

Managing Office 365 Groups

SharePoint Saturday Twin Cities 2018

#SPSTC





Thank you #SPSTC
sponsors!



Drew Madelung



Senior Manager – SharePoint & Office 365

Email : drew.madelung@protiviti.com

Twitter : @dmadelung

Website: drewmadelung.com



Agenda

Managing Office 365 Groups

SharePoint Saturday Twin Cities 2018

What are Office 365 Groups?

How do I work with them?

How do they work technically?

How can I administer?

What's new & What's Next?

Demos, Demos & more Demos

Office 365 Groups



SINGLE DEFINITION



SELF-SERVICE



PRIVATE*** BY DEFAULT



CONTEXT & HISTORY

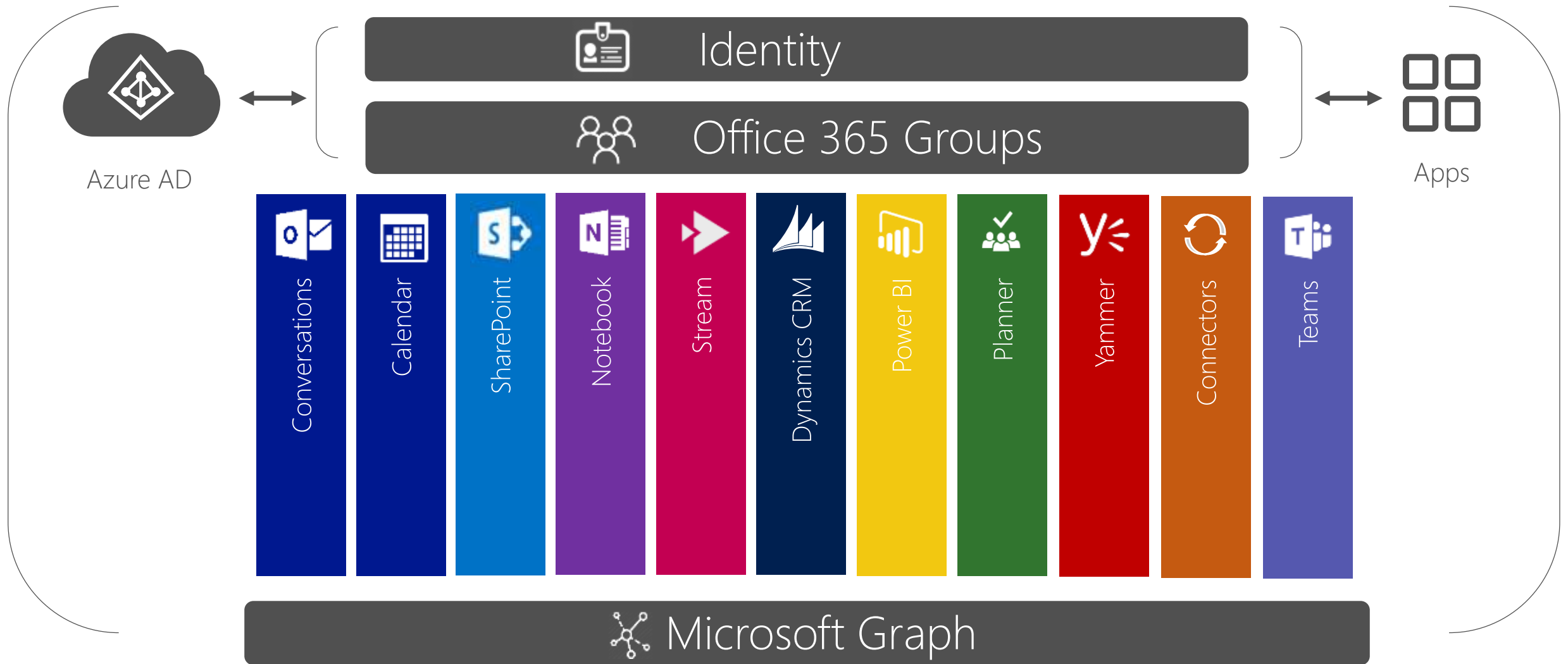


SHARING TO NON-MEMBERS



SIMPLE TO MANAGE

Office 365 Groups building blocks





Demo!

Office 365 Groups things to know

- ➔ By default, anyone can create a group and available in the Global Address List
- ➔ 100 owners and a user can't create more than 250 groups
- ➔ 500,000 tenant max
- ➔ 1000+ members are supported but will decrease performance
- ➔ Content doesn't leave when owner leaves
- ➔ Can be used as security groups in SharePoint (but not O365 Video)
- ➔ Sites under "/sites" managed path -> Not visible classic admin center
- ➔ GROUP#0 site template

What's behind the scenes



One group system across Office 365

One identity

Azure Active Directory (AAD) is the master for group identity and membership across Office 365 (Exchange, SharePoint, etc.)

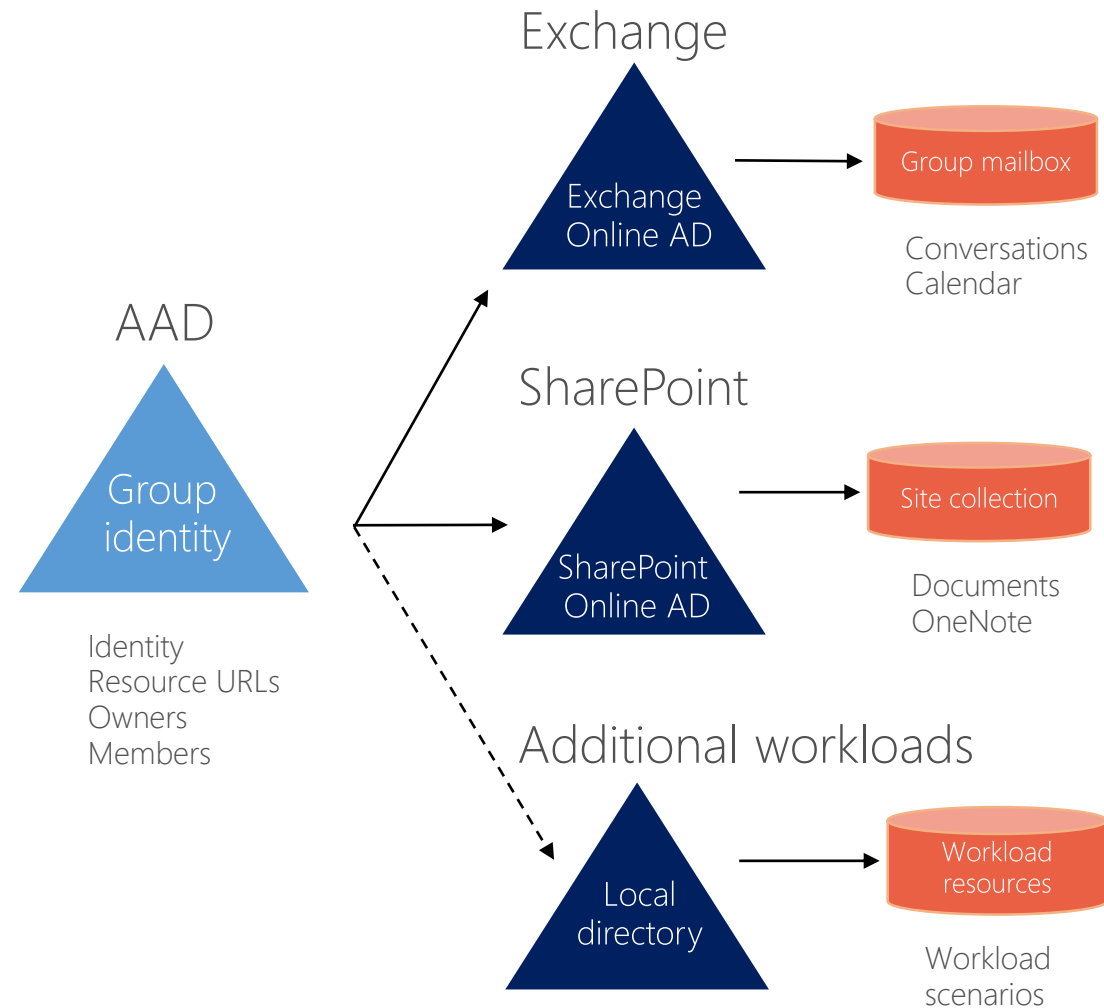
Federated resources

O365 services extend with their data (e.g., conversations stored in Exchange mailbox & documents stored in SharePoint for a group)

Loose coupling

Services notify each other of changes to a group (e.g., creation, deletion, updates)

Using sync from AAD to Exchange Online AD and SharePoint Online AD they achieve reliability if they miss notifications



Management Options – User Interface



Office 365 Admin Center



Office 365 Admin App



Azure AD Admin Portal



Exchange Admin Console



Clients – (Outlook, Planner, PowerBI, Teams, etc.)



Demo!

Management Options – Scripting

Exchange

Azure AD

Manipulating groups & membership

```
Get-UnifiedGroup  
New-UnifiedGroup  
Remove-UnifiedGroup  
Set-UnifiedGroup
```

```
Add-UnifiedGroupLinks  
Get-UnifiedGroupLinks  
Remove-UnifiedGroupLinks
```

Owners | Members | Subscribers

Manipulating governance

```
Get-AzureADMSGGroup  
Get-AzureADDirectorySetting  
Get-AzureADMSDeletedGroup  
Get-AzureADMSGGroupLifecyclePolicy
```

And a lot more...

Install-Module AzureADPreview

Establish a remote session to Exchange Online

```
$creds = Get-Credential
```

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri `
https://outlook.office365.com/powershell-liveid/ -Credential $creds -Authentication Basic -AllowRedirection  
Import-PSSession $Session
```

Useful Scripts for Groups to Get Started

Create group

```
New-UnifiedGroup -DisplayName "Legal" -Alias "Legal" -EmailAddresses legal@domain.com
```

Rename group

```
Set-UnifiedGroup -Identity "Legal" -Alias "Legal" -DisplayName "New Legal" -PrimarySmtpAddress legal@domain.com
```

View all subscribers, members or owners for a group

```
Get-UnifiedGroupLinks -Identity "Legal" -LinkType Subscribers
```

Show detailed info for all groups

```
Get-UnifiedGroup |  
  select Id, Alias, AccessType, Language, Notes, PrimarySmtpAddress, `  
  HiddenFromAddressListsEnabled, WhenCreated, WhenChanged, `  
  @{Expression=([array](Get-UnifiedGroupLinks -Identity $_.Id -LinkType Members)).Count }; `  
  Label='Members'}, `  
  @{Expression=([array](Get-UnifiedGroupLinks -Identity $_.Id -LinkType Owners)).Count }; `  
  Label='Owners'} |  
  Format-Table Alias, Members, Owners
```


Things we can do

Creation permissions

Usage guidelines

Classification

Guest access

Allow/Block guest domains

Naming policy

Expiration policy

Access reviews

Dynamic membership

Soft delete and restore

Managing Group Creation

The old way but still can be used for OWA and Outlook 2016

Use an OWA Mailbox Policy to disable group creation for ALL users or a SUBSET of users

- This does NOT disable group creation EXCEPT when trying to create through Outlook/Exchange
 - Creating groups in other clients/admin areas (PowerBI, Planner, etc...) would NOT disable

```
Set-OwaMailboxPolicy -Identity test.com\OwaMailboxPolicy-Default -GroupCreationEnabled $false
```

Managing Group Creation through Azure AD

The new way uses Azure AD

- No longer dependency on Exchange – All O365 apps
- If OWA policy exists and AAD policy is enabled, OWA policy will be ignored
- Admins bypass
 1. Disable creation for everyone
 2. AAD group for whom can create
 - Can be O365 Group or Distribution Group)
 - Individual users only
- Prerequisites
 - Azure AD Version 2.0.0.98 or later (V2)
 - Azure AD Version 1.1.117.0 or later (V1) - deprecation

Managing Group Creation through Azure AD

Steps to setup

1. Retrieve the Object ID for the group that contains the authorized users
 - Use Azure AD portal to get Object ID
 - Get-AzureADGroup cmdlet to discover GUID via PowerShell
2. Use PowerShell to update the Azure AD policy
 - Pass the GUID of your authorized user group to *GroupCreationAllowedGroupId*

Connect-AzureAD

```
$template = Get-AzureADDirectorySettingTemplate | where-object {$_.displayname -eq "Group.Unified"}  
$setting = $template.CreateDirectorySetting()  
$setting["EnableGroupCreation"] = "false"  
$setting["GroupCreationAllowedGroupId"] = <groupId>
```

```
New-AzureADDirectorySetting -DirectorySetting $setting
```

3. Confirm using PowerShell and test creating a group

```
Get-AzureADDirectorySetting | ForEach Values
```

Group Usage Guidelines

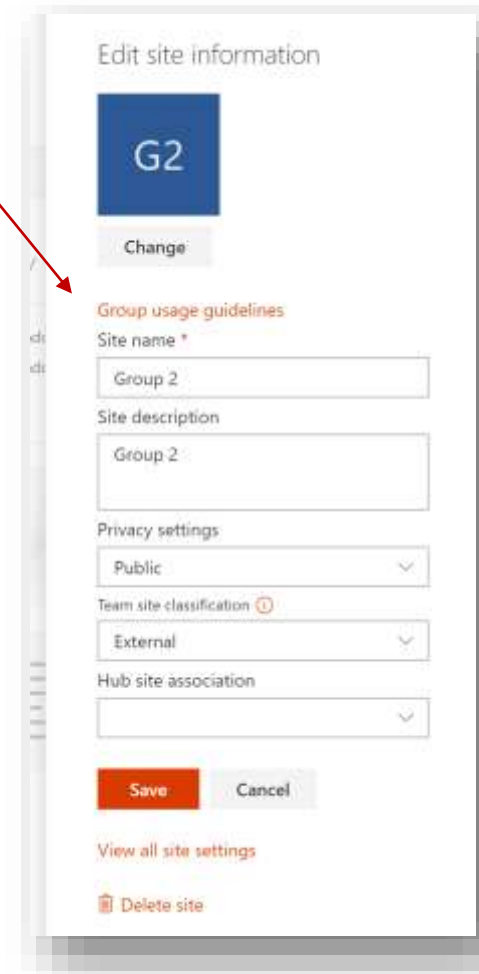
Create a link to Groups documentation available when editing and creating

Not on by default

Only set via PowerShell

Use PowerShell to update the Azure AD policy (if settings object exists)

```
$setting = Get-AzureADDirectorySetting | where-object {$_.displayname -eq "Group.Unified"}  
$setting["UsageGuidelinesUrl"] = "https://domain.sharepoint.com/Pages/U-Guide.aspx"  
Set-AzureADDirectorySetting -Id $setting.Id -Directorysetting $setting
```



Edit site information

G2

Change

Group usage guidelines

Site name *

Group 2

Site description

Group 2

Privacy settings

Public

Team site classification

External

Hub site association

Save Cancel

View all site settings

Delete site

Group Classifications

Create classifications that the users can set per Group

Not on by default

Doesn't actually do anything (yet!)

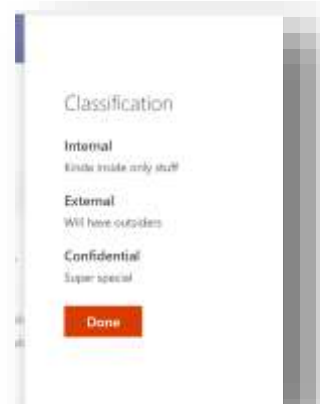
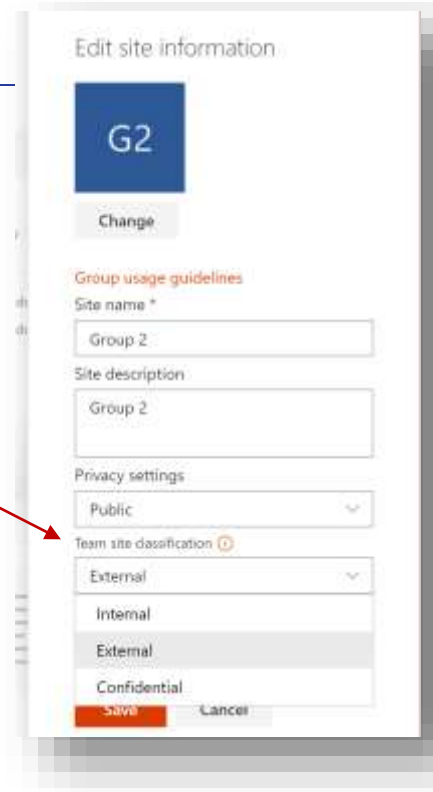
Choices only set via PowerShell

1 set of classifications per tenant

Default value & descriptions available

Use PowerShell to update the Azure AD policy (if settings object exists)

```
$setting = Get-AzureADDirectorySetting | where-object {$_.displayname -eq "Group.Unified"}
$setting["ClassificationList"] = "Internal,External,Confidential"
$settings["ClassificationDescriptions"] = "Internal:xx,External:xx,Confidential:xx"
$settings["DefaultClassification"] = "Internal"
Set-AzureADDirectorySetting -Id $setting.Id -Directorysetting $setting
```





Demo!

Group Guest Access

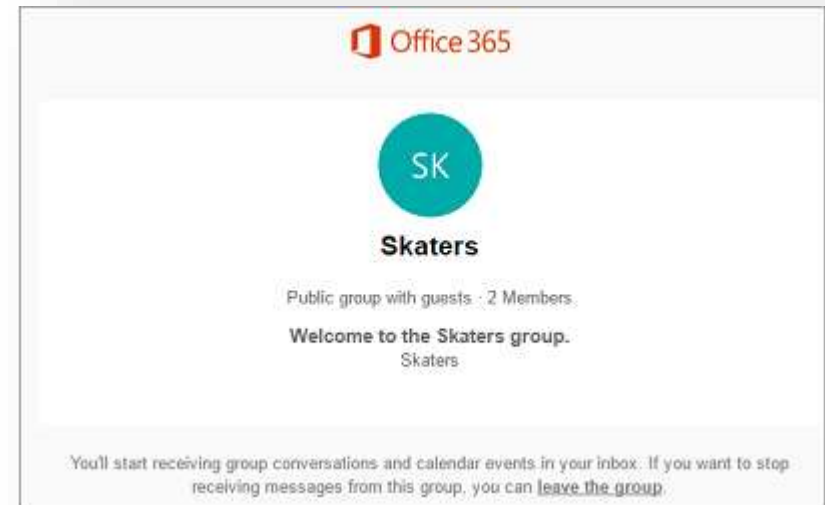
- Does not comply with SPO blacklist/whitelist
- Enabled by default
- Overall Group guest access is managed at the tenant level
- Guests cannot view IRM protected files
- Guests need to access via browser
- Guests cannot:
 - Be an owner
 - View the GAL
 - View Group members or contact cards
 - Be blocked by specific user

Feature	Guest user allowed?
Create a group	No
Add/remove group members	No
Delete a group	No
Join a group	Yes, by invitation
Start a conversation	Yes
Reply to a conversation	Yes
Search for a conversation	Yes
@mention a person in the group	No
Pin/Favorite a group	No
Delete a conversation	Yes
"Like" messages	No
Manage meetings	No
View group calendar	No
Modify calendar events	No
Add a group calendar to a personal calendar	No
View and edit group files	Yes, if enabled by tenant admin
Access the group OneNote notebook	Yes, via link from group member
Browse groups	No

Group Guest Access

Group owners can invite external people to be guest users

Group members can request an invitation for an external person



Group Guest Access Admin Controls

Guest addition to organization

- Allow invitation to guests users in the organization

Office 365 Portal – Settings & Privacy > Sharing

Guest addition to groups

- Allow adding of guests to any group within the organization.

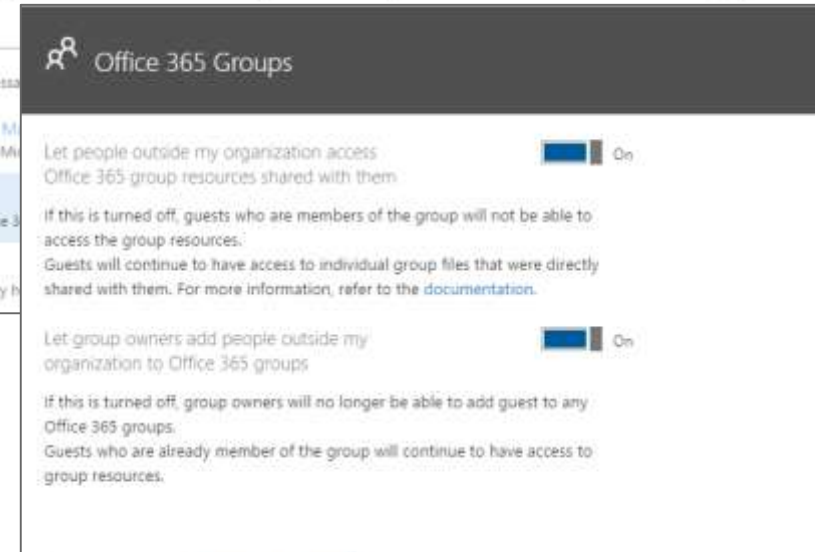
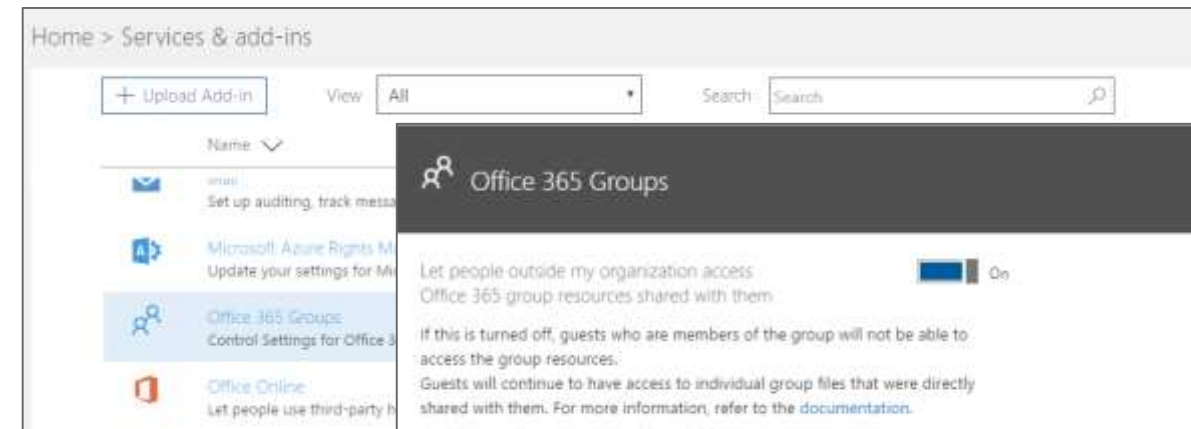
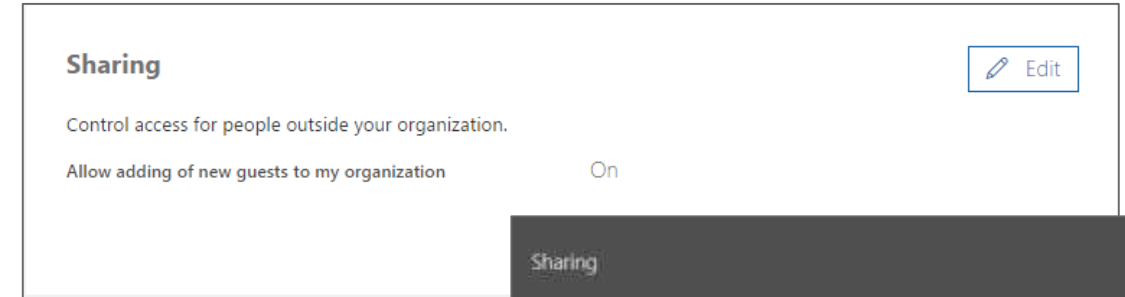
Office 365 Portal – Services & Add-Ins > Office 365 groups

Allow adding of guests to a specific group in the organization (only available in Power Shell)

Guest access to group resources

- Allow guests to access to any Office 365 group resources

Office 365 Portal – Services & Add-Ins > Office 365 groups



Group Guest Access Powershell

Steps to block for tenant

1. Ensure that sharing is allowed in the SharePoint Admin Center / O365 Admin Center
2. Use PowerShell to update the Azure AD policy (if settings object exists)

```
$setting = Get-AzureADDirectorySetting | where-object {$_.displayname -eq "Group.Unified"}  
$setting["AllowToAddGuests"] = "False"  
$setting["AllowGuestsToAccessGroups"] = "True"  
Set-AzureADDirectorySetting -Id $setting.Id -Directorysetting $setting
```

3. Set **AllowGuestsToAccessGroups** to *False* to instantly disable all external users from accessing groups

Can be controlled per group

1. [Through PowerShell](#)

Group Guest Domain Allow/Block

Allow or block guest users by domain

Can only create an allow or block list, not both

1 policy per org

Works separately than SPO allow/block

Doesn't apply to already added group members

1. Azure AD Portal
2. PowerShell - *Set-GuestAllowBlockDomainPolicy.ps1*
 - file: [MS Download Center](#)
 - *-MigrateFromSharePoint*

Home > Madelung Inc. - User settings > External collaboration settings

External collaboration settings

Save Discard

Guest users permissions are limited ⓘ

Yes No

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

Collaboration restrictions

☐ Allow invitations to be sent to any domain (most inclusive)

☒ Deny invitations to the specified domains

☐ Allow invitations only to the specified domains (most restrictive)

Delete

TARGET DOMAINS

gmail.com

example.com or *example.com or example*

Group Naming Policy

Ensure group names follow your standard

Currently in preview

Applies to group name and group alias

Total prefixes and suffixes string length restricted to 53 characters

Total group name length 264 characters

1. Prefix-suffix naming policy

- Can be fixed strings or user attributes

Example:

- Policy = "GRP [GroupName] [Department]"
- User's department = Engineering
- Created group name = "GRP My Group Engineering"

Supported Azure AD attributes:

[Department]

[Company]

[Office]

[StateOrProvince]

[CountryOrRegion]

[Title]

[CountryCode]

Group Naming Policy

2. Custom blocked words

- Upload comma separated list of blocked words
- Done after appending the prefix and suffix
- No sub-string searches occur
- Case-insensitive
- No character restrictions in the blocked words
- No upper limit to number of words that can be set
- Admin roles exempted (Global admin, Partner support, User acct admin, Directory writers)
 - *Example: "CEO, Payroll, HR"*

Use PowerShell to update the Azure AD policy (if settings object exists)

```
$setting = Get-AzureADDirectorySetting | where-object {$_.displayname -eq "Group.Unified"}  
$setting["PrefixSuffixNamingRequirement"] = "Grp_[Department]_[GroupName]_[Country]"  
$setting["CustomBlockedWordsList"] = "Payroll,CEO,HR"  
Set-AzureADDirectorySetting -Id $setting.Id -Directorysetting $setting
```

Group Expiration Policy

Expiration policies can help remove inactive groups

Off by default

Administrators can specify expiration period

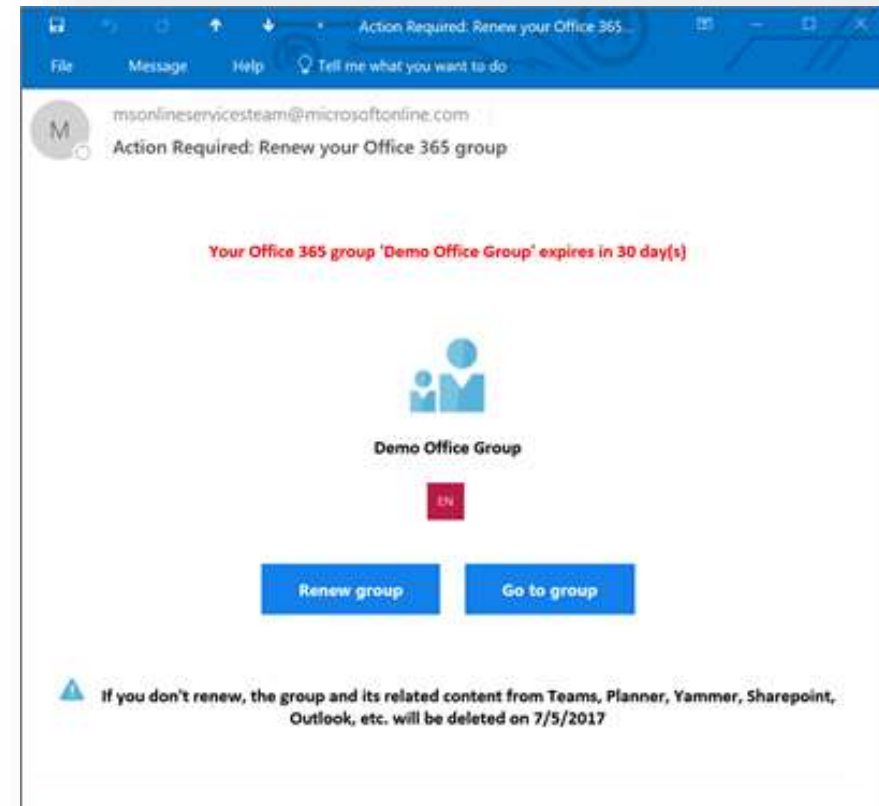
If a Group is not renewed it will be "soft-deleted"

renewedDateTime property holds the last renewal/creation time

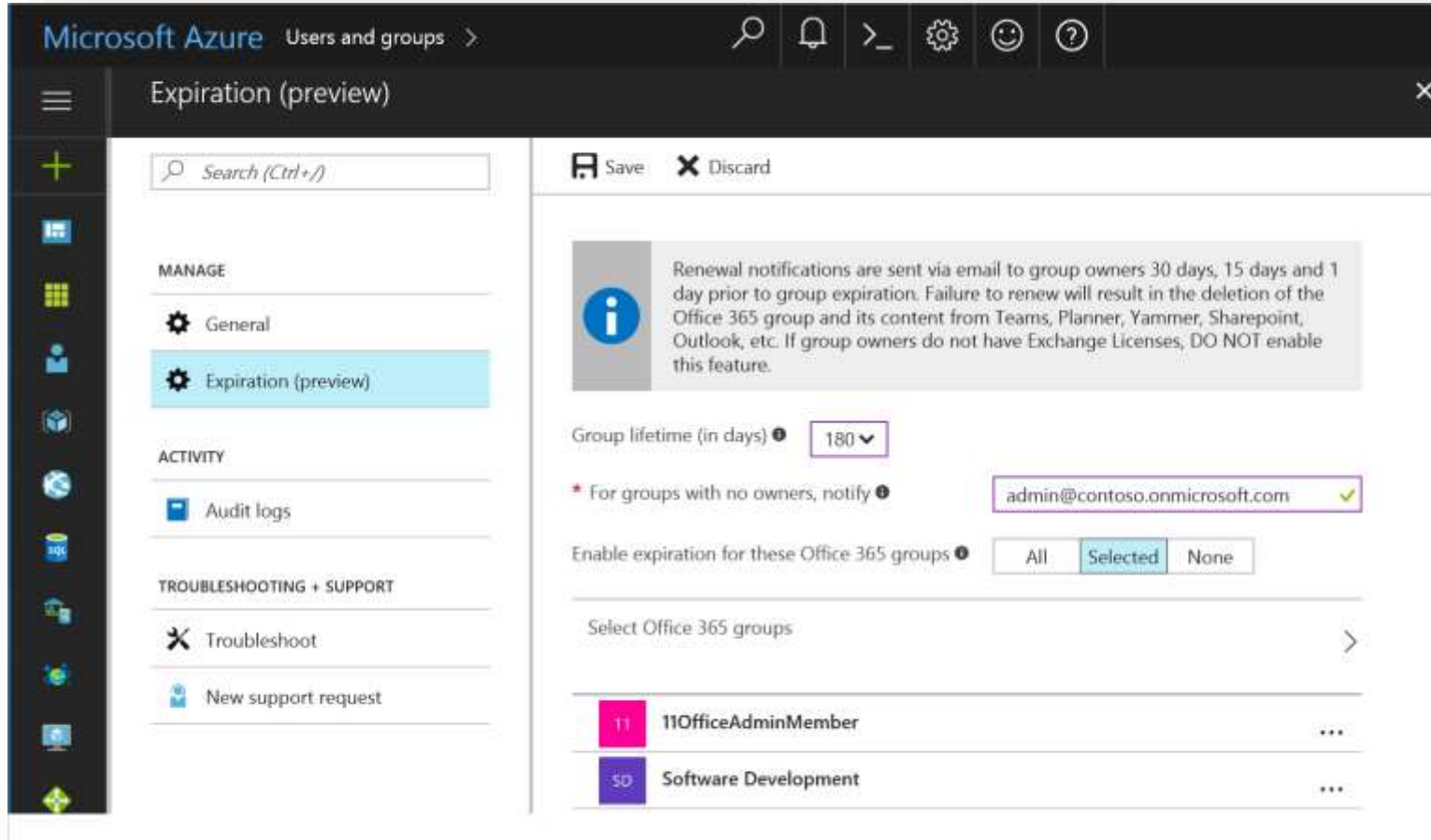
Groups older than expiration will be notified not just removed

Group owners sent email before expiration

- 30, 15, & 1 day prior



Group Expiration Policy



Powershell

View your policy

[Get-AzureADMSGroupLifecyclePolicy](#)

Create a new policy

[New-AzureADMSGroupLifecyclePolicy](#)

Update a policy

[Set-AzureADMSGroupLifecyclePolicy](#)

Add a Group to a policy

[Add-AzureADMSLifecyclePolicyGroup](#)

Azure AD Access Reviews

Ask users to attest users' access

Review just guests or users

Can be set on occurrence

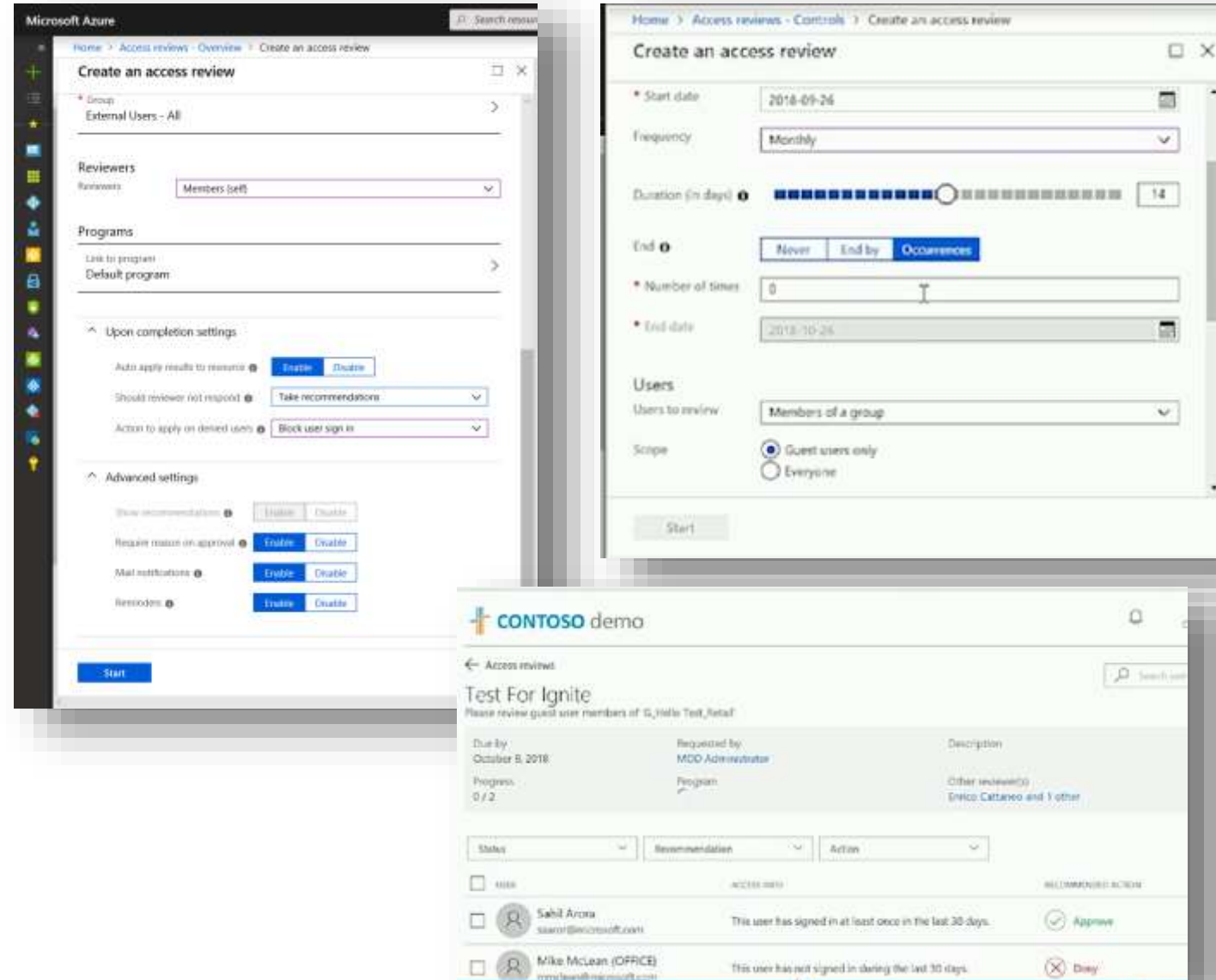
- Weekly, Monthly, Quarterly, Annually

Reviewers can be owners or others

Completion

- If reviewer not responded
- Actions to apply on denied users
 - Delete from AAD
 - Block sign-in

Requires AD P2



Dynamic membership

Membership generated by query

Example: All users in HR

Update membership through query

Basic or advanced queries

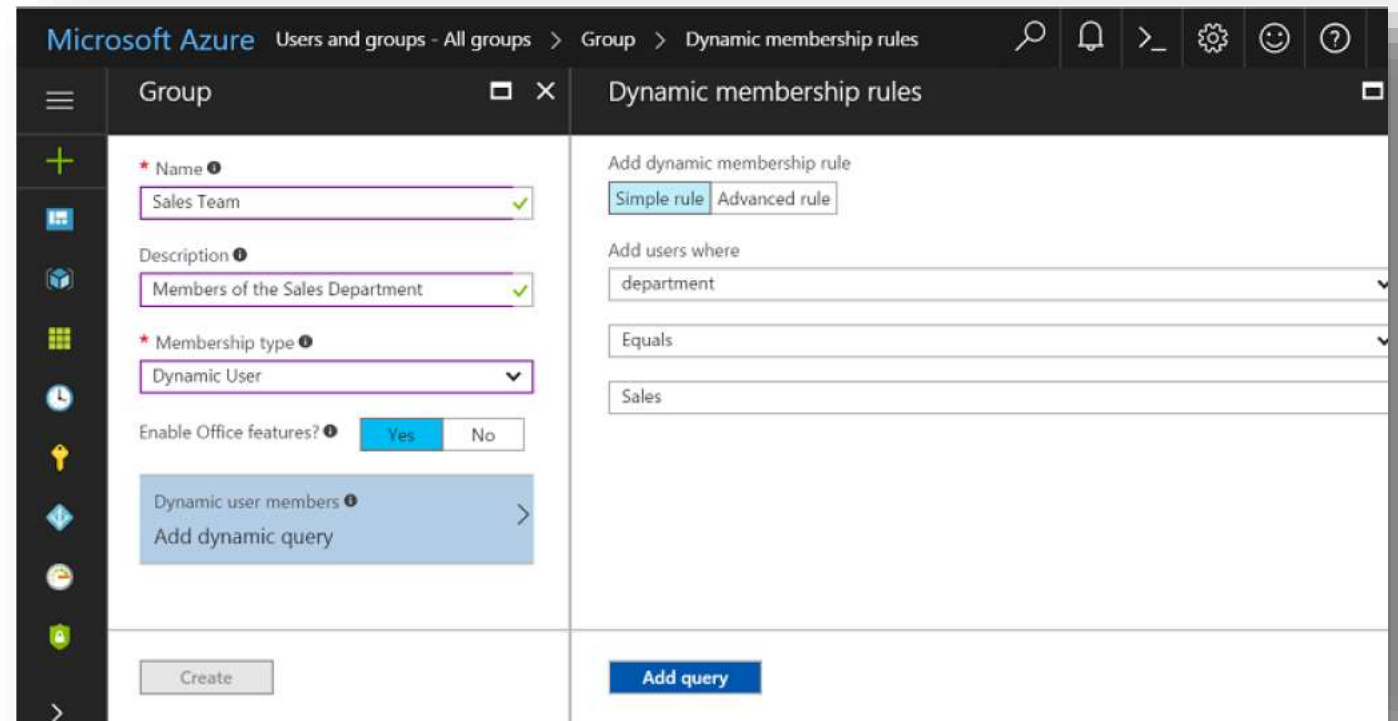
Owners not included in query by default

Users not notified if removed

Planner does not work

Or...

- [Use security groups to drive membership](#)



Pic from O365 for IT Pro book

Restore a deleted Group

Deleted Groups retained for 30 days

If deleted through **Remove-MsolGroup** it is not recoverable

1. Display all soft-deleted Groups and get object ID of deleted Group

Get-AzureADMSDeletedGroup

2. Restore the Group

- Pass the GUID of your Group you got above

Restore-AzureADMSDeletedDirectoryObject -Id <objectId>

Permanently delete the Group via

Remove-AzureADMSDeletedDirectoryObject -Id <objectId>

Can be restored through Exchange Admin Center

Suppressing the Group welcome message

When a user is added a Group they will get a welcome email by default

- What if you want to mass add people and not let them know?

The *UnifiedGroupWelcomeMessageEnabled* switch specifies whether to enable or disable sending system-generated welcome messages to users who are added as members to the Office 365 Group.

- \$true by default

```
Set-UnifiedGroup -Identity "Legal" -UnifiedGroupWelcomeMessageEnabled:$false
```

Hiding from the Global Address List (GAL)

When a group is created it is automatically viewable in the GAL

- What if you don't want people to see it?

The *HiddenFromAddressListsEnabled* specifies whether the Office 365 Group appears in the global address list (GAL) and other address lists in your organization.

- \$true
 - Hidden from the GAL and other address lists.
 - Can still receive messages,
 - Can't see in Outlook or discover option
- \$false
 - Visible in the GAL - default

```
Set-UnifiedGroup -Identity "Legal" -HiddenFromAddressListsEnabled:$true
```



Demo!

What about governance?



Reporting

Activity Reports

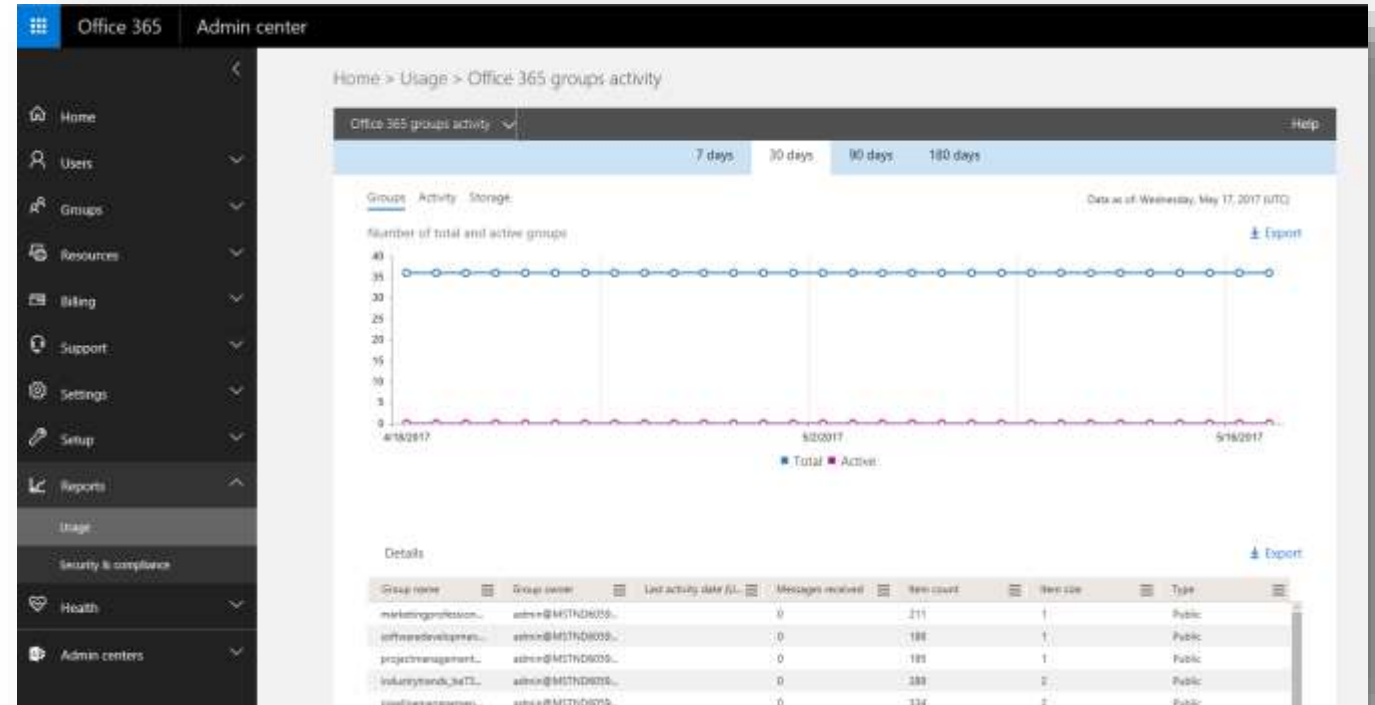
Monitor regularly

Leverage Power BI content packs for insights:

- [Office 365 Adoption content pack](#)
- [Azure AD content pack](#)

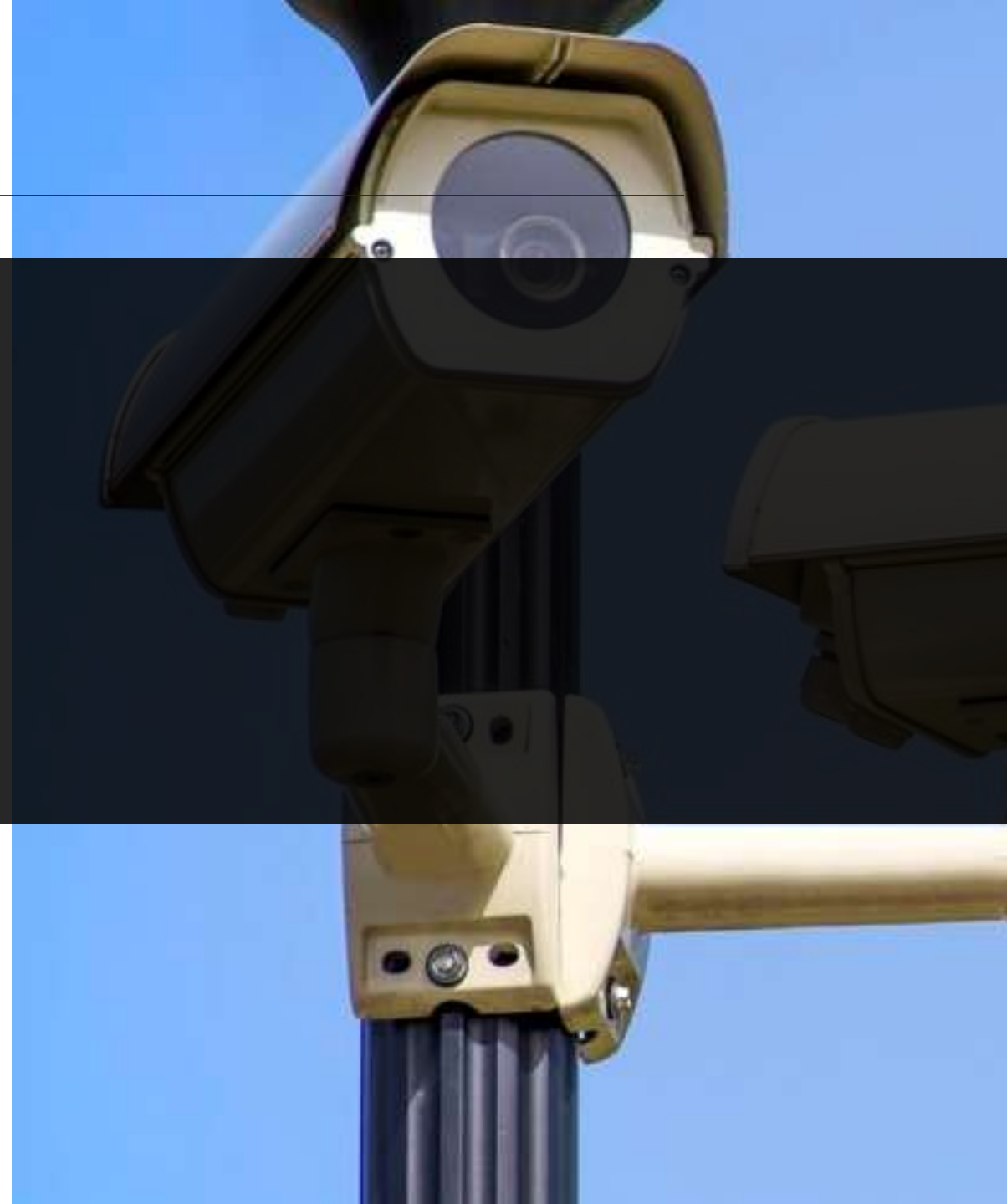
PowerShell cmdlet:

- [Office 365 Groups Report \(Unified Groups\)](#)



Security and Compliance

- ➔ eDiscovery
- ➔ Data loss prevention
- ➔ Retention
- ➔ Audit log and Content search
- ➔ Labels



How are organizations managing groups successfully?



OPEN

- Everyone can create groups (default).
- Using all teamwork apps to meet their diverse needs.
- Consistent classification and policy enforcement.



CONTROLLED

- Creation is limited to certain business units/users.
- Progressively expand self-service during O365 apps onboarding.
- Guide users to collaboration choices.



COMMON

Processes in place

Reporting & monitoring

Change management

How does Microsoft IT manage groups?

Empower employees while protecting content, keeping compliant and holding employees accountable

Self-service group creation and life-cycle

Creation tied to Dynamic Group of all full-time employees; non-employees can't create groups

No naming prefix/suffix but blocked words

180-day group life-cycle; groups must be renewed or will be deleted (unless under retention) (expiry policy)

Usage guidelines shown with plain language; e.g. "Be polite & inclusive"

Custom job emails group members for groups with no owner

Classification, protection & compliance

Classification configured in Azure AD; **Highly Confidential**, **Confidential** (default), **General**

Custom jobs set Privacy to Private and disable external membership/sharing based on classification

Group site provisioned in region tied to user's Preferred Data Location (multi-geo)

Membership reviews for groups with external members (access reviews)

Divisional groups created in SharePoint have retention configured with site template

Custom jobs to enforce ownership policy (2 owners with at least 1 full time employee)

Management tidbits

- Discuss a governance plan for groups
- Figure out if you need group creation policies
- Monitor SharePoint Online Storage to ensure group sites not overtaking total storage
- Establish a process to have groups admin support easily available for users
- Run reports to try to track groups sprawl
- Use *UsageGuidelinesUrl* and *ClassificationList*
- Migrate multiple distribution lists to Office 365 groups – [Link](#) – (also via GUI)

Edit site information

G2

Change

Group usage guidelines

Site name *

Group 2

Site description

Group 2

Privacy settings

Public

Team site classification ⓘ

External

Internal

External

Confidential

Save Cancel

Description	AAD: O365	AAD: P1	License req.
Create, read, update, delete	Yes	Yes	None – Free Feature
Soft-delete and restore	Yes	Yes	None - Free feature
Tenant-wide self-service group creation controls	Yes	Yes	None - Free feature
Dynamic group membership		Yes	Each user that is also a member of a group within tenant.
Granular self-service group creation controls		Yes	Each user that is also a member of a group linked with GroupCreationAllowedGroupId
Group Naming Policy		Yes	Each user that is also a member of a group within tenant.
Group Expiry*		Yes	Each user that is also a member of a group affected by a group's expiration policy.
Usage Guidelines		Yes	Each user that is also a member of a group within tenant.
Default classification		Yes	Each user that is also a member of a group within tenant.

* Admins don't need an AAD P1 license just to configure the expiration settings

* No licenses required for guest access

IMPORTANT: For all the Groups features, if you have an Azure AD Premium subscription, users can join the group whether or not they have an AAD P1 license assigned to them. Licensing isn't enforced.

What's Next

What's next

In workload expiration notification and auto extend notification

New and improved group admin roles

Admin center improvements

Unified Group classification using Microsoft Information Protection Labels

dynamic membership for Teams based groups

Group driven membership

Office 365 Groups UserVoice

<https://office365.uservoice.com/forums/286611-office-365-groups>

Microsoft Tech Community

<https://techcommunity.microsoft.com>

Office 365 Roadmap

<https://fasttrack.microsoft.com/roadmap>

Office Blogs

<https://blogs.office.com/>

Office 365 Admin Center – Message Center

<https://portal.office.com/AdminPortal>

Office 365 for IT Pros

<http://exchangeserverpro.com/ebooks/office-365-for-it-pros>

Essential Powershell for Office 365

<https://www.amazon.com/Essential-PowerShell-Office-365-Productivity/dp/1484231287>



Help Contribute &
Stay Informed!

Questions?

Email: drew.madelung@protiviti.com

Twitter: @dmadelung

Website: drewmadelung.com

Scripts: <http://bit.ly/DrewGroupScripts>

Slides: <http://bit.ly/DrewSlides>



Managing Office 365 Groups

SharePoint Saturday Twin Cities 2018

#SPSTC

