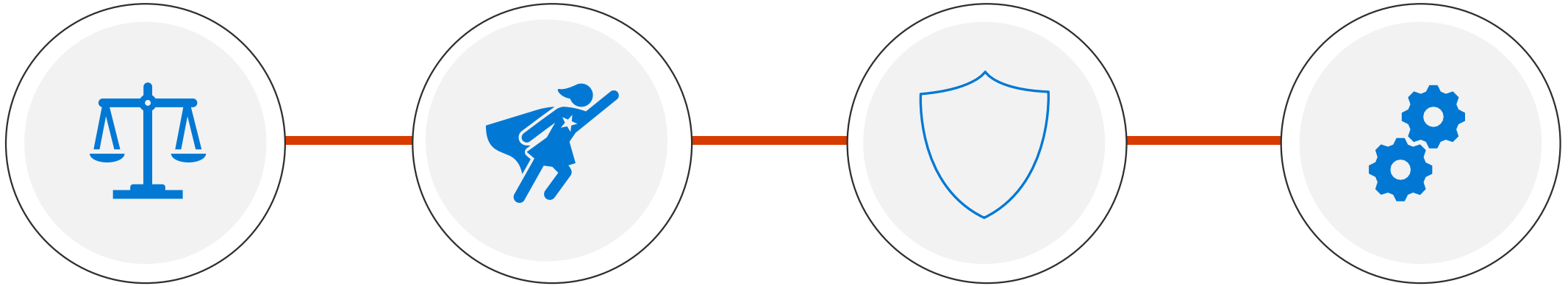
Microsoft

How Microsoft manages Microsoft 365 Groups for its employees

David Johnson
Principal Program Manager
Microsoft Core Services Engineering

Agenda



Collaboration governance

Empowering our employees

Identifying and protecting content

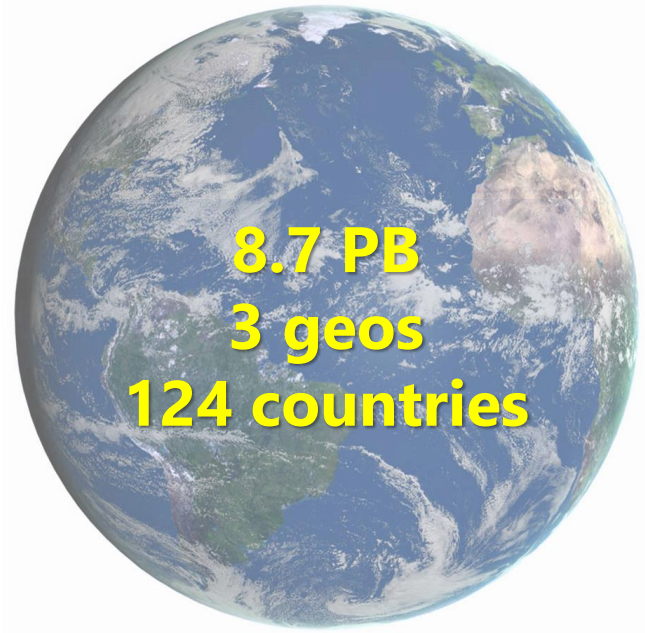
IT Solutions

Microsoft employee collaboration landscape

~250K users, 600k guests

535K sites

252K Teams



270K OneDrive for Business

17K Yammer communities

314K mailboxes

357K Microsoft 365 Groups

Seamless teamwork

Use Microsoft 365 to create productive and aligned teams, and to engage employees with leadership and the company

The fears IT orgs often have:

- Perceived chaos
- Reactive protection & compliance
- Content overexposure internally or externally
- Employees bypassing IT

Microsoft's Core Services Engineering org (our internal IT org) gets a lot of customer questions, including:

- Can anyone create a Team?
- Do we have custom forms or group provisioning?
- How do we prevent sprawl?
- How do we protect if anyone can create a group?
- How do we deal with membership rules?

This Photo by Unknown Author is licensed under CC BY-NC-ND

Enabling collaboration

The unique workstyle of every Group

Outlook

Email
and calendar

SharePoint

Intranet and
content management

Yammer

Connect across
the organization

Microsoft Teams

Hub for
teamwork

Microsoft 365 Groups

Single team membership across
apps and services

Security and compliance

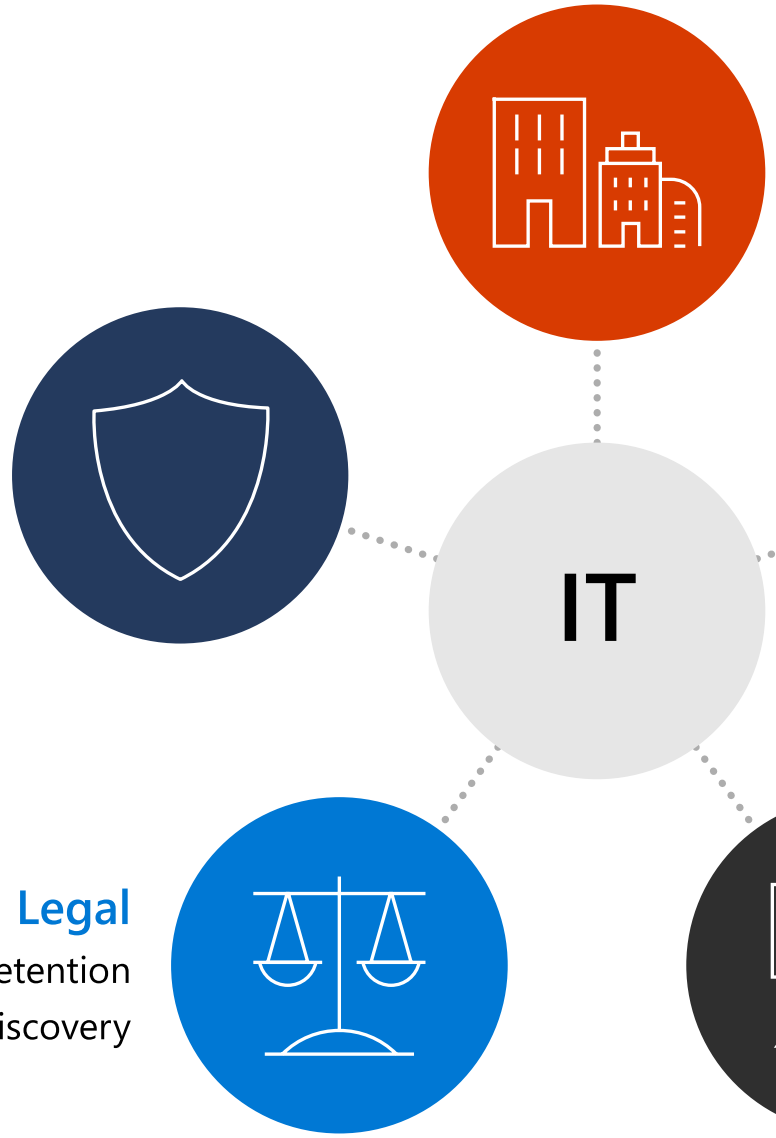
Centralized policy management

Membership service for Microsoft 365 teamwork apps

Centrally managed and governed

Extensible

Roles and their needs



Business

Accomplish business goals as simply as possible—if it's too hard, find an easier way

Limit business disruption

Employee

Get out of my way

Make it easy for me to get my work done fast

Let me share easily, but protect my secret stuff

Security officer

Prevent data leaks and breaches

Protect high value information

Legal

Comply with retention

Support eDiscovery

IT admin

Manage the increasing volume of data

Keep up with changing services and threats

Make all other roles happy

Within Microsoft, we have come a long way…

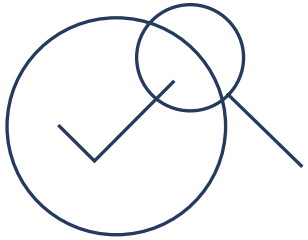
- Safe self-service creation
- Group ownership
- Container classification / sensitivity
- Reduced oversharing
- Keep collaboration on the tenant

Principles of container and content governance

Empower employees

Support self-service creation

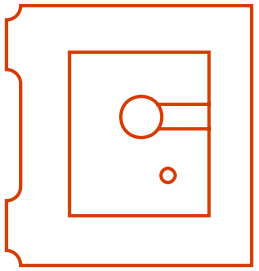
Use life-cycle management



Identify valuable content

Require classification for containers

Scan with data loss prevention (DLP)



Protect assets

Limit reach

Enforce policy

Use conditional access

Use Information Rights Management (IRM)

Ensure accountability

Manage group/site ownership

Review external membership

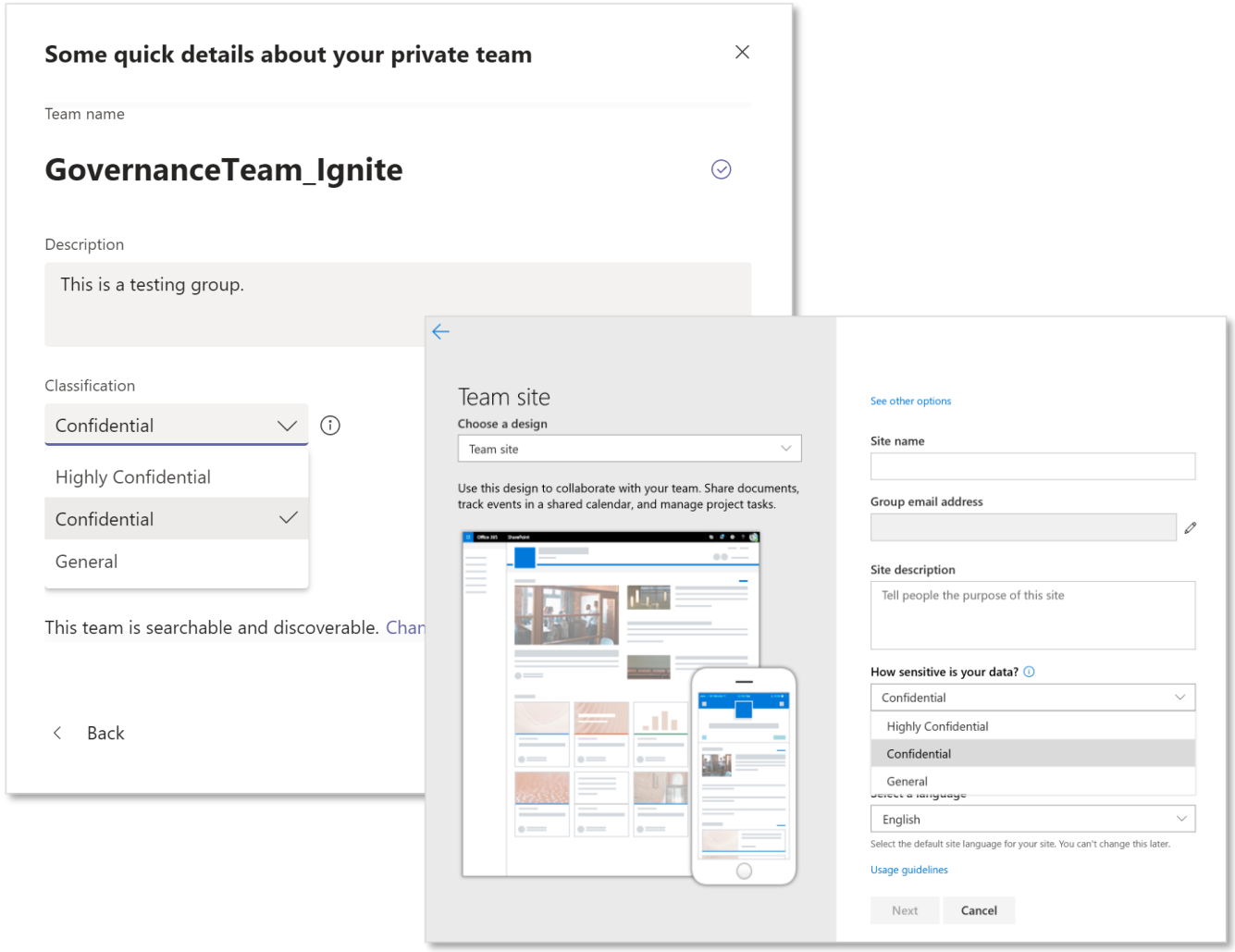
Use IT services

Enable self-service

Any Microsoft Full-time employee can create groups

Dynamic group consisting of all AAD users with extension attribute showing employment status

Employees use the in-product UI for containers creation



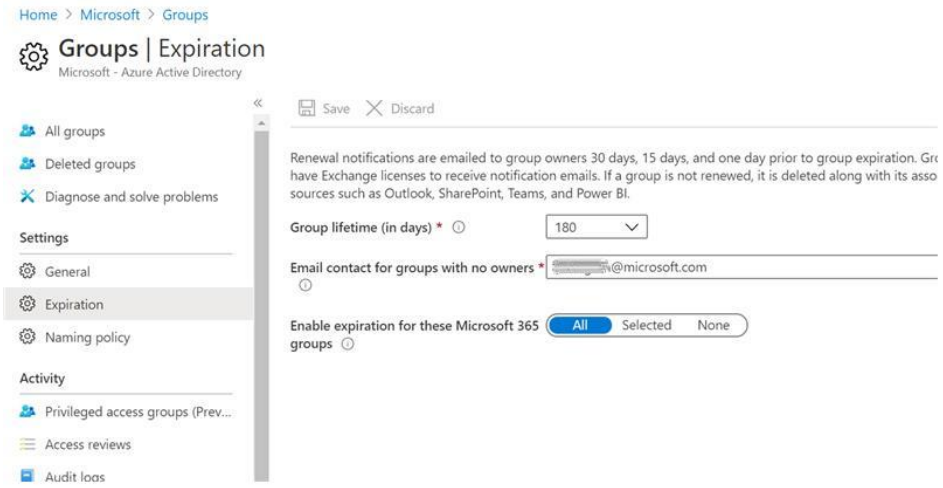
Enable in-product Lifecycle management

Microsoft enforces 180 days Lifecyle

A phased approach was adopted to deploy this policy; we started with cycles of 360 days and progressively reduced the window

What you can define when setting Expiration Policies

- Set expiration timeline
- Notification intervals are set automatically
- Set fallback email address for ownerless groups
- Apply policy to selected groups
- Groups are auto-renewed based on membership activity

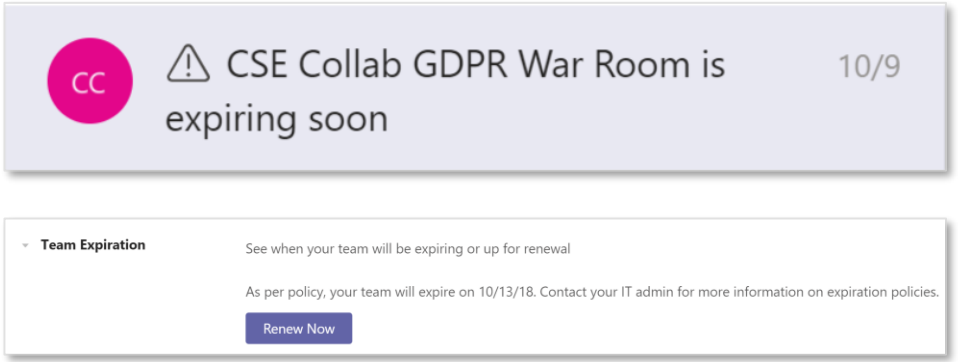


Lifecycle management

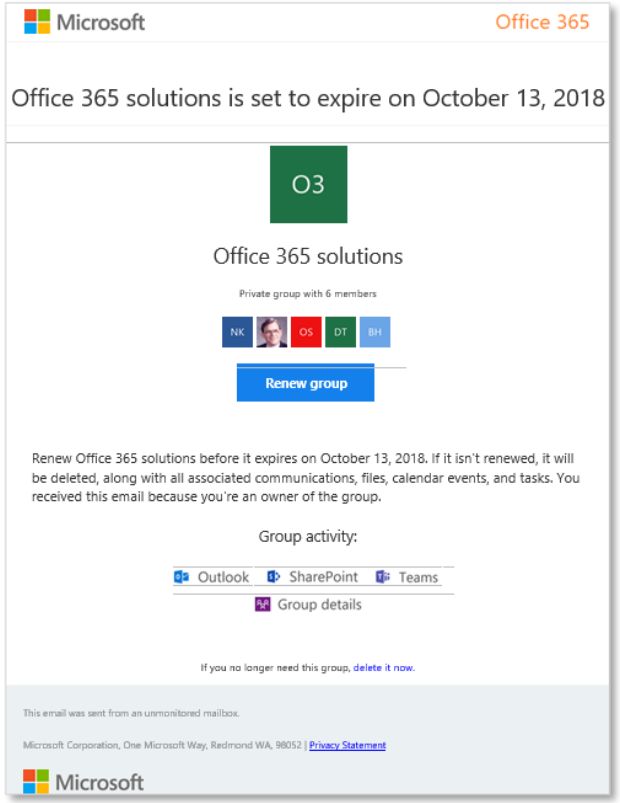
Group owner experience of expiration policy

Empower employees

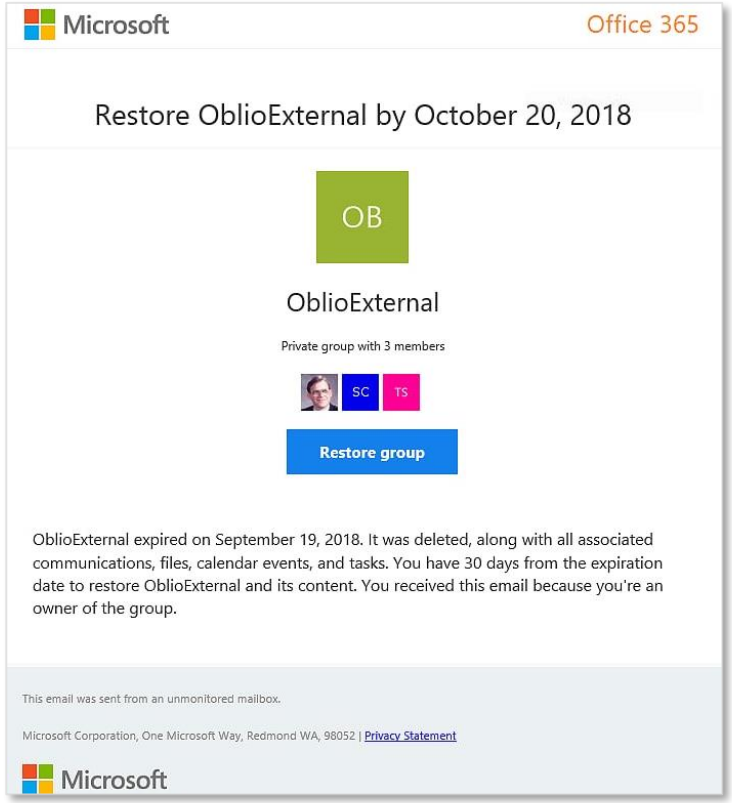
Teams renewal notice



Outlook renewal notice



Outlook restore notice



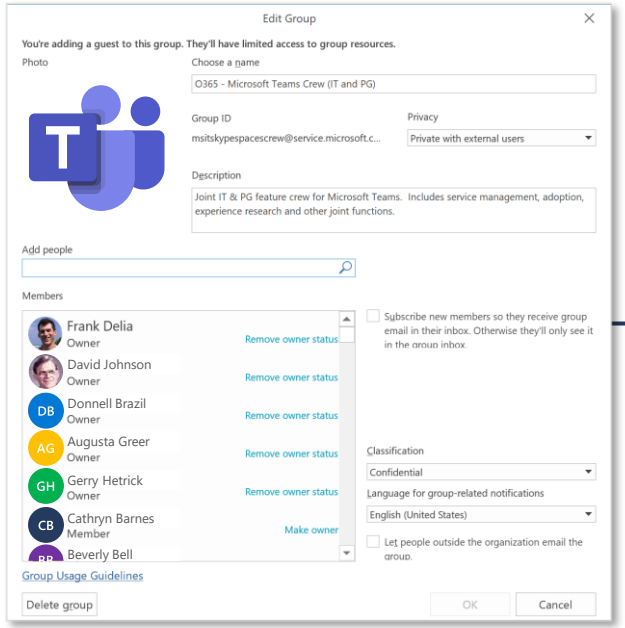
External collaboration

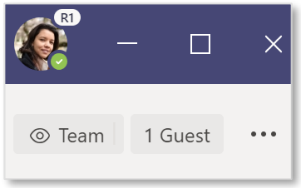
Empower employees

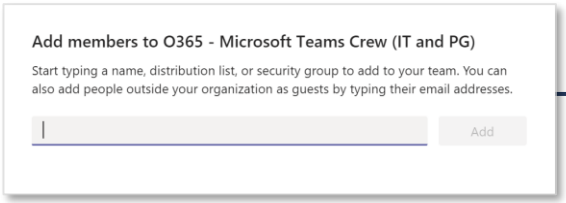
Identify valuable content

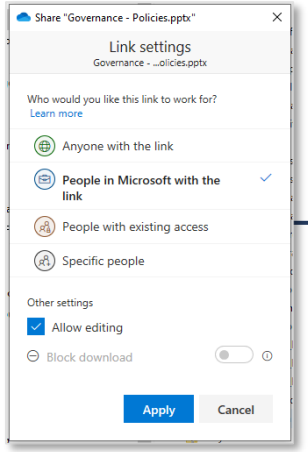
Invited member

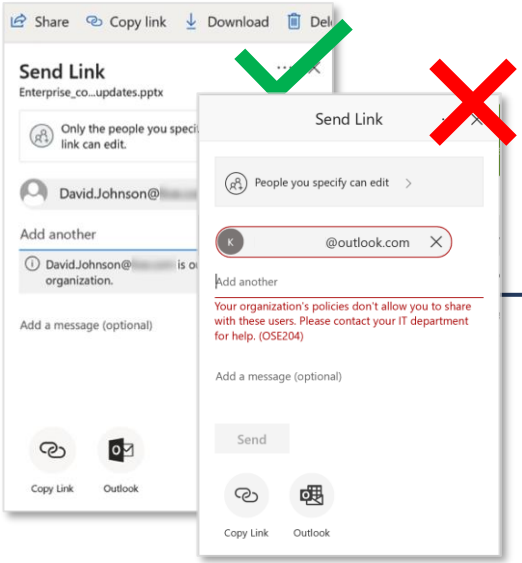
Targeted guest











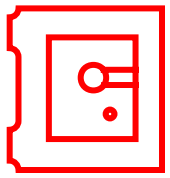
Office 365 data

SharePoint

Teams

Word

Container and file classification



Highly confidential

The most critical data for Microsoft. Share it only with named recipients.

Confidential

Crucial to achieving our goals. Limited distribution—on a need-to-know basis.

General

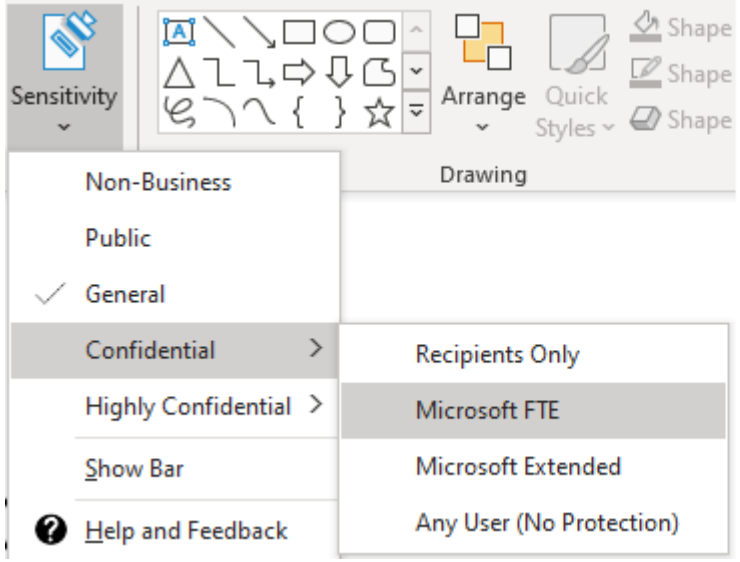
Daily work product used and shared throughout Microsoft, like personal settings and postal codes. Share it throughout Microsoft internally.

Public

Public data is unrestricted data meant for public consumption, like publicly released source code and announced financials. Share it freely.

Content classification

- Enable Sensitivity label in the file level
- Scan file with data loss prevention (DLP)
- Warn employees when classification should be different
- Employees can overwrite DLP suggestion with proper justification
- **General** is the default classification for items



Container classification

- Microsoft internally implemented AAD Classification scheme
- Consistent across all workloads
- Confidential is the default classification in the container level
- Custom policies are enforced based on classification

```
Name          : ClassificationList
Description   : A comma-delimited list of valid classification values that can be applied
                to Unified Groups.
Type          : System.String
DefaultValue  :
```

- ClassificationList
- Type: String
- Default: “”

A comma-delimited list of valid classification values that can be applied to Unified Groups.

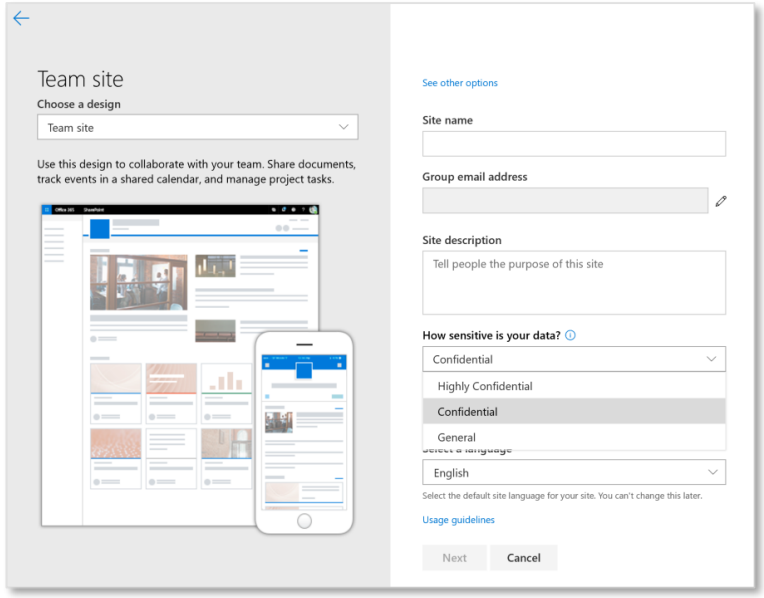
- ClassificationDescriptions
- Type: String
- Default: “”

A comma-delimited list of classification descriptions.

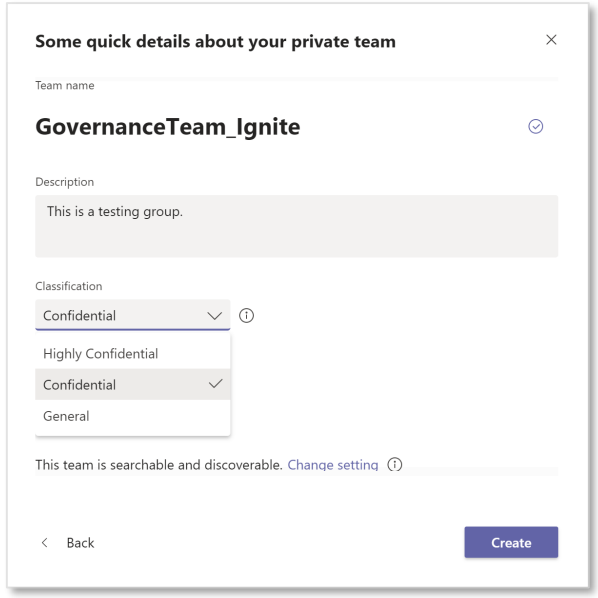
- DefaultClassification
- Type: String
- Default: “”

The classification that is to be used as the default classification for a group if none was specified.

SharePoint

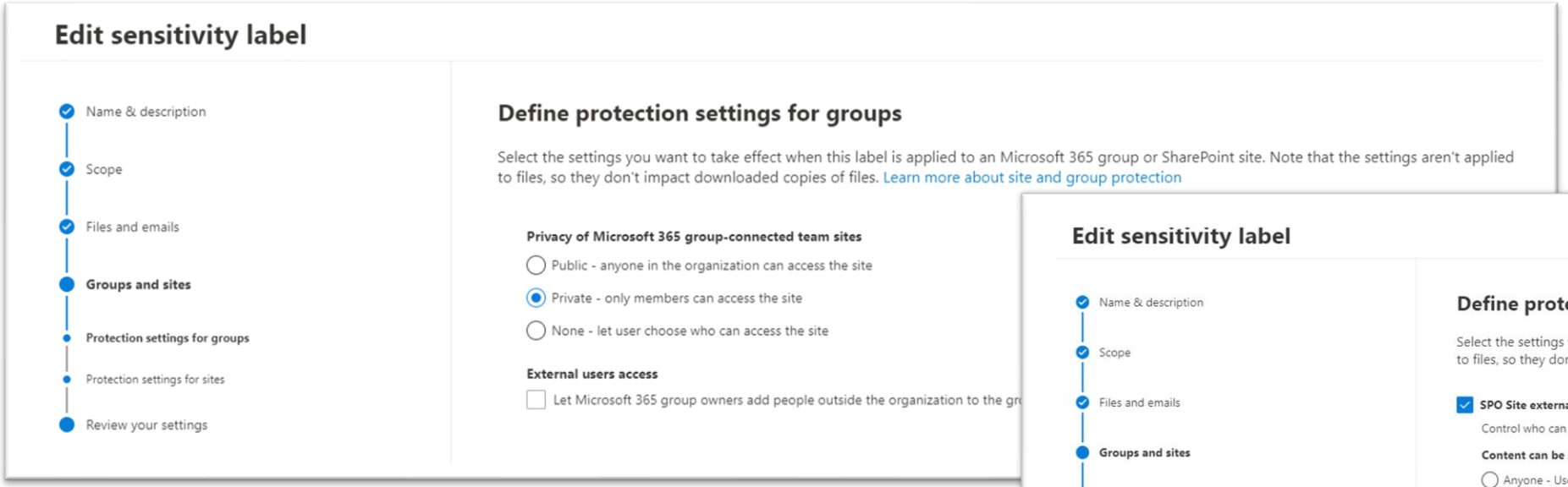


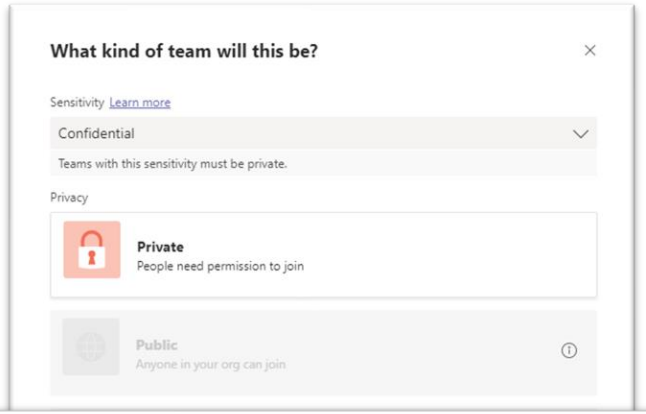
Teams

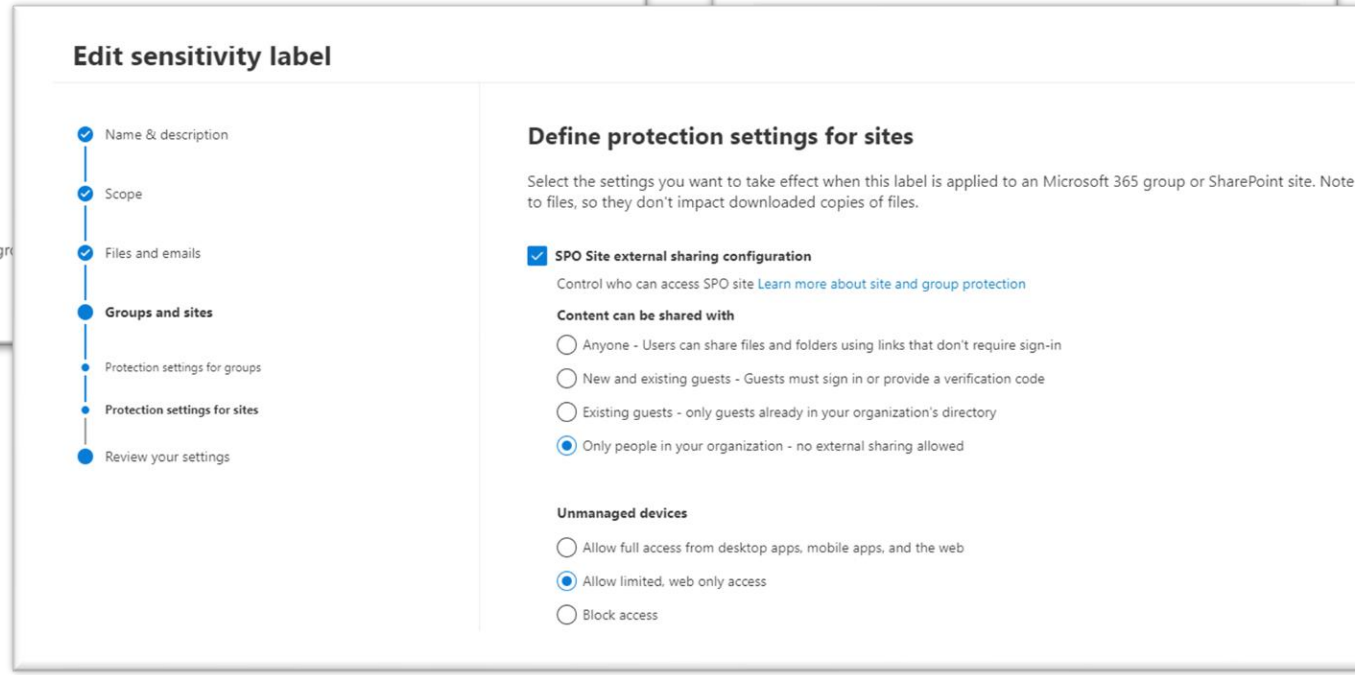


New sensitivity labels

- Unified labels across Microsoft 365
- Consistent and simple experience for users across Files, Sites, Groups, Teams
- Associate richer policies with labels







To learn more:

https://aka.ms/SC1108 - What's new in Security & Compliance in SharePoint and OneDrive

https://aka.ms/Admin1018 - Governance and management best practices for Microsoft 365 Groups

How will we structure container & item labels?

Parent Label	Child Label	Container/Item Label or Both	Scoped	External Guest Policy	Privacy Policy
General		Both	No	Allowed	Private & Public
Confidential					
	MS FTE	Item			
	Microsoft Extended and External	Container	No	Allowed	Private
	MS Extended	Both	No	Not Allowed	Private
Highly Confidential					
	MS Extended	Both	No	Not Allowed	Private
	MS FTE	Item			
	Microsoft Extended and External	Container	Yes	Allowed	Private

IT Custom Solutions

Example: Microsoft 365 Groups policies

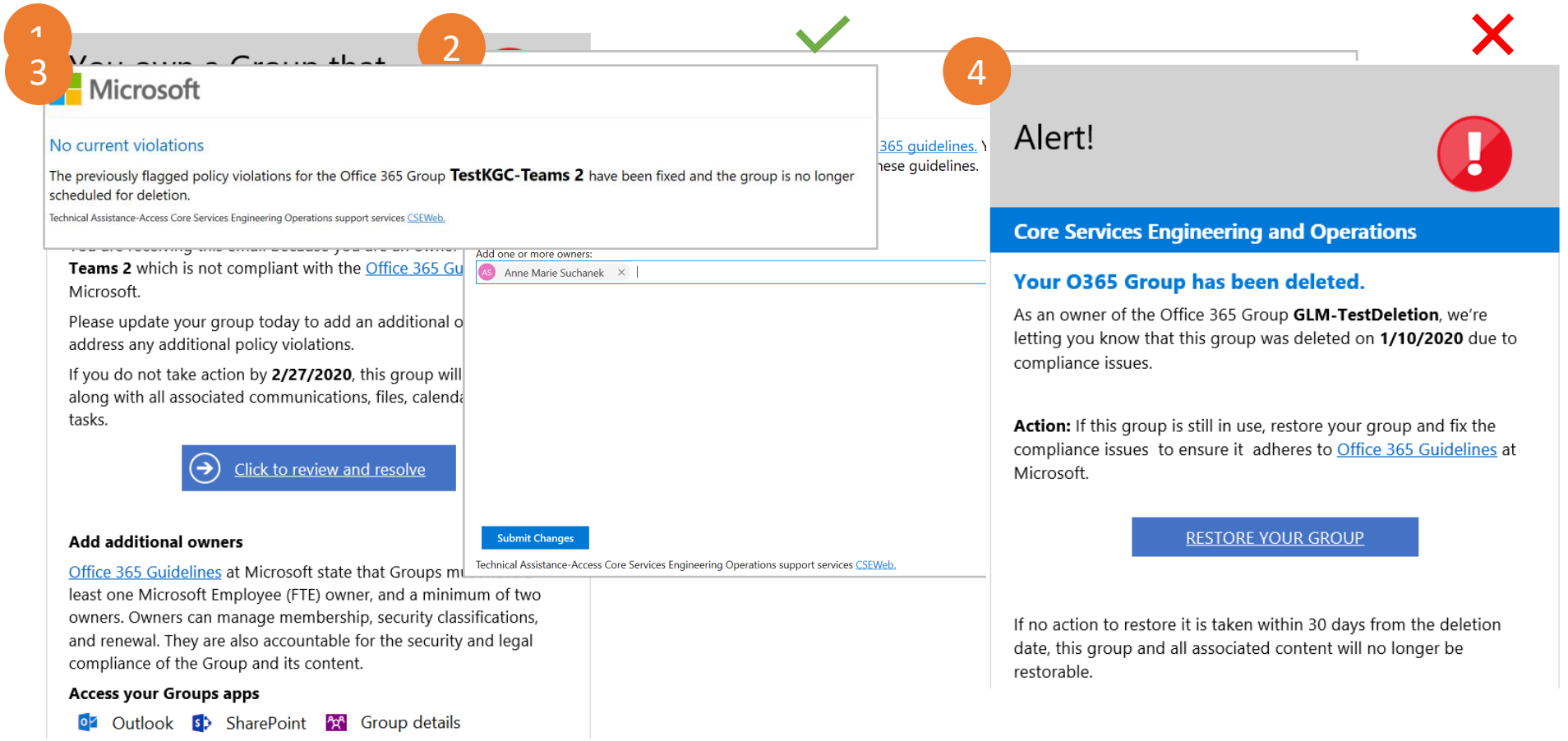
Protect assets

Ensure accountability

Within Microsoft, we require that a Group has a Full Time Employee is an owner and we have 2 owners

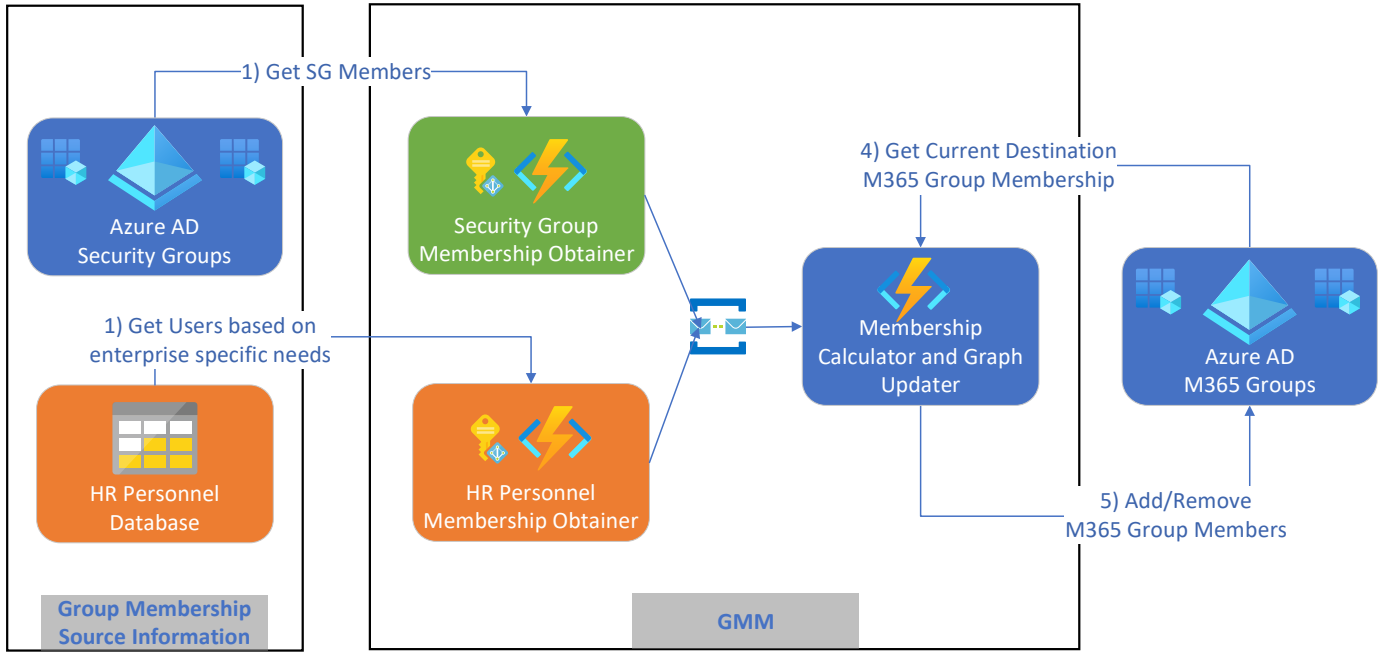
2 owners lowers risk of non-action or Groups becoming orphaned.

We scan the tenant to evaluate all Groups using Microsoft Graph APIs



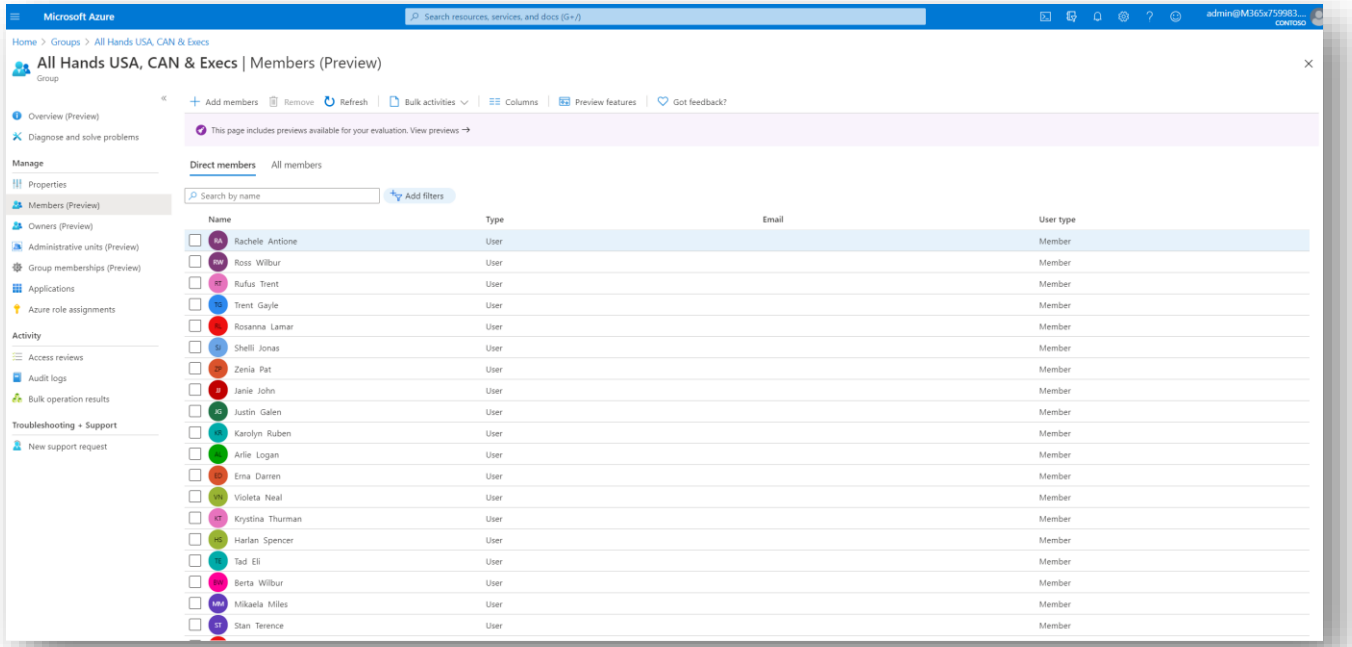
Group Membership Management

- Needed solution to Manage the Memberships of Microsoft 365 Groups
- AAD Dynamic Groups can handle some dynamic groups BUT…
- Need to create organizational groups
  - All Full Time Employees under a leader
- Need to create groups based on HR attributes
  - People with a given profession
  - People in Retail
- Security Groups (managed on prem) don't serve as membership for Microsoft Group



Group Driven Management

- Built on Microsoft Graph APIs
- Based on .Net, Azure Functions and Azure Table Storage
- Supports Azure AD based Security Groups (SGs) as members of Microsoft 365 Groups
- Membership shown as direct members in parent group
- Membership synchronized with source groups at set frequency



To learn more:

https://aka.ms/Admin1011
Making IT more efficient with improvements to Microsoft 365 Groups

https://aka.ms/Admin1013
Microsoft 365 Groups roadmap updates

Take aways

Enforce policy

Groups governance reduces customization

In product (Microsoft 365/Azure AD)

- Enable self-service site collection or group creation
- Collect classification for all containers
- User awareness: display classification
- Enforce naming rules
- Usage guideline visibility
- Life cycle: 6-month expiry
- Multi-Geo; provision based on user's region
- Membership life cycle: enforce external renewals
- Set public vs. private based on classification
- External sharing limited based on classification (HC)
- Guest membership disallowed with classification (HC)

CSEO customizations

- Ownership accountability: one full-time, two people, re-attestation
- Limit reach based on classification
- Set and validate policies and divisional policies on groups and SharePoint
- Membership management (organization-based; user attribute-based) for large or managed groups

Hear from Microsoft Core Services Engineering (CSE) experts who power the systems and services that run Microsoft

IT Showcase

How Microsoft does IT

Microsoft.com/ITShowcase

Microsoft

Related Content for Microsoft 365 Admins

	Improved IT Efficiency and Agility	
	Role-based Access Control in Microsoft 365	https://aka.ms/Admin1008
	Microsoft 365 admin mobile app: administration on-the-go with productivity with flexibility	https://aka.ms/Admin1009
	Improve IT efficiency and agility and stay informed as you enable self-service tasks	https://aka.ms/Admin1010
★	**Making IT more efficient with improvements to Microsoft 365 Groups**	**https://aka.ms/Admin1011**
	Leveraging user feedback about Microsoft 365 in your organization	https://aka.ms/Admin1015
★	**Drive external collaboration for your organization using Microsoft 365 Groups**	**https://aka.ms/Admin1007**
	Modern Cloud Management	
	How to manage Microsoft 365 in a remote work world	https://aka.ms/Admin3010
	Transform change management by syncing Message Center posts to Planner	https://aka.ms/Admin1019
	Managing updates of Microsoft 365 Apps using servicing automation	https://aka.ms/Admin1016
★	**Microsoft 365 Groups roadmap updates**	**https://aka.ms/Admin1013**
★	**Microsoft 365 Groups architecture overview and deep dive**	**https://aka.ms/Admin1017**
★	**Governance and management best practices for Microsoft 365 Groups**	**https://aka.ms/Admin1018**
	Effective controls for Microsoft 365 Apps in the Microsoft 365 admin center	https://aka.ms/Admin1120
★	**Managing work and life with Microsoft 365 Groups**	**https://aka.ms/Admin1022**
	Complex Org Investments	
	Multi-tenant management in the Microsoft 365 admin center	https://aka.ms/Admin1004
	Supporting Mergers, Acquisitions, and Divestitures in Microsoft 365	https://aka.ms/Admin1002
	Aggregated views of Service Health and Message Center for admins that manage multiple tenants	https://aka.ms/Admin1006
★	**How Microsoft manages Microsoft 365 Groups for its employees**	**https://aka.ms/Admin1003**

© Copyright Microsoft Corporation. All rights reserved.