



BeConnected *day*



BeConnected
day

Information Barriers and Supervision Policies in Microsoft Teams



Alessio Giombini
Architect, Business Productivity

Microsoft UK



“Businesses and users are going to embrace technology only if they can trust it.”

Satya Nadella
Chief Executive Officer
Microsoft Corporation



Information Barriers

Agenda

1. Learn

You learn about the solution,
we learn about you

1. What are Information Barriers
2. Use cases and scenarios
3. When/who and requirements

2. Plan

Make informed decisions
that influence the design

1. Planning key concepts
2. Segments and attributes

3. Deploy

Decide how we're going
to complete the work

1. IB deployment workflow
2. IB PowerShell generator

4. User experience

1. Admin experience
2. User experience

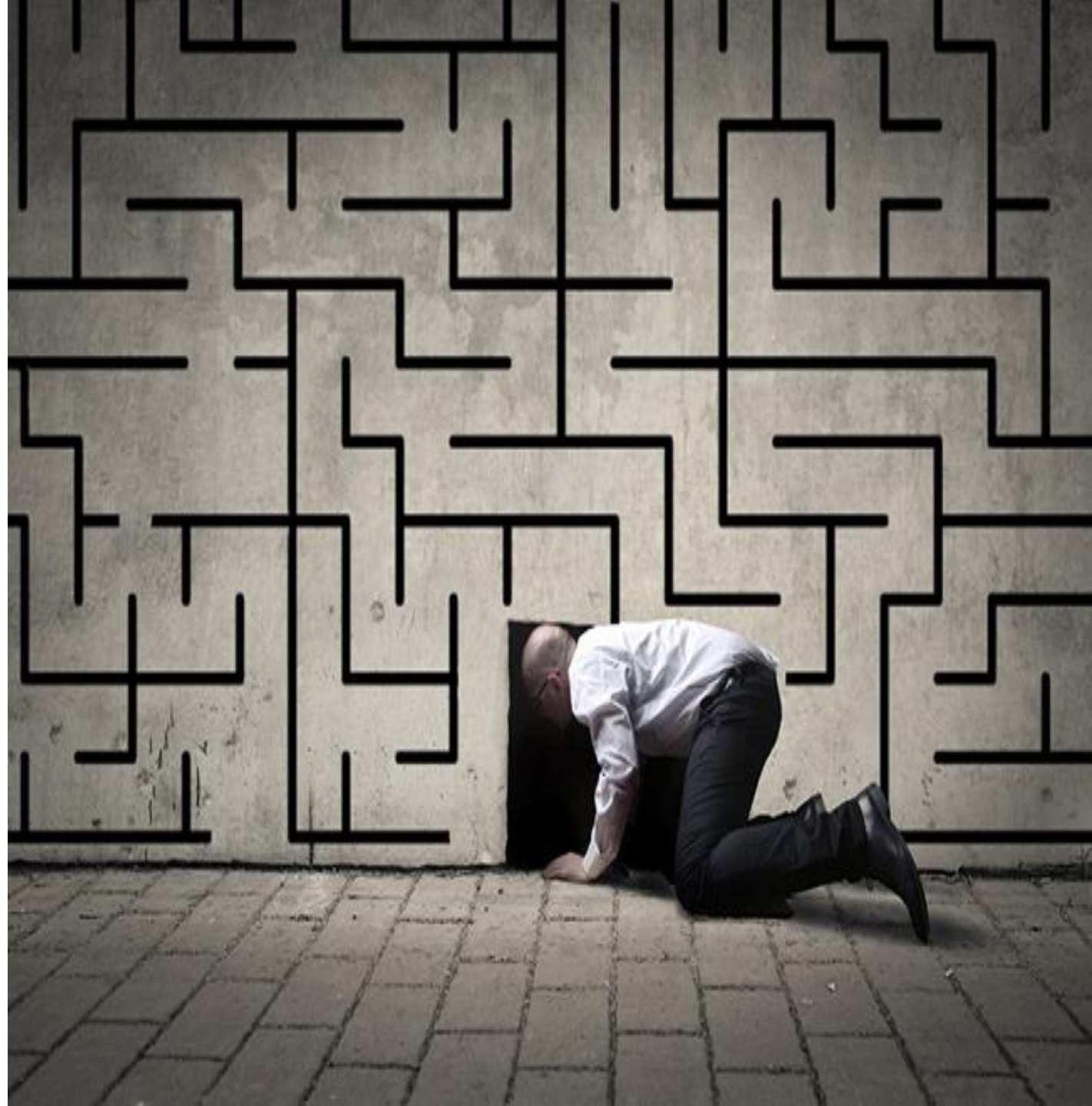
Learn IB

Information barriers are designed to properly control the flow of information from one part of the organization to another.

Also known as:

- Ethical firewall

information barriers are independent from [compliance boundaries](#).





Banking & Finance

Separating advisory and brokering department, protect insider information from being shared



Education

Students in one school/classroom cannot look find contact details of students from different school/classroom



Law Firms

Prevent information obtained while representing a client from being disclosed to employees in the same firm who represent other clients



Professional Services

Group of people inside a company is only allowed to chat with one or few specific groups



Department of Defense

Group of peoples presence information cannot be seen

The primary driver for information barriers comes from the financial services industry. The Financial Industry Regulatory Authority (FINRA) reviews information barriers and conflicts of interest within member firms and provides guidance as to how to manage such conflicts (FINRA 2241, Debt Research Regulatory Notice 15-31).

What you should know about IB

Functional

Known gotchas and limitations

- In-tenant only. IB do not work across tenants
- Using bots to add users not supported in v1
- Works with new and existing threads
- ~~Managed in S&CC (PowerShell only)~~

Scope

- Prevent lookup and discovery
- Applies to:
 - private chat (1:1, group)
- Currently does not apply to:
 - ~~SPO or ODFB~~
 - Email



License requirements

What licenses do you need?

- Microsoft 365 E5
- Office 365 E5
- Office 365 Advanced Compliance
- Microsoft 365 E5 Information Protection and Compliance

New announcements at Ignite 2019

Description	Status	Products	Release
<p>Information barriers (private preview)</p> <p>Not only in governance, we are also evolving our Compliance controls for highly regulated verticals like Finance, Healthcare, etc., FINRA like compliance regulations for finance vertical require controls in place to avoid insider trading between different department users in the organization. You can now achieve these advanced regulations with the Information Barriers scenario in SharePoint and OneDrive. Sign up if you are interested in joining any of the above security private previews: https://aka.ms/SecurityPreviews.</p> <p>More info</p>	In development	SharePoint O365 Preview Worldwide (Standard Multi-Tenant)	Q2 CY2020

Featured ID: 57313
Added to Roadmap: 11/4/2019
Last Modified: 11/4/2019
Tags: SharePoint, O365, Preview, Worldwide (Standard Multi-Tenant)

Microsoft 365 compliance

Search

Home

All Alerts

Reports

All Policies

Compliance score

Data classification

Solutions

Catalog

Information protection

Permissions

Information Barrier Policy

Use information barrier policies to control communication and collaboration in M365 workload between two groups of people. [Learn more](#)
Before setting up information barriers in your org, there are some important prerequisites to consider.

Segments

Policies

Applications

Policies

+ Create a policy

Refresh

✓

Name ↓

✓

Investment banking to Advisory

Megan Bowen

October 18, 2019 at 05:05 AM

Investment Banking

Segment Name

Investment Banking

Communication and Collaboration

Allowed

Blocked

Segment

Advisory

Policy status

On

Communication (email, Teams)

Collaboration (SharePoint, OneDrive for Business)

When are IB policies checked?

- ✓ Searching for a user
- ✓ Add users to a Team^(*)
- ✓ New chat is requested (1:1, group)
- ✓ Users invited to Teams meetings
- ✓ Screen sharing (2 or more users)
- ✓ Teams call

(*) From within Teams. However admin can still add unapproved users via O365 group membership or Teams Admin Centre



Who creates/edit IB policies?

To define or edit IB policies you need the following access level:

- ✓ Microsoft 365 global administrator
- ✓ Office 365 global administrator
- ✓ Compliance administrator
- ✓ IB Compliance Management (this is a new role!)



What about existing threads?

Users who were engaged in past conversations are now blocked. What happens?

- **1:1 Chat**
 - Existing chats become read-only
 - Further chat blocked
- **Group chat**
 - User(s) who violate the policy are removed from the group
 - Further chat blocked
 - Old conversation can still be seen
- **Team**
 - Removed from the team
 - Unable to see or participate in existing or new conversations



Plan IB

IB key concepts

- **User account attributes:** defined in Azure Active Directory (or Exchange Online). AD attributes that can be used to group users are *hold your breath for next slide*
- **Segments:** sets of users that are defined in the Office 365 Security & Compliance Center using a selected user account **AD attribute**
- **Information barrier policies** determine communication limits or restrictions. When you define information barrier policies, you choose from two kinds of policies:
 - "Block" policies prevent one segment from communicating with another segment.
 - "Allow" policies allow one segment to communicate with only certain other segments
- **Policy application:** is done after all information barrier policies are defined, and you are ready to apply them in your organization.

What attributes can be used to segment users?

Azure Active Directory property name (LDAP display name)	Exchange property name
Co	Co
Company	Company
Department	Department
ExtensionAttribute1~15	CustomAttribute1~15
MSEchExtensionCustomAttribute1~5	ExtensionCustomAttribute1~5
MailNickname	Alias
PhysicalDeliveryOfficeName	Office
PostalCode	PostalCode
ProxyAddresses	EmailAddresses
StreetAddress	StreetAddress
TargetAddress	ExternalEmailAddress
UsageLocation	UsageLocation
UserPrincipalName	UserPrincipalName
Mail	WindowsEmailAddress
Description	Description
MemberOf	MemberOfGroup

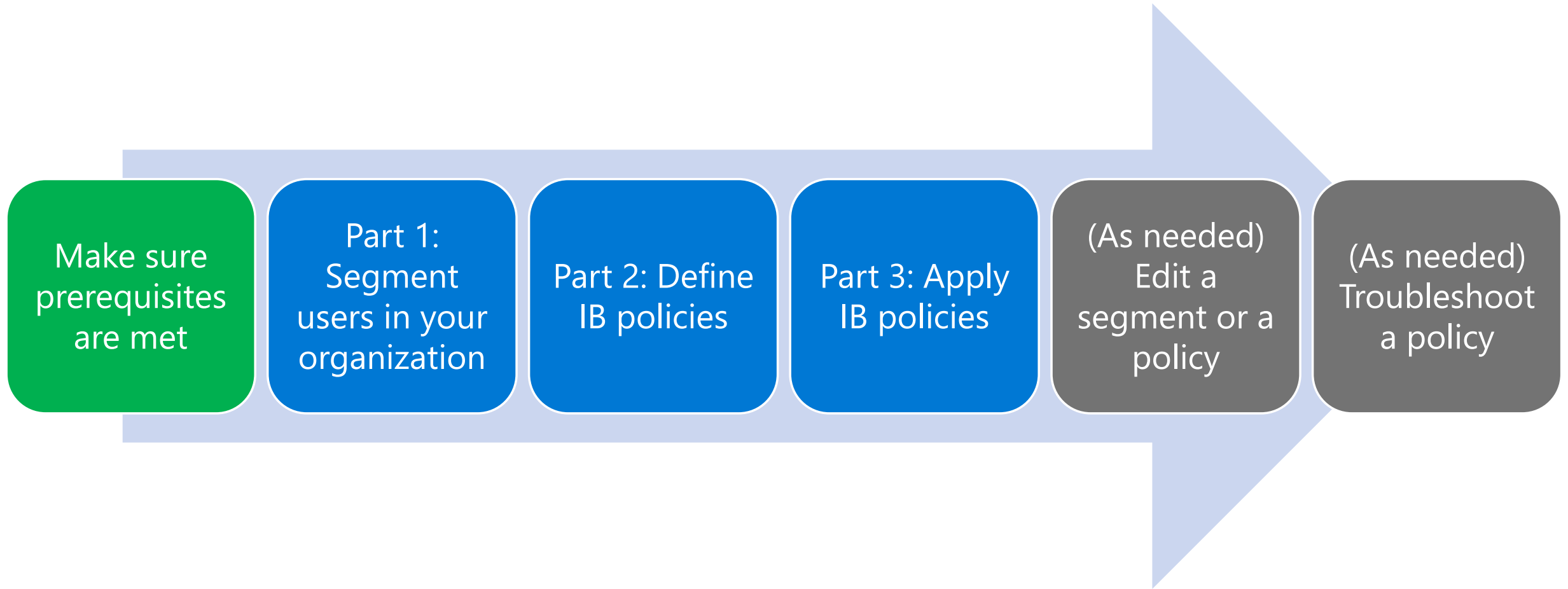
Design your segmentation approach carefully!

- ✓ no user should belong to two or more segments.
- ✓ Each segment can have only one IB policy applied.



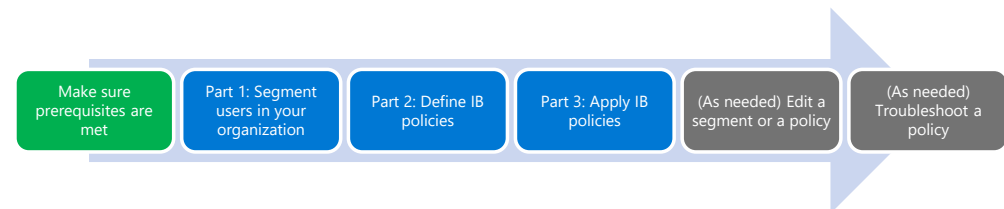
Deploy IB

IB workflow



IB workflow – Make sure prerequisites are met

- Verify that you have the [required licenses and permissions](#)
- Verify that your directory includes data for segmenting users (make sure that user account attributes used for IB are *consistently* populated in AD/AAD or EXO)
- Enable scoped directory search for Microsoft Teams
- Make sure audit logging is turned on
- Make sure no Exchange address book policies are in place
- Provide admin consent for Microsoft Teams



IB workflow

Enable scoped directory search for Teams

- <https://docs.microsoft.com/en-us/microsoftteams/teams-scoped-directory-search>

Audit Logging

- `Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true`

Ensure no EXO AB policies are in place

Preliminary IB configuration

- `$appId="bcf62038-e005-436d-b970-2a472f8c1982"`
- `$sp=Get-AzADServicePrincipal -ServicePrincipalName $appId`
- `if ($sp -eq $null) { New-AzADServicePrincipal -ApplicationId $appId }`
- `if ($sp -eq $null) { Get-AzADApplication -ApplicationId $appId | New-AzAdServicePrincipal }`

Provide admin consent for Microsoft Teams

- `Start-Process`
`"https://login.microsoftonline.com/common/adminconsent?client_id=\$appId"`

Run IB configuration

```
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
PS C:\Users\algiombi\Documents\OneDrive\Documents>
```



admin@bs291es.onmicrosoft.com

Permissions requested Accept for your organisation

Information Barrier Processor

[App info](#)

This app would like to:

- ✓ Read and write directory data
- ✓ Read and write all groups
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel

Accept

```
-e005-436d-b970-2a472f8c1982"
icePrincipal -ServicePrincipalName $a
1) { Get-AzAdApplication -Application
https://login.microsoftonline.com/comm
```


Meet the *InfoBarriers-PowerShellGenerator.xlsx*

InfoBarriers-PowerShellGenerator.xlsx				
AutoSave Off				
File Home Insert Draw Page Layout Formulas Data Review View Help				
Clipboard Font Alignment Protection Number				
G1				
Sensitivity: General				
1 Information Barrier segments and policies with PowerShell				
2 This workbook generates the PowerShell commands to create information barrier segments and policies.				
3 See this article for the step-by-step process: Define policies for information barriers				
6 1. Connect to the Security & Compliance Center and provide admin consent				
7 Run these commands at your PowerShell command prompt.				
9 \$UserCredential = Get-Credential				
10 \$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.compliance.prote				
11 Import-PSSession \$Session -DisableNameChecking				
12 Connect-AzAccount				
13 \$appId="bcf62038-e005-436d-b970-2a472f8c1982"				
14 \$sp=Get-AzADServicePrincipal -ServicePrincipalName \$appId				
15 if (\$sp -eq \$null) { New-AzADServicePrincipal -ApplicationId \$appId }				
16 Start-Process "https://login.microsoftonline.com/common/adminconsent?client_id=\$appId"				
20 2. Create segments and policies				
21 Fill in or specify the values of the cells with the blue background.				
23 Create new segments				
24 Segment name Filter attribute Filter operator Filter attribute value				Resulting PowerShell commands to paste int
25 Islands	Department	-eq	Islands	New-OrganizationSegment -Name '
26 Nations	Department	-eq	Nations	New-OrganizationSegment -Name '
27 Planets	Department	-eq	Planets	New-OrganizationSegment -Name '

Define policies for information barriers

08/07/2019 • 15 minutes to read • Q Q

Overview

With information barriers, you can define policies that are designed to prevent certain segments of users from communicating with each other, or allow specific segments to communicate only with certain other segments. Information barrier policies can help your organization maintain compliance with relevant industry standards and regulations, and avoid potential conflicts of interest. To learn more, see [Information barriers](#).

This article describes how to plan, define, implement, and manage information barrier policies. Several steps are involved, and the work flow is divided into several parts. Make sure to read through the [prerequisites](#) and the entire process before you begin defining (or editing) information barrier policies.

Tip

This article includes an [example scenario](#) and a [downloadable Excel workbook](#) to help you plan and define your information barrier policies.

Download from Microsoft Docs

<https://github.com/MicrosoftDocs/OfficeDocs-O365SecComp/raw/public/SecurityCompliance/media/InfoBarriers-PowerShellGenerator.xlsx>

InfoBarriers-PowerShellGenerator.xlsx

Demo

Part 1 – Segment users in your organisation

```
New-OrganizationSegment -Name "Islands" -UserGroupFilter "Department -eq 'Islands'"
New-OrganizationSegment -Name "Nations" -UserGroupFilter "Department -eq 'Nations'"
New-OrganizationSegment -Name "Planets" -UserGroupFilter "Department -eq 'Planets'"
```

```
PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts> New-OrganizationSegment -Name "Islands" -UserGroupFilter "Department -eq 'Islands'"

RunspaceId      : 6a1133f2-445e-4d39-95bf-03cd2deaa50b
Type            : OrganizationSegment
UserGroupFilter  : Department -eq 'Islands'
ExoSegmentId    : 8a74d1d4-764a-41b6-8b8b-2d98f7758ffd
ObjectVersion   : f11fca90-c628-4474-978b-08d7392a06a2
CreatedBy       : Alessio Giombini
LastModifiedBy  : Alessio Giombini
Comment         :
ModificationTimeUtc : 14/09/2019 15:41:35
CreationTimeUtc  : 14/09/2019 15:41:35
Identity        : FFO.extest.microsoft.com/Microsoft Exchange Hosted
                  Organizations/BS291ES.onmicrosoft.com/Configuration/Islands
Id              : FFO.extest.microsoft.com/Microsoft Exchange Hosted
                  Organizations/BS291ES.onmicrosoft.com/Configuration/Islands
ExchangeVersion : 0.20 (15.0.0.0)
Name            : Islands
DistinguishedName : CN=Islands,CN=Configuration,CN=BS291ES.onmicrosoft.com,OU=Microsoft Exchange Hosted
                  Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com
ObjectCategory  :
ObjectClass     : {msExchUnifiedPolicy}
WhenChanged     : 14/09/2019 16:41:36
WhenCreated     : 14/09/2019 16:41:36
WhenChangedUTC  : 14/09/2019 15:41:36
WhenCreatedUTC  : 14/09/2019 15:41:36
ExchangeObjectId : 23da7140-b685-4d60-8a70-8358195911f6
OrganizationId  : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/BS291ES.onmicrosoft.com -
                  FFO.extest.microsoft.com/Microsoft Exchange Hosted
                  Organizations/BS291ES.onmicrosoft.com/Configuration
Guid            : 23da7140-b685-4d60-8a70-8358195911f6
OriginatingServer :
IsValid         : True
ObjectState     : New

PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts>
```



Part 2 – Define IB policies

```
New-InformationBarrierPolicy -Name "Islands-to-Planets" -AssignedSegment "Islands" -SegmentsBlocked "Planets" -State Active  
New-InformationBarrierPolicy -Name "Planets-to-Islands" -AssignedSegment "Planets" -SegmentsBlocked "Islands" -State Active
```

```
PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts> New-InformationBarrierPolicy -Name "Islands-to-Planets" -AssignedSegment "Islands" -SegmentsBlocked "Planets" -State Active  
  
RunspaceId      : 6a1133f2-445e-4d39-95bf-03cd2deaa50b  
Type            : InformationBarrier  
AssignedSegment : Islands  
SegmentsAllowed : {}  
ExoPolicyId     : 8997af3f-c7c0-451f-b566-85bcfdffa503  
SegmentsBlocked : {Planets}  
SegmentAllowedFilter :  
BlockVisibility : True  
BlockCommunication : True  
State          : Active  
ObjectVersion  : 54b770f0-0dbe-4e4f-9c14-08d7392a8582  
CreatedBy      : Alessio Giombini  
LastModifiedBy : Alessio Giombini  
Comment        :  
ModificationTimeUtc : 14/09/2019 15:45:08  
CreationTimeUtc  : 14/09/2019 15:45:08  
Identity       : FFO.extest.microsoft.com/Microsoft Exchange Hosted  
Organizations/BS291ES.onmicrosoft.com/Configuration/Islands-to-Planets  
Id             : FFO.extest.microsoft.com/Microsoft Exchange Hosted  
Organizations/BS291ES.onmicrosoft.com/Configuration/Islands-to-Planets  
ExchangeVersion : 0.20 (15.0.0.0)  
Name           : Islands-to-Planets  
DistinguishedName : CN=Islands-to-Planets,CN=Configuration,CN=BS291ES.onmicrosoft.com,OU=Microsoft Exchange Hosted  
Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com  
ObjectCategory  :  
ObjectClass     : {msExchUnifiedPolicy}  
WhenChanged     : 14/09/2019 16:45:08  
WhenCreated     : 14/09/2019 16:45:08  
WhenChangedUTC  : 14/09/2019 15:45:08  
WhenCreatedUTC  : 14/09/2019 15:45:08  
ExchangeObjectId : 127b210a-9ce4-403c-a918-e51d820d124d  
OrganizationId  : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/BS291ES.onmicrosoft.com -  
FFO.extest.microsoft.com/Microsoft Exchange Hosted  
Organizations/BS291ES.onmicrosoft.com/Configuration  
Guid           : 127b210a-9ce4-403c-a918-e51d820d124d  
OriginatingServer :  
IsValid        : True  
ObjectState     : New  
  
WARNING: Your changes will take into affect after you run Start-InformationBarrierPoliciesApplication cmdlet.  
Start-InformationBarrierPoliciesApplication cmdlet only applies Active state policies.
```

2 Possible approaches

- `-SegmentsBlocked` parameter
Explicitly block 2 segments from mutual communication (segments can talk to other segments)
- `-SegmentsAllowed` parameter
Explicitly allow communication between 2 or more segments (segments cannot talk to other segments)



Part 3 – Apply IB policies

```
PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts> Start-InformationBarrierPoliciesApplication
WARNING: It may take several hours for the application to finish. Please check the status using
Get-InformationBarrierPoliciesApplicationStatus cmdlet. Execution of New/Set cmdlets will be prevented until start/stop
is finished.
```

```
RunspaceId      : 6a1133f2-445e-4d39-95bf-03cd2deaa50b
Identity        : 26a96e60-e071-47ad-8fa3-2713d9a8eefb
CreatedBy       : Alessio Giombini
CancelledBy     :
Type            : ExoApplyIBPolicyJob
ApplicationCreationTime : 09/14/2019 15:49:49
ApplicationEndTime :
ApplicationStartTime : 09/14/2019 15:49:49
TotalBatches    : 0
ProcessedBatches : 0
PercentProgress : 0
TotalRecipients : 0
SuccessfulRecipients : 0
FailedRecipients : 0
FailureCategory : None
Status          : NotStarted
IsValid         : True
ObjectState     : Unchanged
```

```
PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts> Get-InformationBarrierPoliciesApplicationStatus
```

```
RunspaceId      : 924b69c5-c1d7-4f35-a41e-8c75061b3807
Identity        : 26a96e60-e071-47ad-8fa3-2713d9a8eefb
CreatedBy       : Alessio Giombini
CancelledBy     :
Type            : ExoApplyIBPolicyJob
ApplicationCreationTime : 09/14/2019 15:49:49
ApplicationEndTime : 09/14/2019 16:07:45
ApplicationStartTime : 09/14/2019 15:49:49
TotalBatches    : 1
ProcessedBatches : 1
PercentProgress : 100
TotalRecipients : 52
SuccessfulRecipients : 52
FailedRecipients : 0
FailureCategory : None
Status          : Completed
IsValid         : True
ObjectState     : Unchanged
```

1. Use `Get-InformationBarrierPolicy` to see a list of defined policies. Note the status and identity (GUID) of each policy.
2. Use `Set-InformationBarrierPolicy` with an `Identity` parameter, and the `State` parameter set to `Active` to enable IB policies
3. When ready use `Start-InformationBarrierPoliciesApplication` to apply
4. **BE PATIENT! ;-)**
 1. After approximately 30 mins, policies are applied, user by user, for your organization.
 2. For large organizations may take 24 hours (or more) to complete.
 3. Rule of thumb: it takes about an hour to process 5,000 user accounts.



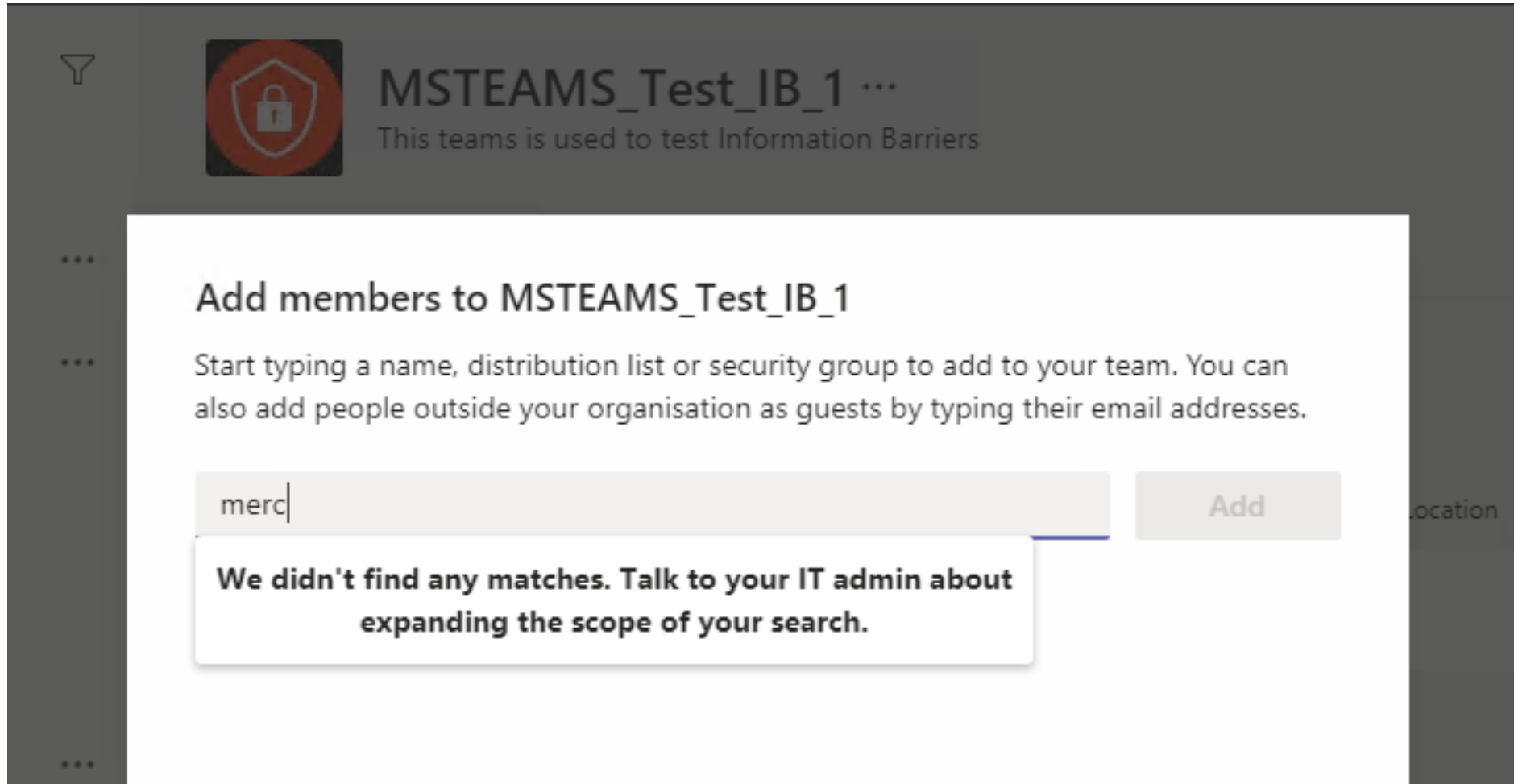
Part 3 – Apply IB policies...too fast

```
PS C:\Users\algiombi\Documents\OneDrive\Documents\AppData\Scripts> Start-InformationBarrierPoliciesApplication
Your request failed to complete. Please retry. Error Details:
Microsoft.Exchange.Management.Tasks.AsymmetricPoliciesException,IB Policies are not symmetric. Please ensure that the
policies are defined two-ways. For example, if there is a policy where Segment1 cannot communicate with Segment2, then
there must be another policy where Segment2 cannot communicate with Segment1.
Status: ProtocolError
Status code: InternalServerError (500)
Status description: Internal Server Error
Response headers:
Pragma: no-cache
request-id: f2585759-7215-46d7-ab30-bcdc2228f6b9
X-CalculatedBETarget: bn7pr05mb4420.namprd05.prod.outlook.com
X-RUM-Validated: 1
X-UserType: Business
X-MailboxGuid: 35e2fc28-4650-4138-b336-f4bd4c4025b2
x-ms-appId: 00000007-0000-0fff1-ce00-000000000000
X-Psws-ErrorCode: 840001
X-Psws-Exception: Microsoft.Exchange.Management.Tasks.AsymmetricPoliciesException,IB Policies are not symmetric.
Please ensure that the policies are defined two-ways. For example, if there is a policy where Segment1 cannot
communicate with Segment2, then there must be another policy where Segment2 cannot communicate with Segment1.
X-Content-Type-Options: nosniff
DataServiceVersion: 1.0;
X-DiagInfo: BN7PR05MB4420
X-BEServer: BN7PR05MB4420
Cache-Control: no-cache, no-store
Content-Type: application/xml; charset=utf-8
Expires: -1
Set-Cookie: X-BackEndCookie2=Migration.8f3e7716-2011-43e4-96b1-aba62d229136@BS291ES.onmicrosoft.com=u56Lnp2ejJqBz8/Ixpu
dyp3Smp2ex9LLm8eZ0p7Lys3SxsvKz83Hmp2ZnM7MgcbNzcvNzZvG0pnHy8zSy8rNxtKenZub0p7HzsjIzM/Jns/PzoHNz87G0s7P0s7Lq87KxcvIxc/LgZ
Geko+Nm8/K0Y+NkJvRkIqLk5CQlNGckJI=; expires=Mon, 14-Oct-2019 15:47:04 GMT; path=/psws; secure; HttpOnly,X-BackEndCookie
=Migration.8f3e7716-2011-43e4-96b1-aba62d229136@BS291ES.onmicrosoft.com=u56Lnp2ejJqBz8/Ixpudyp3Smp2ex9LLm8eZ0p7Lys3Sxsv
Kz83Hmp2ZnM7MgcbNzcvNzZvG0pnHy8zSy8rNxtKenZub0p7HzsjIzM/Jns/PzoHNz87G0s7P0s7Lq87KxcvIxc/L; expires=Mon, 14-Oct-2019
15:47:04 GMT; path=/psws; secure; HttpOnly
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
```



User experience

Segmented user
trying to add a user
from another
(blocked) segment
in a Team



The screenshot shows the Microsoft Teams interface. At the top, a team header for 'MSTEAMS_Test_IB_1' is visible, with a subtitle 'This teams is used to test Information Barriers'. Below the header, a modal dialog titled 'Add members to MSTEAMS_Test_IB_1' is open. The dialog contains instructions: 'Start typing a name, distribution list or security group to add to your team. You can also add people outside your organisation as guests by typing their email addresses.' Below this text is a search input field containing the text 'merc' and an 'Add' button to its right. A message box at the bottom of the dialog states: 'We didn't find any matches. Talk to your IT admin about expanding the scope of your search.'

Add members to MSTEAMS_Test_IB_1

Start typing a name, distribution list or security group to add to your team. You can also add people outside your organisation as guests by typing their email addresses.

merc

We didn't find any matches. Talk to your IT admin about expanding the scope of your search.

Add

Non-segmented user trying to add a user from a segment in a Team where there are already users from another segment which is blocked for the user you're trying to add

- *Islands* and *Planets* are mutually blocked segments
- *Islands* users already present in the Team
- Admin tries to add Mercury (*Planet*) in the Team


Add members to MSTEAMS_Test_IB_2

Start typing a name, distribution list or security group to add to your team. You can also add people outside your organisation as guests by typing their email addresses.

Add

We couldn't add member.

Retry all ↺



Mercury

MERCURY

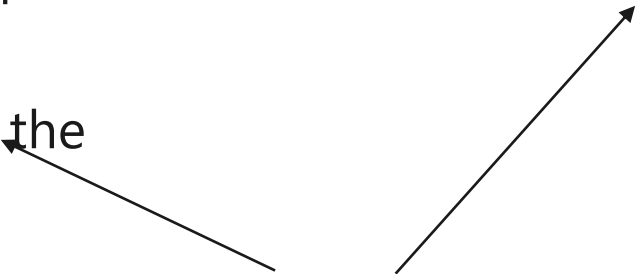
Unable to add user due to IT admin settings. [Learn more](#)

Retry ↺

✕

Blocked!

Close



MSTEAMS Test IB 2



MSTEAMS_Test_IB_2 ...

Public Teams-MedSec

This teams is used to test Information Barriers. In this team ALESSIO GIOMBINI (who is an admin and not a member ...

Members Channels Settings Analytics Apps

Search for members

Q

Add member

Owners (1)

Name	Title	Location	Role
Alessio Giombini	CEO	Office of the CEO	Owner <div>▼</div>

Members and guests (2)

Name	Title	Location	Role
Cuba	User		Member <div>▼</div> <div>✕</div>
Sicily	Architect		Member <div>▼</div> <div>✕</div>

AG	Alessio Giombini	algiombi@microsoft.com	-	-	Guest
	Mercury	mercury@doulouz.com	-	-	Member <div>▼</div>

Current experience	Improved experience (coming soon)
People tab - A user may see some blocked users on the People tab. The user can select the blocked users.	People tab - A user cannot see blocked users on the People tab.
Activity tab - If a user visits the Activity tab of a blocked user, no posts will appear. (The Activity tab displays channel posts only, and there would be no common channels between the two users.)	
Org charts - If a user accesses an org chart on which a blocked user appears, the user will see the blocked user on the chart and can click actions on the chart, but the actions (such as calling) will not go through.	Org charts - If a user accesses an org chart on which a blocked user appears, the blocked user will not appear on the org chart and an error message will appear instead.
People card - If a user participates in a conversation and is subsequently blocked, other users can still see the people card for the blocked user. All actions listed on the card (such as calling and chat) will be available, but the actions will not go through.	People card - If a user participates in a conversation and the user is subsequently blocked, other users will see an error message instead of the people card when they hover over the blocked user's name. Actions listed on the card (such as calling and chat) will be unavailable.
Suggested contacts - On the suggested contacts list (the initial contact list that appears for new users), users can see all suggested contacts (including blocked users). However, if a user clicks the name of a blocked user to open the Chats pane, the message will be blocked.	Suggested contacts - Blocked users do not appear on the suggested contacts list (the initial contact list that appears for new users).
Chat contacts - A user can see blocked users on the chat contact list.	Chat contacts - A user cannot see blocked users on the chat contact list.
Calls contacts - A user can see blocked users on the calls contact list and actions such as calling and messaging will appear, but when the user tries to call or send a message to the blocked user, the call or message will not go through.	Calls contacts - A user can see blocked users on the calls contact list, but the blocked users will be identified and the only action the user can perform is to delete them.
Skype to Teams migration - During a Skype for Business to Teams migration, all users, even those blocked by information barrier policies, will be migrated to Teams and then will be handled as described above.	

Codice Mattina 2/5

__ ZL __ _ _ _ _ _

Supervision Policies

Agenda

1. Learn

You learn about the solution,
we learn about you

1. What are Supervision Policies
2. Use cases and scenarios
3. When/who and requirements

2. Plan

Make informed decisions
that influence the design

1. Planning key concepts

3. Deploy

Decide how we're going
to complete the work

1. SP deployment workflow

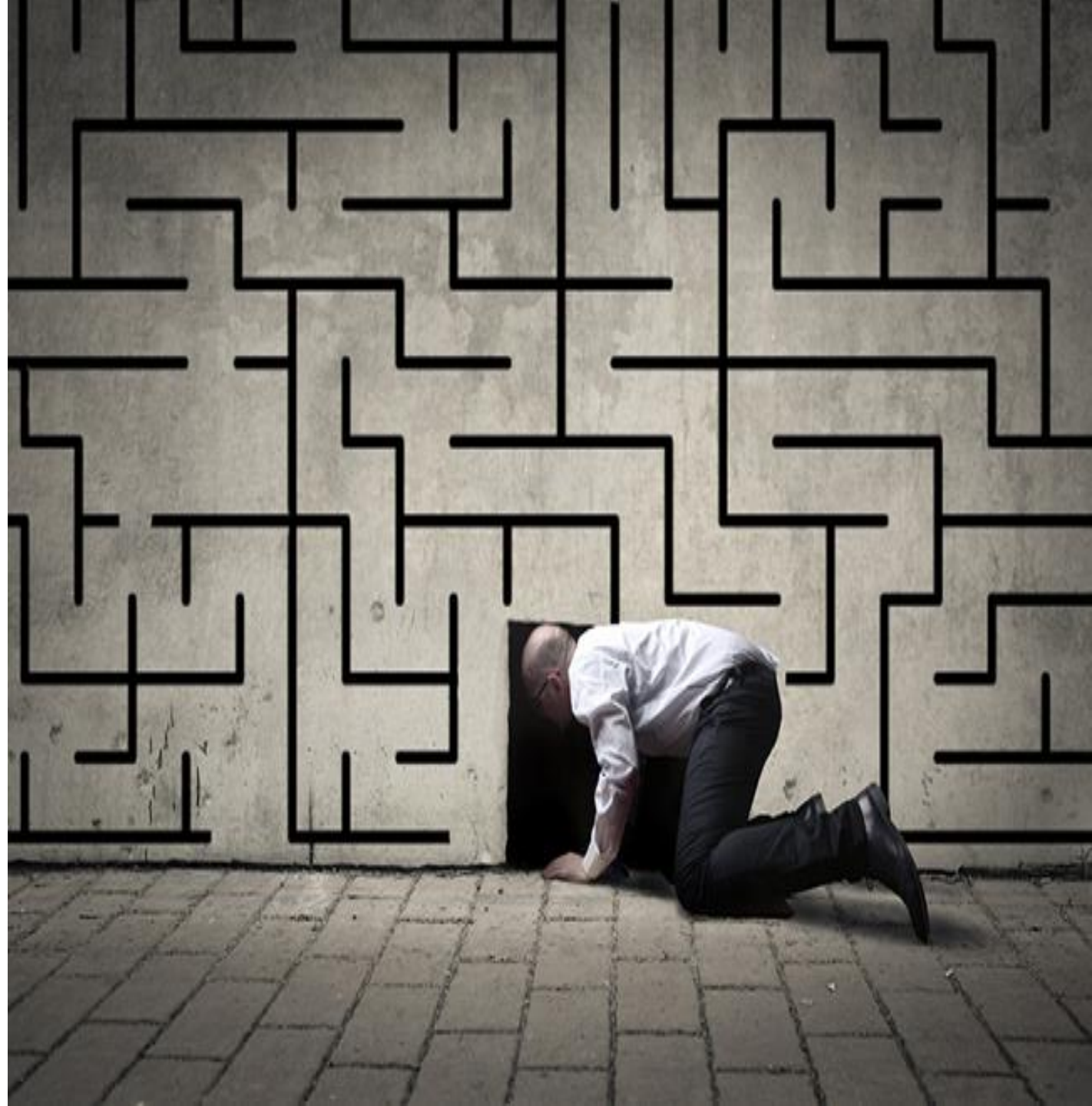
4. User experience

1. Demo

Learn SP

Supervision Policies allow to capture employee communications for review/examination by designated reviewers

Do not confuse with DLP



Address Modern Workplace compliance challenges:

- Increasing types of communication channels
- Increasing volume of data
- Regulatory enforcement and risk of fines
- Support Corporate policies
 - Ethical standards
 - Acceptable Use
 - Harassment
- Risk Management
- Regulatory compliance

What you should know about SP

Functional

Known gotchas and limitations

- Retained for 7 years by default
- Retained even when related mailboxes are deleted
- Supervise offensive/harassing language via ML/AI
- Supervise via existing/custom Sensitive Information types
- Supervise via custom keywords (100K per dictionary)

Scope

- Exchange Online including supported attachments (instantly)
- Microsoft Teams
 - 1:1/Private/Group chats (processed every 24 hrs)
 - Channel conversations (processed every 24 hrs)
 - Files
- Skype for Business Online (processed every 24 hrs)
- 3rd party sources (e.g. Facebook, DropBox)



License requirements

What licenses do you need?

- Microsoft 365 E5
- Office 365 E5
- Office 365 Advanced Compliance
- Microsoft 365 E5 Information Protection and Compliance

Who creates/edit SP policies?

To define or edit SP policies you need the following access level:

- ✓ Microsoft 365 global administrator
- ✓ Office 365 global administrator
- ✓ Compliance administrator

You also need to define:

- ✓ Supervisory Review role



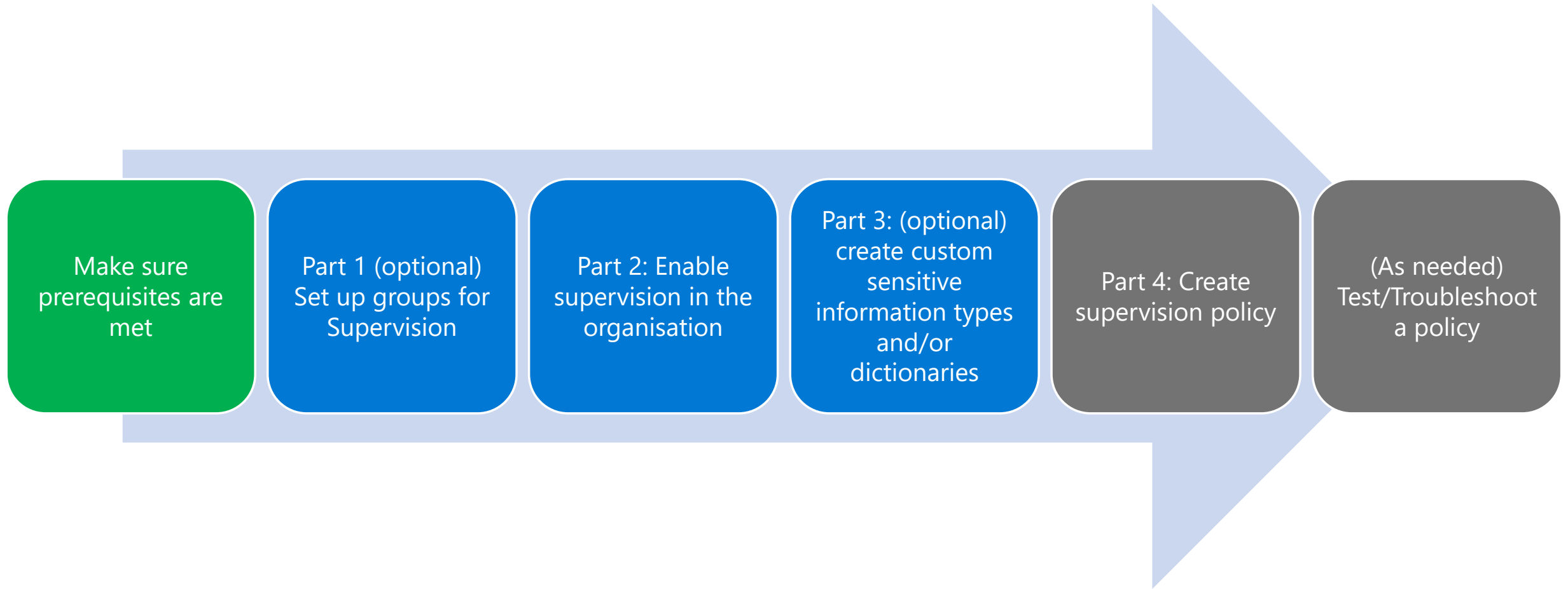
Plan SP

SP Building Blocks

- Supervision Policies
 - Sensitive information types (new or pre-defined)
 - Offensive language (use a mix of AI/ML/Keywords) – English only
 - Profanity
 - Slurs
 - Taunts
 - Disguised expressions
 - Custom dictionary (up to 100K words per dictionary) – single policy can use multiple dictionaries
- Supervised users
- Reviewers
- Direction
- Conditional settings
- Supervision policy dashboard
- Reports
- Audits

Deploy SP

SP workflow



SP workflow – Set up groups for supervision

Use Groups to facilitate management and lifecycle of supervised user.
Supported Groups:

- Supervised user: DG or O365 group (no Dynamic DG)
- Reviewers: Mail-enabled SG (no DG or Dynamic DG)

Create dedicated DGs for your global SP and use these properties:

- **MemberDepartRestriction = Closed.** Ensures that users cannot remove themselves from the distribution group.
- **MemberJoinRestriction = Closed.** Ensures that users cannot add themselves to the distribution group.
- **ModerationEnabled = True.** Ensures that all messages sent to this group are subject to approval and that the group is not being used to communicate outside of the supervision policy configuration.

Use PowerShell to configure a DG

- `New-DistributionGroup -Name <your group name> -Alias <your group alias> -MemberDepartRestriction 'Closed' -MemberJoinRestriction 'Closed' -ModerationEnabled $true`

Select an unused EXO custom attribute to track users added to the supervision policy in the organisation.

Run a PowerShell script on a recurring schedule to add users to the supervision policy

User experience

Q&A



BeConnected *day*