draft | Next

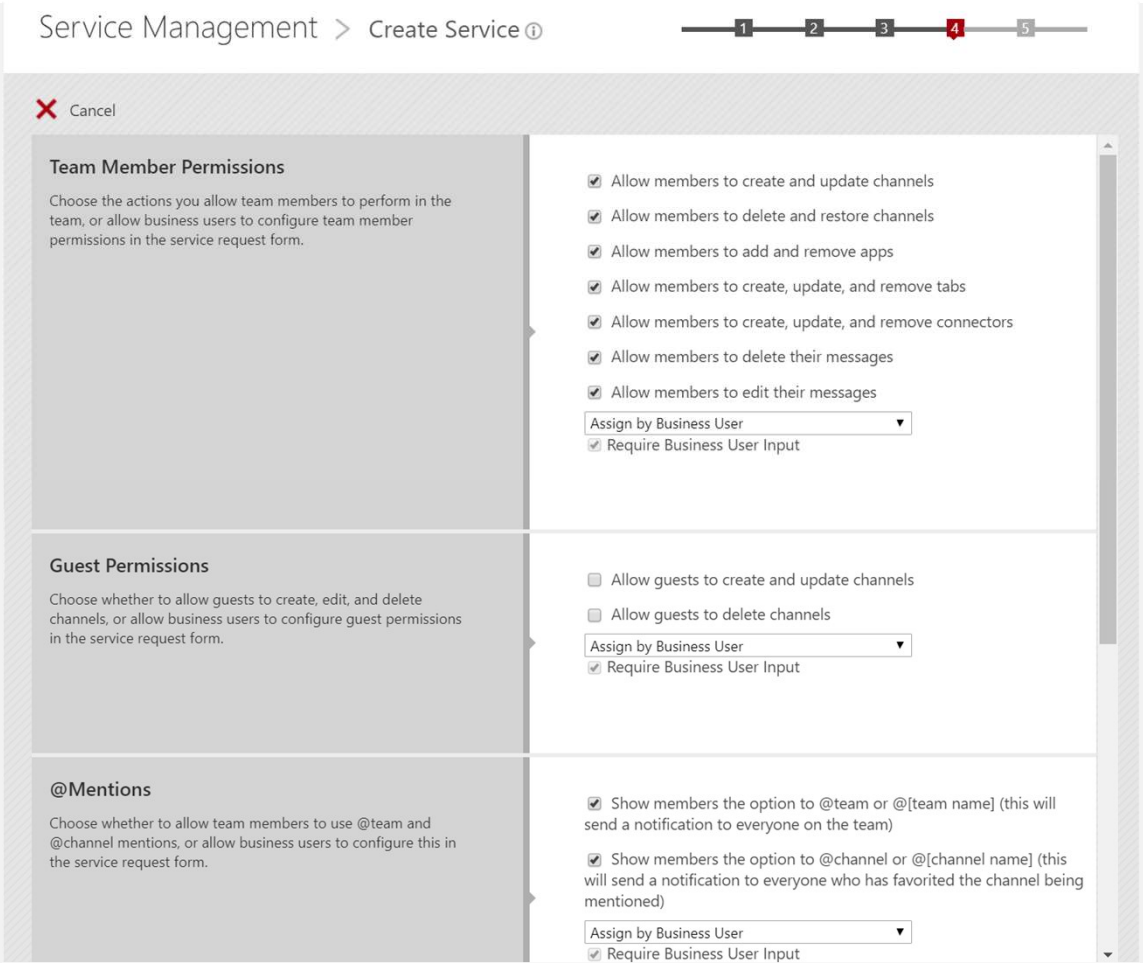


Governing external access through Policy

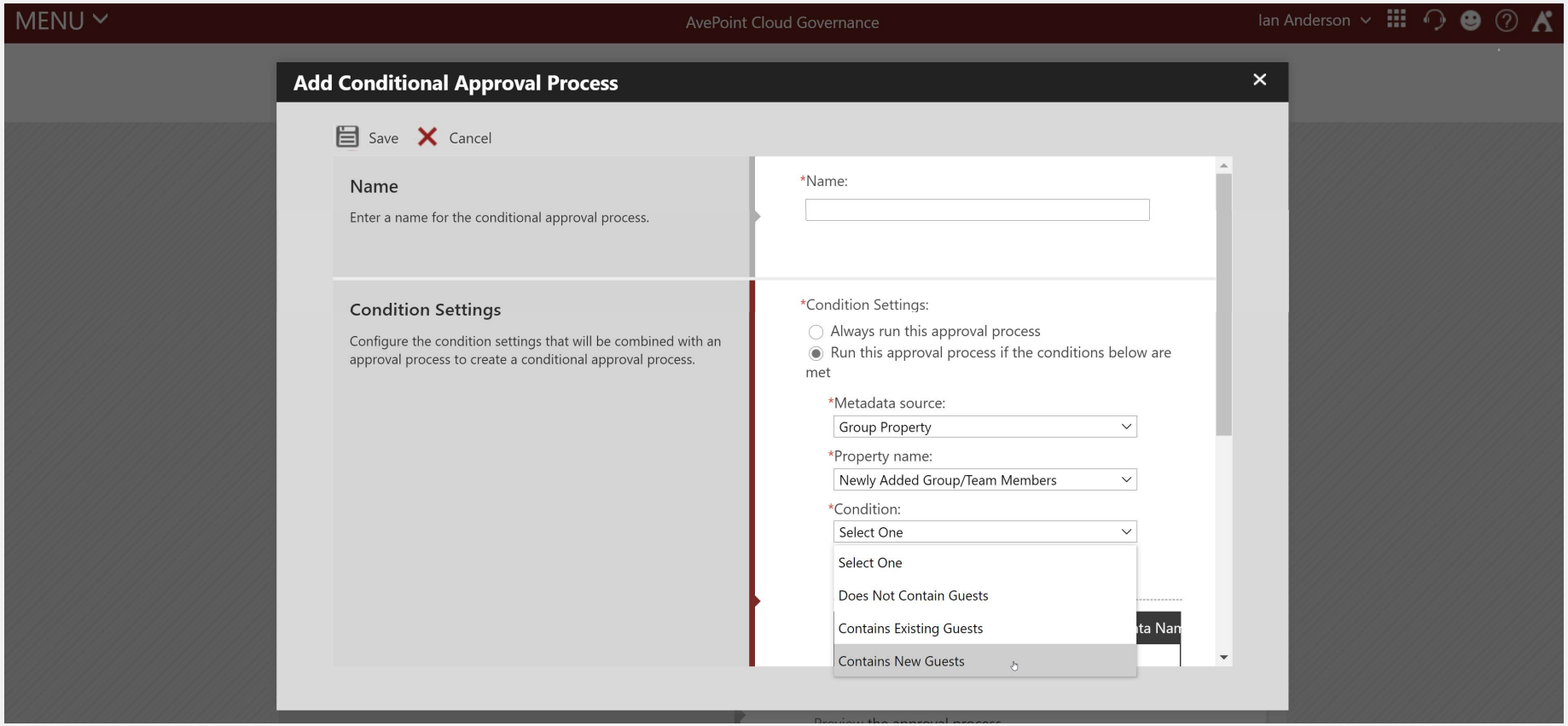


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Defining options available for request



Conditional approval…



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

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 **A** Services

Division **B** Services

Division **C** Services

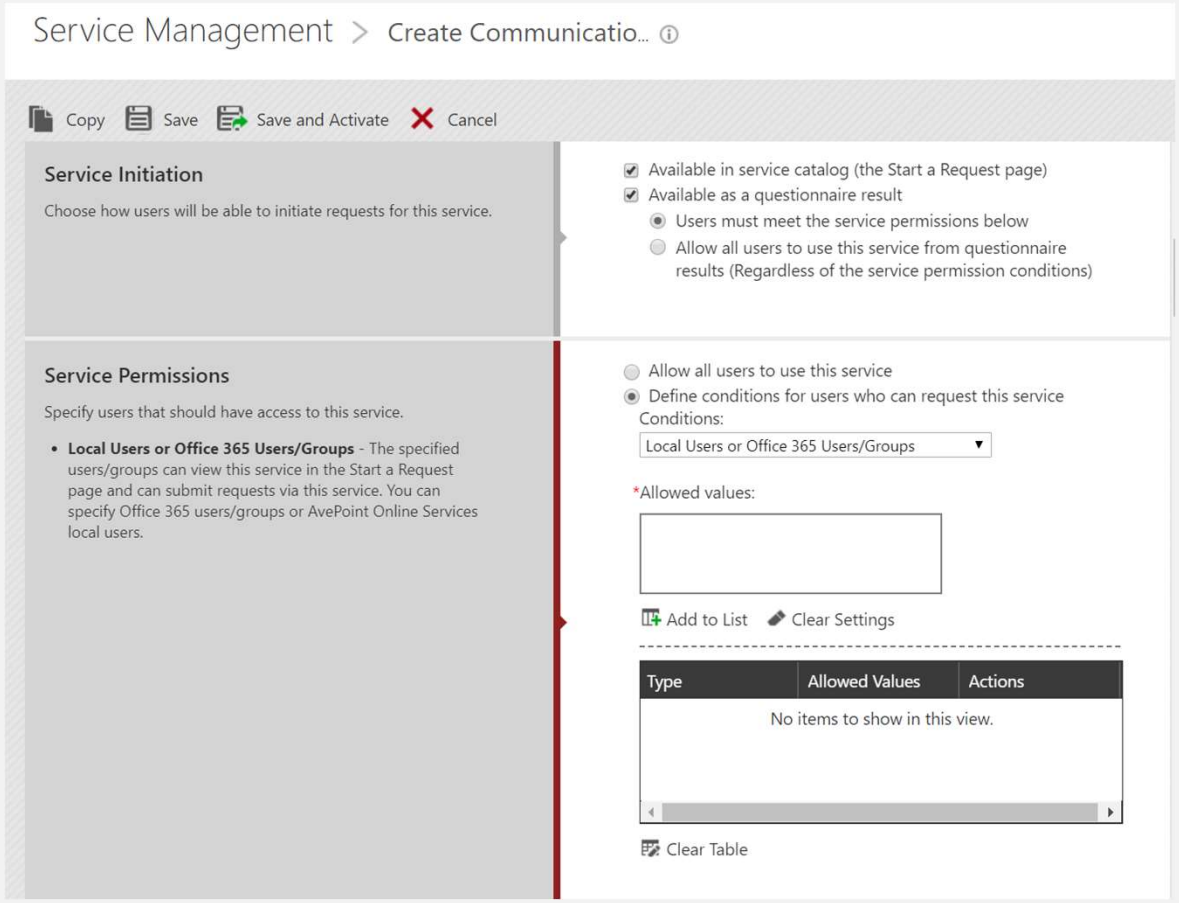
Specialized Services Smaller Groups

- Unique needs can be addressed
- Pilots of future services

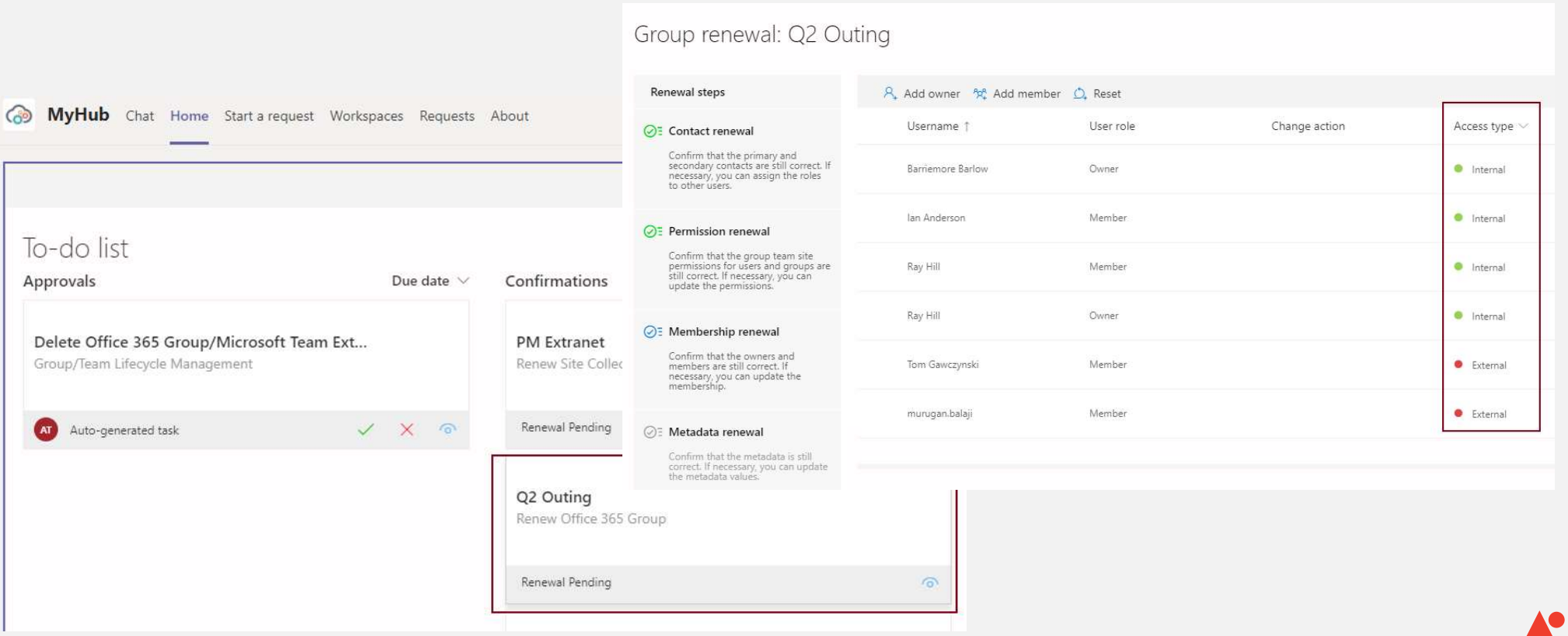
Team C-1
specialized Services

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

Leveraging “Service Permissions” to map services to the right users…



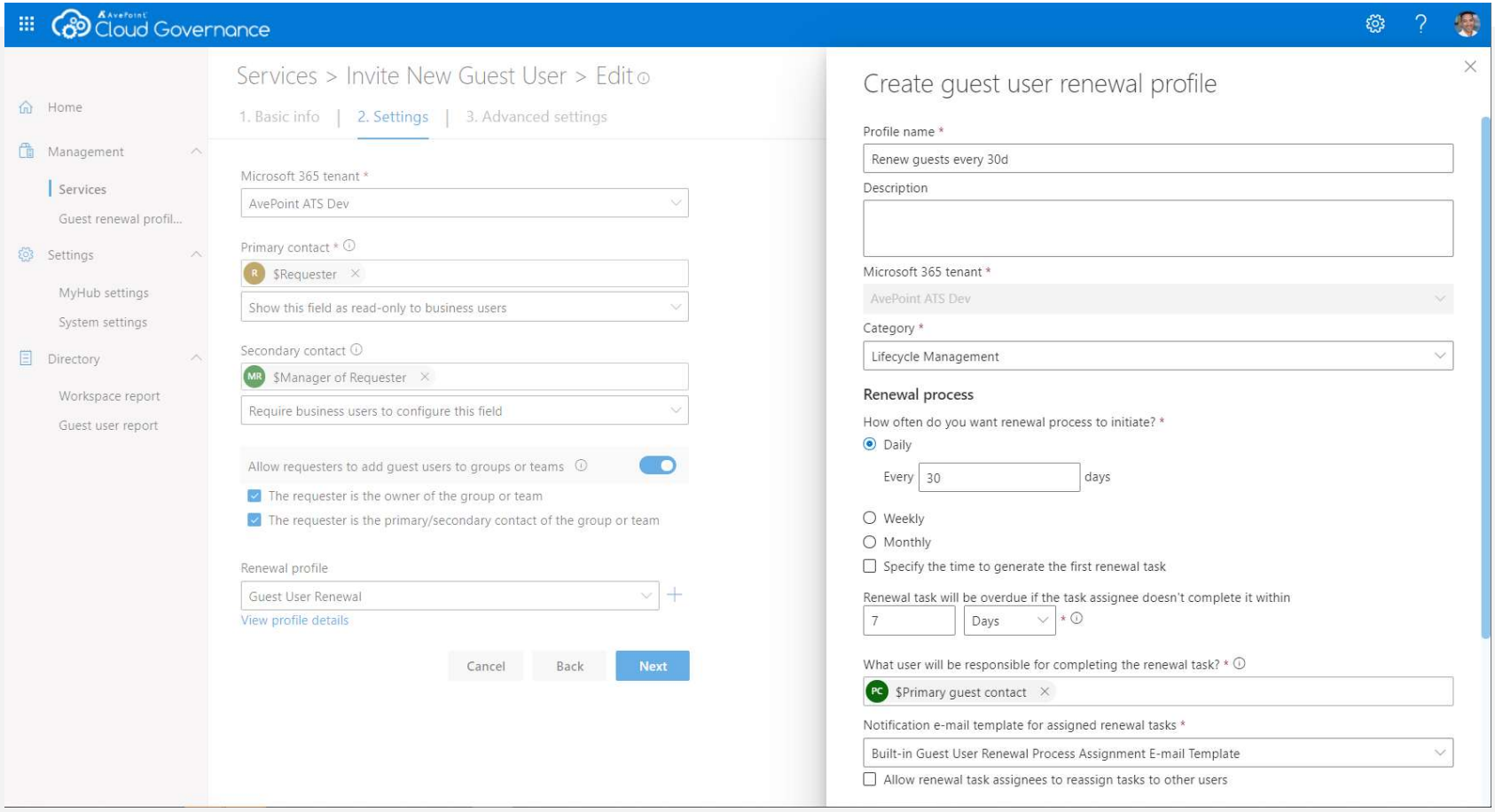
External sharing review by workspace owners during Renewal process…



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

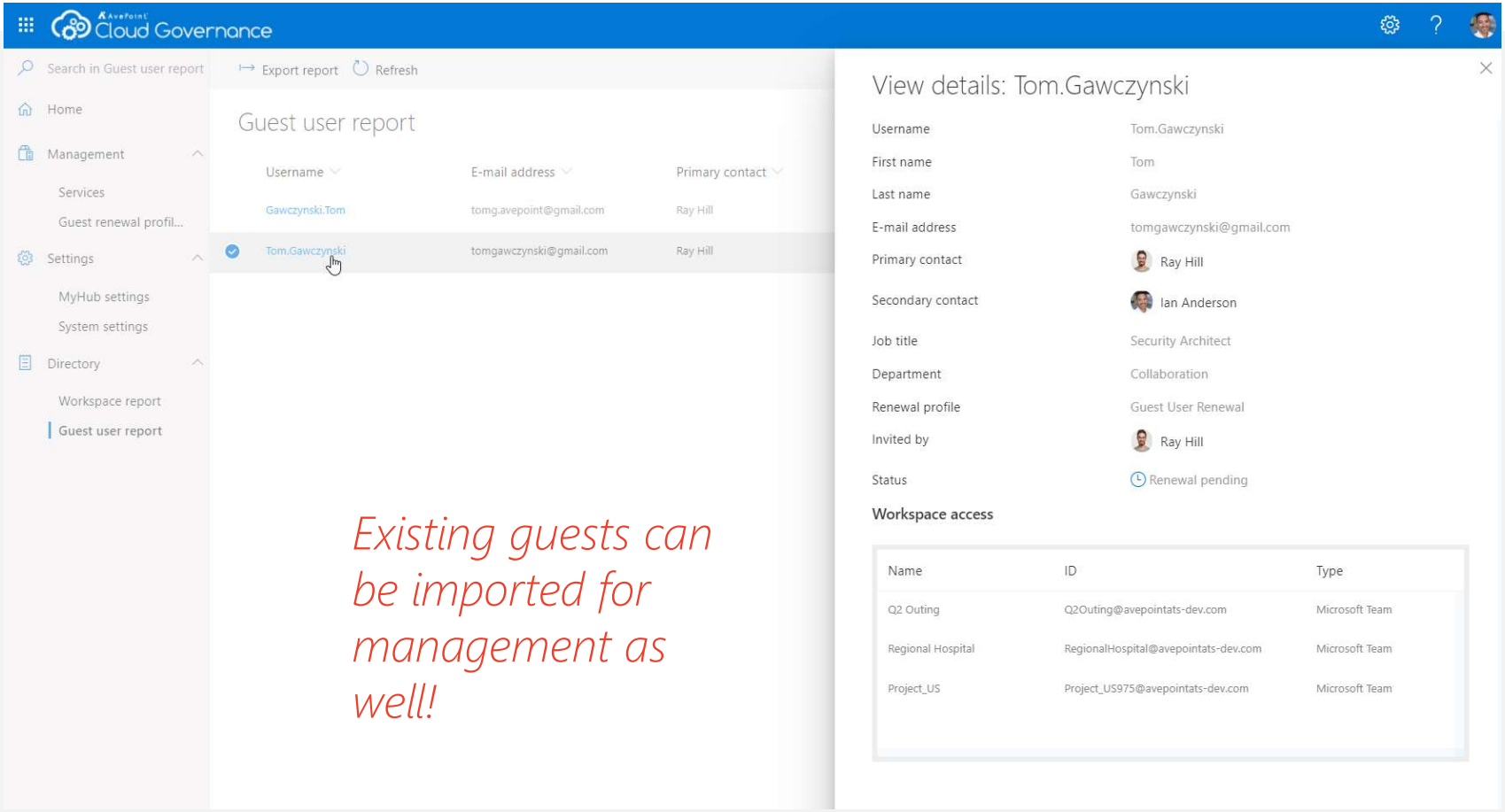
What about a managed process for *provisioning, management and lifecycle* of guests?

Designing the “Guest User Request” service



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

Admin monitoring of Guests



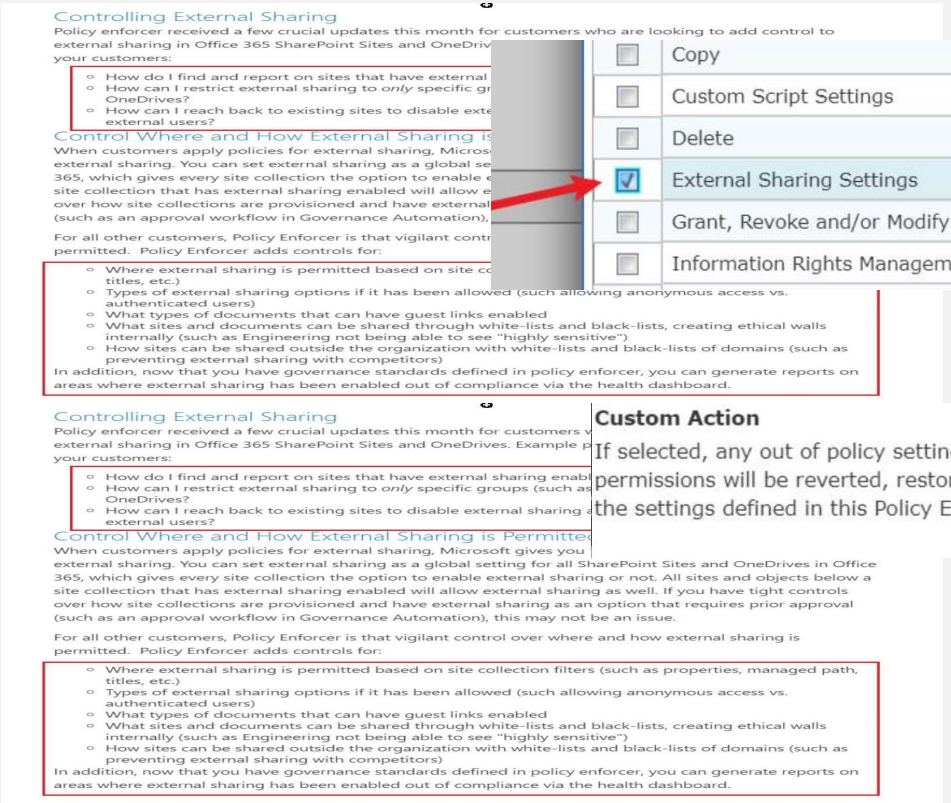
Existing guests can be imported for management as well!

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

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



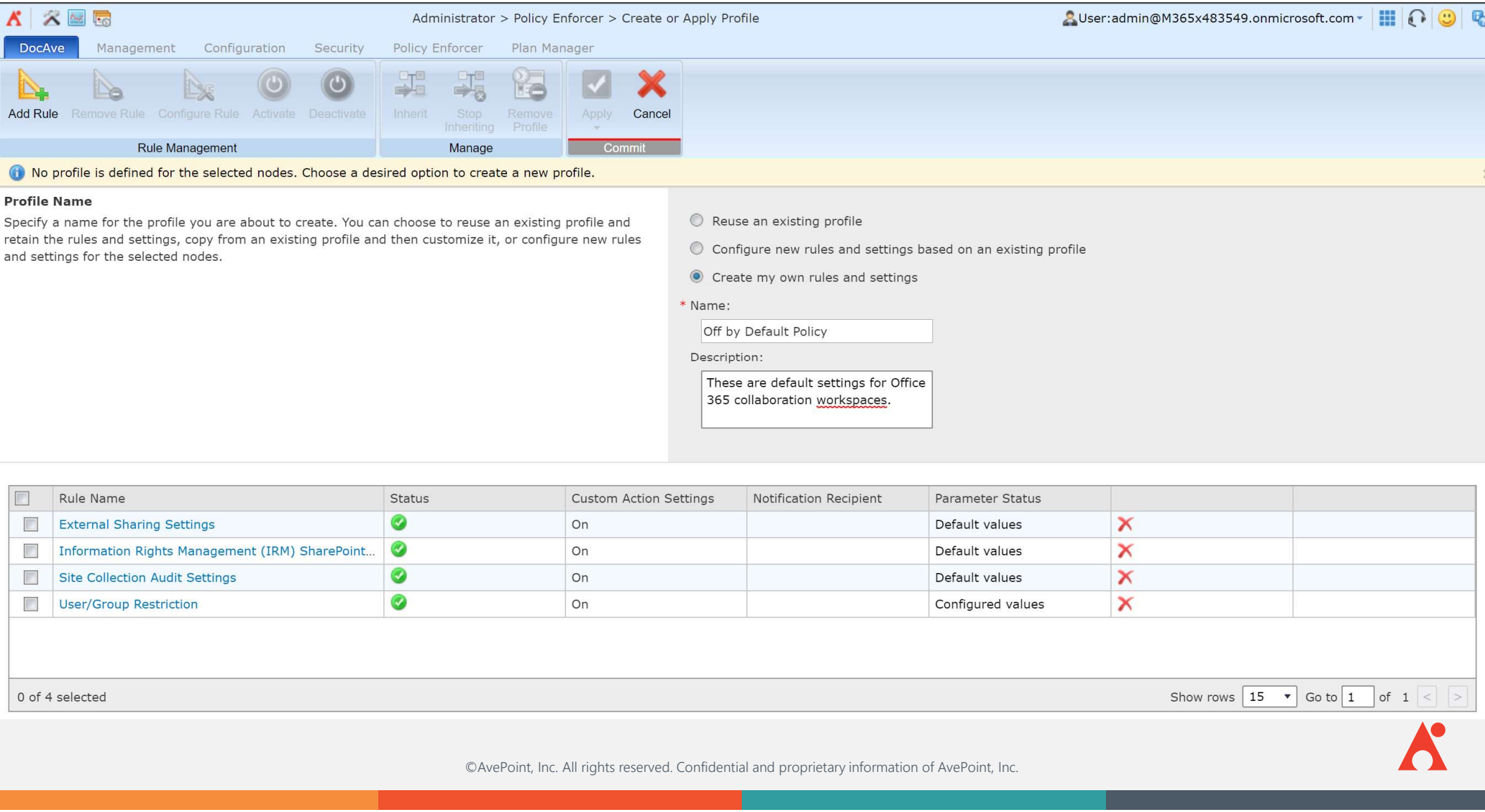
☐	Copy	Restrict or allow individual users or groups to copy SharePoint objec...	Copy
☐	Custom Script Settings	Control custom script settings on SharePoint sites (except for OneDr...	Scan Site Collection Le...
☐	Delete	Restrict or allow individual users or groups to delete items, files, list...	Delete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

Custom Action

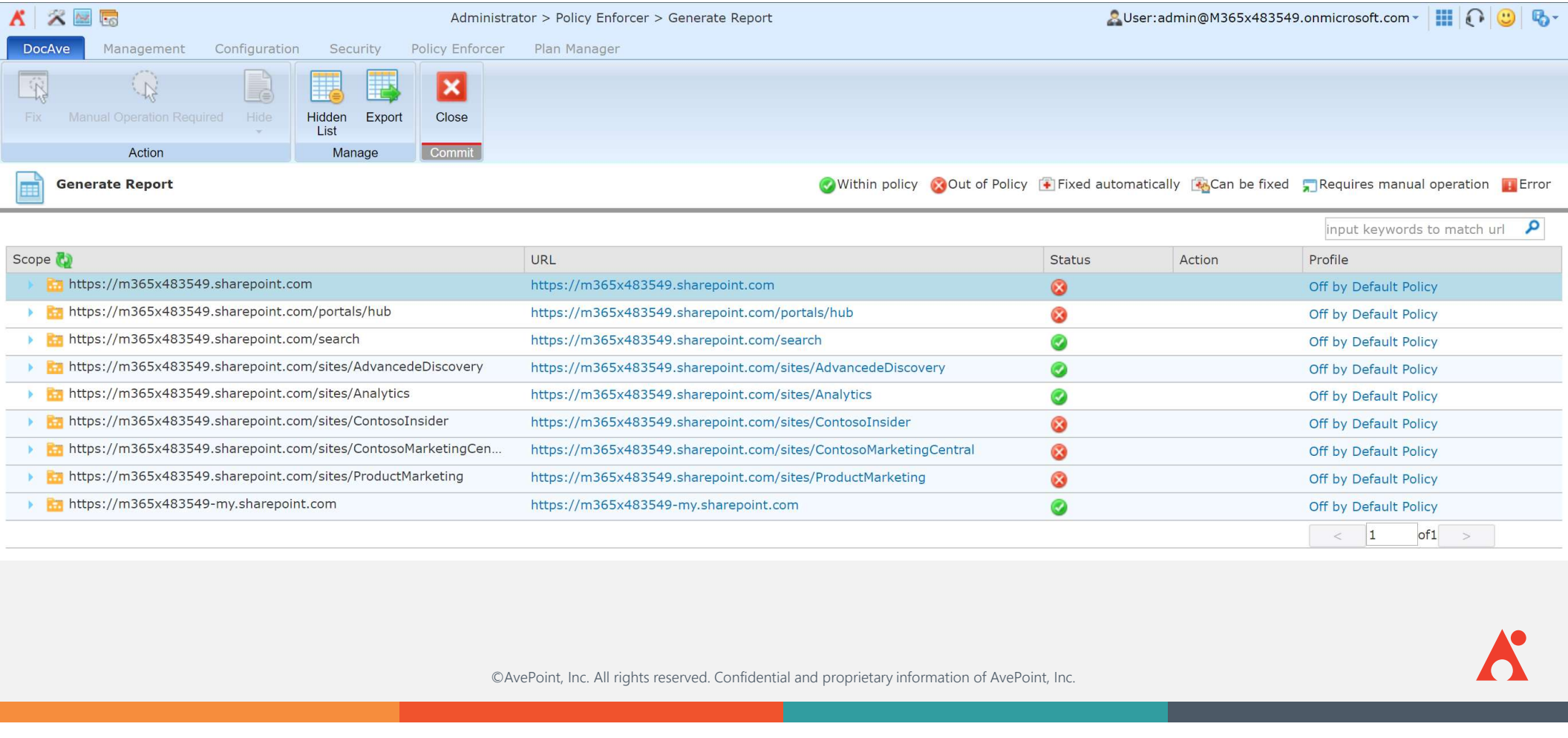
If selected, any out of policy settings, objects and/or permissions will be reverted, restored or deleted based on the settings defined in this Policy Enforcer rule.

☑ Remove external users from the site collections where external sharing is disabled

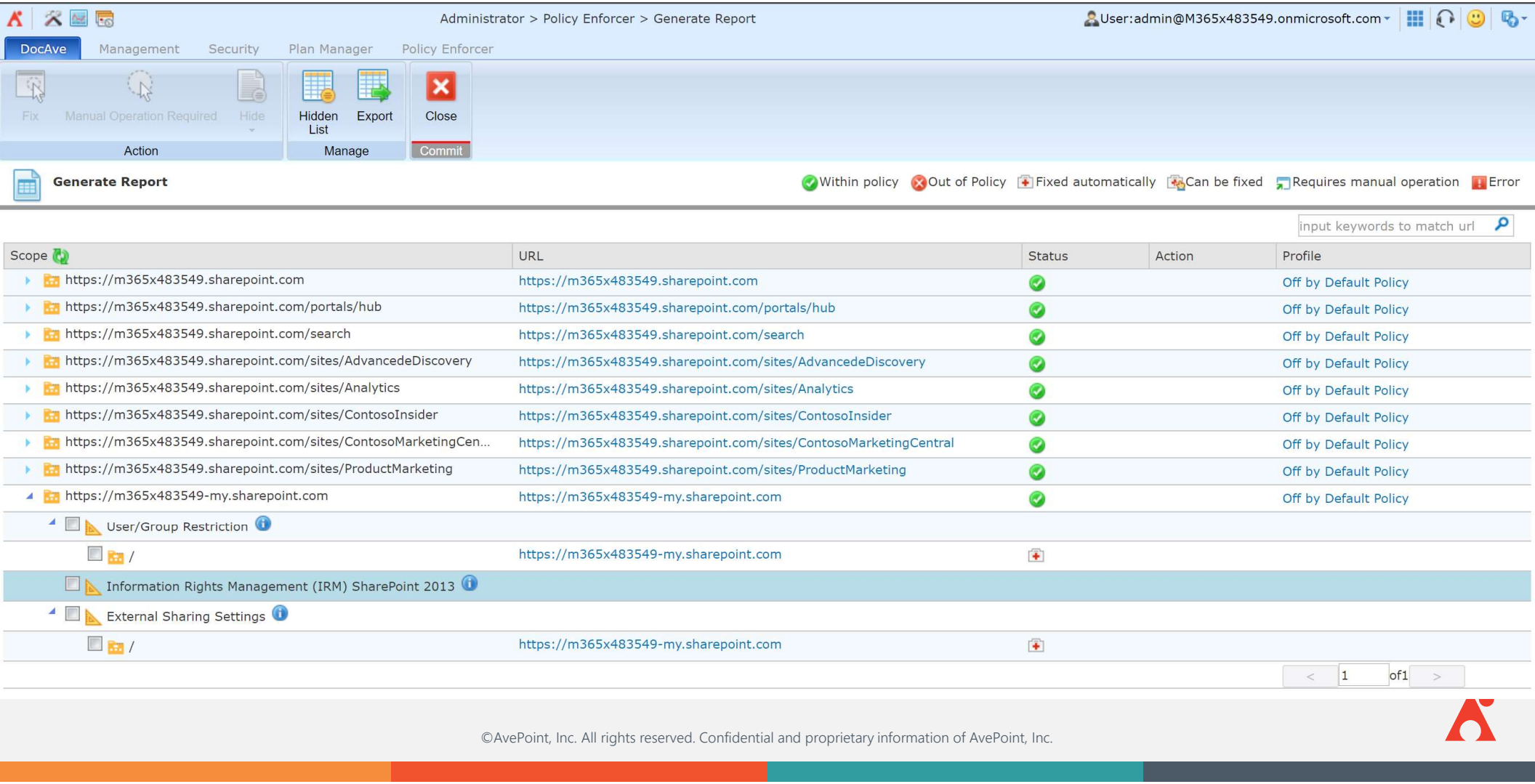
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



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

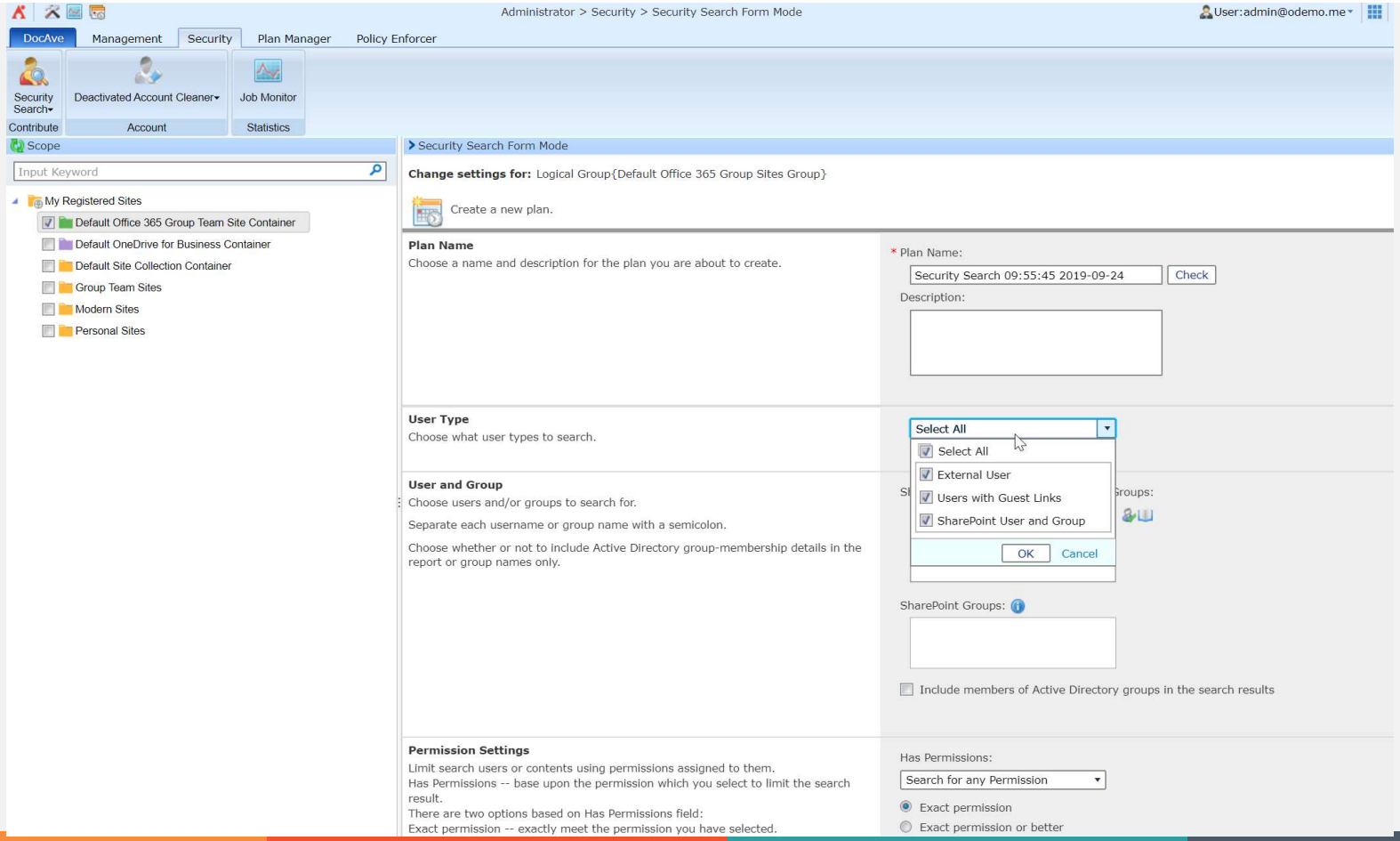


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

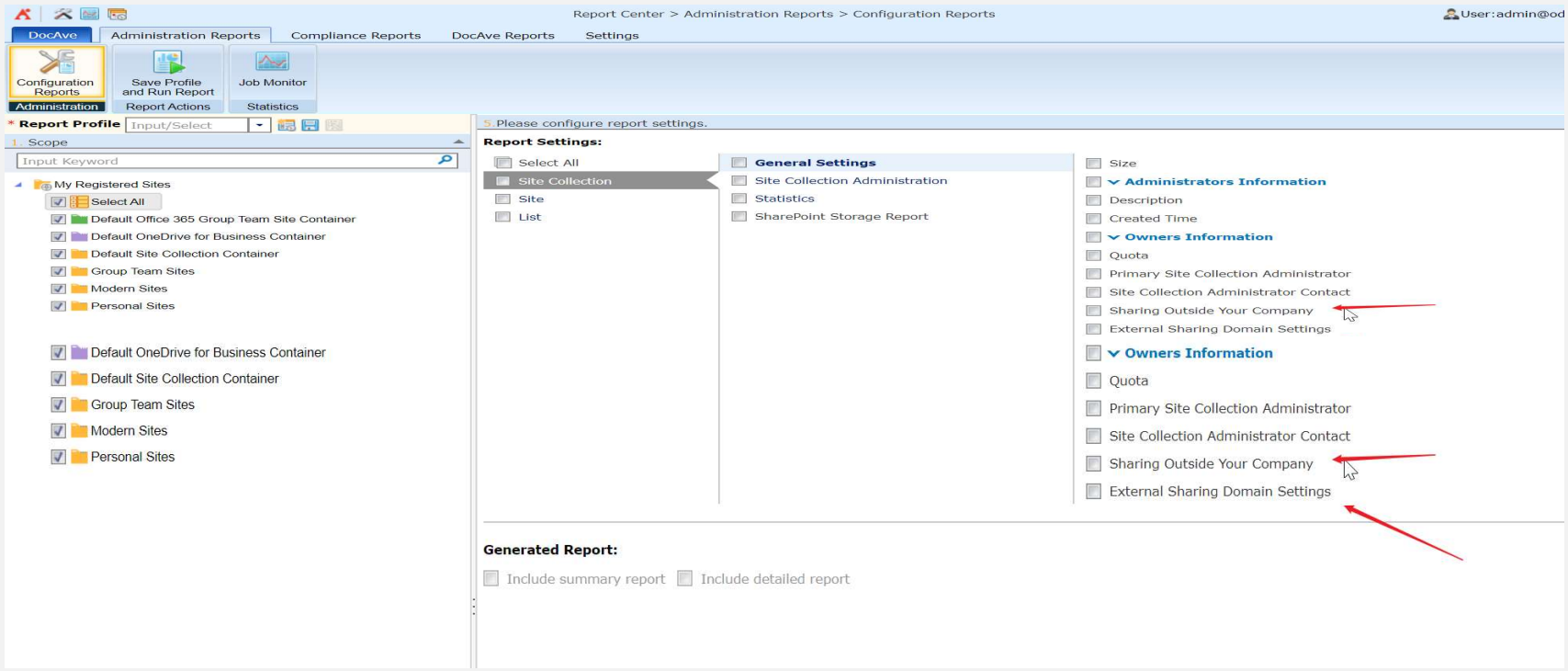


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Report on external users across SPO and ODFB with Security Search



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



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

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	متشكرم	Salamat Po	감사합니다
Cám ơn	شكريه	Terima Kasih	Dank u Wel	Děkuji
நன்றி	Köszönöm	ありがとうございます	ขอบคุณครับ	Dziękuję
谢谢	Tack	Mulţumesc	спасибо	Merci
תודה	多謝晒	дякую	Ďakujem	

AvePoint®

Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com