

**nikki chapple**

Blog de Microsoft 365 y equipos

Cómo aplicar el acceso justo a tiempo a los roles de seguridad y cumplimiento

Publicado en **4 abril 2022** Actualizado en **8 abril 2022**

Administración de Microsoft 365, Gobernanza y cumplimiento de Microsoft 365

A menudo, los clientes me preguntan cómo pueden proporcionar niveles adicionales de controles a sus roles privilegiados de seguridad y cumplimiento para mitigar los riesgos de permisos de acceso excesivos, innecesarios o mal utilizados a recursos importantes.

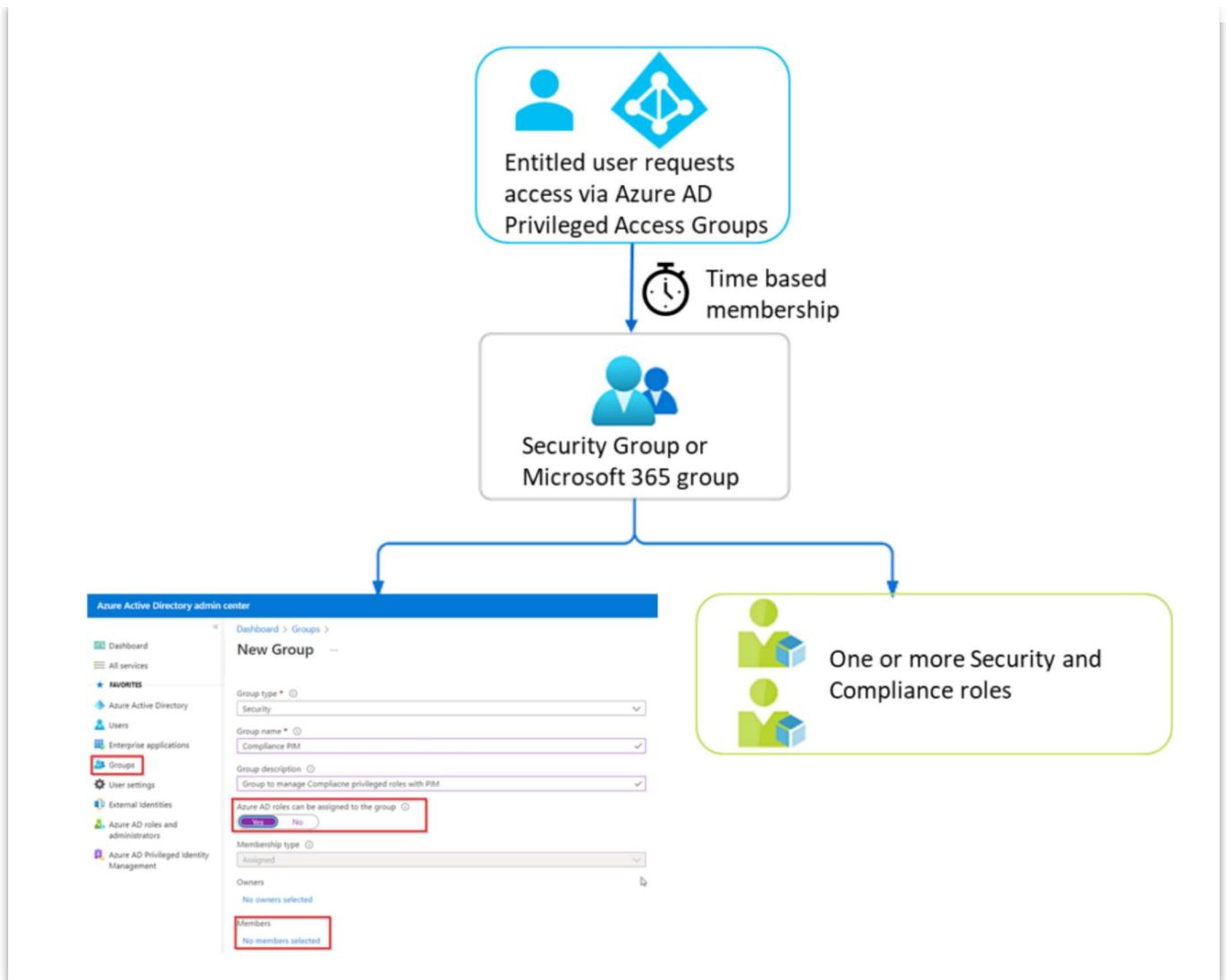
Microsoft recomienda las siguientes prácticas recomendadas para administrar cuentas con privilegios:

- Usar acceso con privilegios mínimos
- Active la autenticación multifactor para todas sus cuentas de administrador
- Use Privileged Identity Management para otorgar acceso justo a tiempo con aprobaciones opcionales
- Configure revisiones de acceso recurrentes para revocar permisos innecesarios con el tiempo

Si tiene una licencia de Azure AD Premium 2, puede usar **Azure AD Privilege Identity Management (PIM)** para proporcionar acceso justo a tiempo a las cuentas de administrador con privilegios. PIM solo proporciona acceso justo a tiempo a Azure AD y roles privilegiados de Azure. El problema con los roles de seguridad y cumplimiento es que se administran en los centros de administración de seguridad y cumplimiento y no en Azure AD.

Entonces, ¿cómo podemos proteger los roles de seguridad y cumplimiento con acceso justo a tiempo para mitigar los riesgos de permisos de acceso excesivos, innecesarios o mal utilizados a recursos importantes?

Continúe leyendo para descubrir cómo usar los **grupos de acceso privilegiado en PIM** para proporcionar indirectamente acceso justo a tiempo a sus funciones de seguridad y cumplimiento. Además, este proceso funcionará con otros roles que no sean de Azure AD, como los roles de Exchange o SharePoint.



¿Qué es la gestión de identidad privilegiada?

Privileged Identity Management (PIM) proporciona una activación de roles basada en el tiempo y la aprobación para mitigar los riesgos de permisos de acceso excesivos, innecesarios o mal utilizados a recursos importantes.

PIM le permite permitir un conjunto específico de acciones en un ámbito particular. Características clave:

- Proporcione acceso privilegiado **justo a tiempo** a los recursos
- Asignar **elegibilidad para membresía o propiedad** de grupos de acceso privilegiado
- Asigne acceso con **límite de tiempo** a los recursos utilizando fechas de inicio y finalización
- Requerir **aprobación** para activar roles privilegiados
- Aplique **la autenticación multifactor** para activar cualquier rol
- Use **la justificación** para comprender por qué los usuarios activan
- Reciba **notificaciones** cuando se activen los roles privilegiados
- Realice **revisiones de acceso** para garantizar que los usuarios aún necesiten roles
- Descargue el **historial de auditoría** para auditoría interna o externa

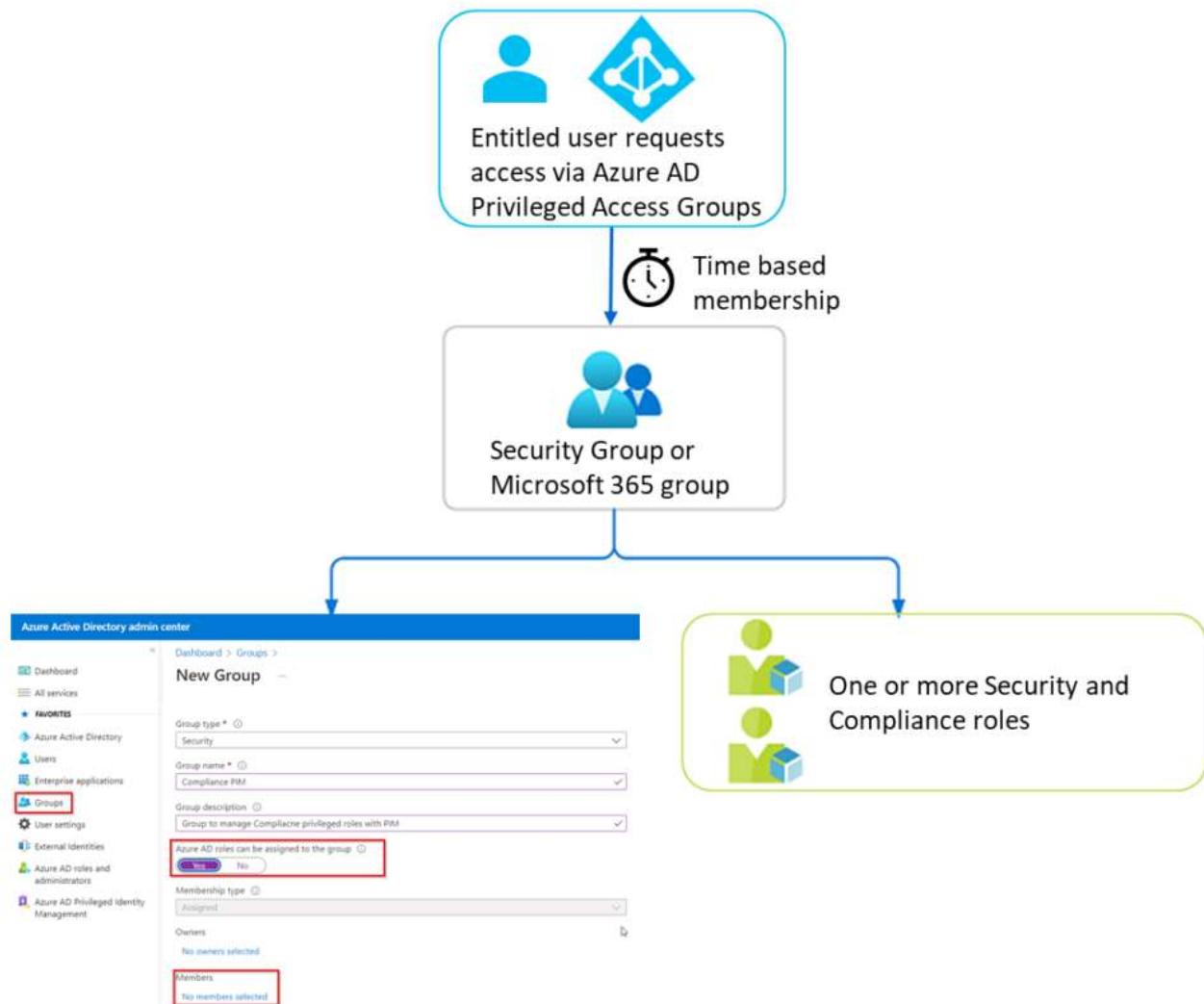
PIM proporciona acceso justo a tiempo a Azure AD y roles privilegiados de Azure. El problema es que los roles de seguridad y cumplimiento se administran en los centros de seguridad y cumplimiento de Microsoft

365 y no en Azure AD, por lo que PIM no puede asignar acceso justo a tiempo a estos roles. Afortunadamente, PIM tiene una nueva función llamada **Grupos de acceso privilegiado** que podemos usar.

¿Qué son los grupos de acceso privilegiado?

Los grupos de acceso privilegiado brindan acceso justo a tiempo a grupos de seguridad y grupos de Microsoft 365. Es importante destacar que los roles de Seguridad y Cumplimiento se pueden agregar como miembros de un grupo, de modo que cuando aplicamos el acceso justo a tiempo a un grupo, también proporcionamos acceso justo a tiempo a los roles de Seguridad y Cumplimiento.

Como se muestra en el diagrama a continuación, cuando a un usuario se le asigna una membresía justo a tiempo para el grupo, heredará automáticamente las funciones de seguridad y cumplimiento asignadas al grupo. Una vez que caduque la asignación, el usuario ya no formará parte del grupo y, lo que es más importante, perderá el acceso a los roles privilegiados.



Simplemente siga estos cuatro pasos para configurar grupos de acceso privilegiado y acceso justo a tiempo para sus roles de seguridad y cumplimiento.

Paso 1: Cree un grupo de Azure AD para administrar las asignaciones de roles de Cumplimiento

Cree un grupo de seguridad o un grupo de Microsoft 365 con la siguiente configuración:

En mi escenario, estoy creando un nuevo grupo de seguridad llamado 'Cumplimiento de PIM'.

Asegúrese de configurar "**Se pueden asignar roles de Azure AD al grupo**" en "**Sí**". Esta configuración permite agregar roles privilegiados como miembros del Grupo; no se puede actualizar después de crear el grupo.

No agregue miembros al grupo aquí, ya que esto les daría a los usuarios acceso permanente a los roles.

Asignaremos usuarios más tarde usando **Grupos de acceso privilegiado**.

New Group ...

Group type * ⓘ
Security

Group name * ⓘ
Compliance PIM

Group description ⓘ
Group to Add Compliance roles

Azure AD roles can be assigned to the group ⓘ
 Yes No

Membership type ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Paso 2: use PowerShell para agregar los roles privilegiados al grupo

El segundo paso es agregar los roles de seguridad y cumplimiento al nuevo grupo de Seguridad llamado '**Cumplimiento PIM**'. No es posible agregar grupos como miembros en los Centros de administración de seguridad o cumplimiento; solo puede agregar usuarios a los roles. Por lo tanto, debe usar PowerShell para agregar el grupo como miembro de sus funciones.

En mi escenario, quiero agregar tres grupos de roles al grupo de seguridad 'Cumplimiento PIM'.

1. 'Visor de lista de Content Explorer'
2. 'Explorador de contenido Visor de contenido'
3. 'Administrador de Cumplimiento'

Conéctese al PowerShell del Centro de seguridad y cumplimiento con la versión más reciente de Exchange Online V2.

```
$UserCredential = Get-Credential
```

```
#check which version of Exchange Online V2 (EXO V2) is installed  
Import-Module ExchangeOnlineManagement; Get-Module ExchangeOnlineManagement  
  
#Update EXO V2  
Update-Module -Name ExchangeOnlineManagement  
  
#import latest EXO V2 module  
Import-Module ExchangeOnlineManagement  
  
#Connects to Security & Compliance Center PowerShell  
Connect-IPPSSession -Credential $UserCredential
```

Utilice **Add-RoleGroupMember** para agregar el grupo 'Cumplimiento de PIM' a los tres grupos de funciones.

```
Add-RoleGroupMember -Identity 'ContentExplorerListViewer' -Member 'Compliance PIM'  
Add-RoleGroupMember -Identity 'ContentExplorerContentViewer' -Member 'Compliance PIM'  
Add-RoleGroupMember -Identity 'ComplianceAdministrator' -Member 'Compliance PIM'
```

Use **Get-RoleGroupMember** para verificar que los grupos se hayan agregado a los grupos de roles al verificar la pertenencia al grupo de roles de cada grupo.

```
Get-RoleGroupMember 'ContentExplorerContentViewer'  
Get-RoleGroupMember 'ContentExplorerListViewer'  
Get-RoleGroupMember 'ComplianceAdministrator'
```

En mi escenario, el grupo 'Cumplimiento de PIM' ahora es miembro de cada uno de los tres grupos de roles. También verá las personas que son miembros. En mi escenario, el 'Administrador de MOD' es miembro del grupo de roles 'Administrador de cumplimiento'.

```
PS C:\Users\Nikki> Get-RoleGroupMember 'ContentExplorerContentViewer'
```

Name	RecipientType
-----	-----
Compliance PIM Group	

```
PS C:\Users\Nikki> Get-RoleGroupMember 'ContentExplorerListViewer'
```

Name	RecipientType
-----	-----
Compliance PIM Group	

```
PS C:\Users\Nikki> Get-RoleGroupMember 'ComplianceAdministrator'
```

Name	RecipientType
-----	-----
MOD Administrator	MailUser
Compliance PIM	Group

También puede comprobar la pertenencia al grupo de roles desde los Centros de administración de cumplimiento o seguridad.

Compliance Administrator

[Edit role group](#)[Delete role group](#)[Copy role group](#)

INFORMATION PROTECTION ROLES

Insider Risk Management Admin

Manage Alerts

Organization Configuration

RecordManagement

Retention Management

View-Only Audit Logs

View-Only Case

View-Only Device Management

View-Only DLP Compliance Management

View-Only IB Compliance Management

View-Only Manage Alerts

View-Only Recipients

View-Only Record Management

View-Only Retention Management

Members

[Edit](#)

MOD Administrator

Compliance PIM

importante _ No use Azure AD para verificar la asignación de roles. No puede ver qué roles se han asignado a los grupos en Azure AD. Este es el comportamiento esperado porque los roles de seguridad y cumplimiento no se administran en Azure AD.

Paso 3: agregue miembros que tengan derecho a usar el grupo

Importante. No agregue miembros a través de la opción de menú de miembros, ya que esto otorga acceso permanente al grupo y, por lo tanto, acceso permanente a los roles privilegiados.

Los miembros deben agregarse a través del menú de **acceso privilegiado (vista previa)** a través de + **Agregar asignaciones** para asignaciones **elegibles**. De esta manera, solo tienen derecho y no se les otorgan permisos permanentes. Necesitan solicitar acceso cuando requieren acceso por tiempo limitado al grupo.

Compliance PIM | Privileged access (Preview)

Group

Add assignments Settings Refresh Export Got feedback?

Overview Diagnose and solve problems

Manage

~~Members~~

Properties Owners Roles and administrators Administrative units Group memberships Assigned roles Applications Licenses Azure role assignments

Activity

Privileged access (Preview)

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type
No results		

En mi escenario, Adele se agrega como una asignación Eligible al grupo 'PIM de Cumplimiento', por lo que puede solicitar acceso justo a tiempo al grupo a través de Grupos de Acceso Privilegiado cuando necesita acceso a los roles de Cumplimiento.

Add assignments

Privileged Identity Management | Privileged access groups (Preview)

[Membership](#) [Setting](#)

Resource

Compliance PIM

Resource type

Security

Select role ⓘ

Member



Select member(s) * ⓘ

1 Member(s) selected

Selected member(s) ⓘ



Adele Vance

AdeleV@nikkichapple.com | Last sign-in: 4/2/2022 7:47:44 PM | California, USA

Remove

Adele se muestra como una asignación elegible en el grupo Cumplimiento PIM.

Compliance PIM | Privileged access (Preview) ...

Overview Diagnose and solve problems Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Membership	Start time	End time	Action
Adele Vance	AdeleV@nikkichapple.com User	User	Direct	4/2/2022, 7:47:44 PM	4/2/2023, 7:36:10 PM	Remove Update Extend

Properties Members Owners Roles and administrators Administrative units Group memberships Assigned roles Applications Licenses Azure role assignments

Privileged access (Preview) Access reviews Audit logs Bulk operation results Troubleshooting + Support New support request

Add assignments

...

Privileged Identity Management | Privileged access groups (Preview)

[Membership](#) [Setting](#)

Assignment type ⓘ

 Eligible Active

Maximum allowed eligible duration is 1 year(s).

Assignment starts *

04/02/2022



7:36:10 PM

Assignment ends *

04/02/2023



7:36:10 PM

Paso 4: configure los ajustes de la función de miembro para el grupo de acceso privilegiado

El último paso es definir la configuración para la pertenencia al Grupo de acceso privilegiado. Esto le permite:

- Proporcione acceso privilegiado **justo a tiempo** a los recursos
- Asignar **eleibilidad para membresía o propiedad** de grupos de acceso privilegiado
- Asigne acceso con **límite de tiempo** a los recursos utilizando fechas de inicio y finalización
- Requerir **aprobación** para activar roles privilegiados
- Aplique **la autenticación multifactor** para activar cualquier rol
- Use **la justificación** para comprender por qué los usuarios activan
- Reciba **notificaciones** cuando se activen los roles privilegiados

En mi escenario, mantuve los permisos predeterminados que se muestran a continuación.

Role setting details - Member

Privileged Identity Management | Privileged access groups (Preview)

 Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	1 year(s)
Allow permanent active assignment	No
Expire active assignments after	6 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False
Notification to the assigned ...	Assignee	None	False
Request to approve a role as...	Approver	None	False

Send notifications when members are assigned as active to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False
Notification to the assigned ...	Assignee	None	False
Request to approve a role as...	Approver	None	False

Send notifications when eligible members activate this role:

Type	Default recipients	Additional recipients	Critical emails only
Role activation alert	Admin	None	False
Notification to activated user...	Requestor	None	False
Request to approve an activa...	Approver	None	False

Experiencia de usuario: activar roles de grupo de acceso privilegiado en Privileged Identity Management

Mis roles en [Privileged Identity Management](#) enumera los roles de Azure AD, los grupos de acceso privilegiado y los recursos de Azure que el usuario puede activar.

Para obtener acceso a un grupo, un usuario simplemente selecciona Grupos de acceso privilegiado y selecciona el grupo relevante.

En este escenario, Adele necesita **Activar** el grupo '**Cumplimiento PIM**' para que herede los tres grupos de roles de Cumplimiento:

- 'Visor de lista de Content Explorer'
- 'Explorador de contenido Visor de contenido'
- 'Administrador de Cumplimiento'

[Home](#) > [Privileged Identity Management](#) > [My roles](#)

My roles | Privileged access groups (Preview)

Privileged Identity Management | My roles

Activate

- Azure AD roles
- Privileged access groups (Preview)**
- Azure resources

Eligible assignments Active assignments Expired assignments

Role	Group	Group type	Membership	End time	Action
Member	Compliance PIM	Security	Direct	4/2/2023, 7:36:10 PM	Activate Extend

Troubleshooting + Support

X Troubleshoot **?** New support request

Se le solicita a Adele que seleccione la duración de la membresía; en mi caso, un máximo de ocho horas. Adele también debe proporcionar una razón para la activación. Las notificaciones también se envían si están habilitadas.

Nota. Los detalles variarán según las funciones de los miembros establecidas para el grupo de acceso privilegiado.

Activate - Member

Privileged Identity Management | Privileged access groups (Preview)

Roles **Activate** Status

Custom activation start time

Duration (hours) i

8

*Reason (max 500 characters) i

To investigate sensitive information types in Content explorer ✓

Se activa un paso de aprobación si se requiere aprobación; de lo contrario, se otorgará acceso al grupo.

My roles | Privileged access groups (Preview)

Privileged Identity Management | My roles

Activate

- Azure AD roles
- Privileged access groups (Preview)**
- Azure resources

Eligible assignments **Active assignments** Expired assignments

Role	Group	Group type	Membership	State	End time	Action
Member	Compliance PIM	Security	Direct	Activated	4/3/2022, 6:42:45 AM	Deactivate

Troubleshooting + Support

X Troubleshoot **?** New support request

Adele ahora es miembro del grupo de seguridad 'Cumplimiento PIM' durante las próximas 8 horas y hereda los tres grupos de funciones de Cumplimiento.

- 'Visor de lista de Content Explorer'
- 'Explorador de contenido Visor de contenido'
- 'Administrador de Cumplimiento'

Después de 8 horas de acceso al grupo, los roles asignados se eliminan automáticamente.

The screenshot shows the 'Compliance PIM | Members' page. On the left, there's a sidebar with 'Overview', 'Diagnose and solve problems', 'Manage' (with 'Properties', 'Members' selected, and 'Owners'), and a search bar. The main area has tabs for 'Direct members' (selected) and 'All members'. Below is a table with columns: Name, Type, Email, and User type. A row for Adele Vance is selected and highlighted with a red border. The table data is as follows:

Name	Type	Email	User type
Adele Vance	User	AdeleV@...	Member

Resumen

En conclusión, PIM no puede proporcionar acceso justo a tiempo a roles privilegiados de seguridad y cumplimiento directamente, ya que se administran en centros de administración de seguridad y cumplimiento y no en Azure AD. Sin embargo, en PowerShell, podemos agregar funciones de seguridad y cumplimiento como miembros de un grupo de seguridad o un grupo de Microsoft 365. Luego, podemos usar **grupos de acceso privilegiado** para proporcionar acceso justo a tiempo al grupo y proporcionar acceso justo a tiempo a los roles privilegiados de seguridad y cumplimiento. Además, este proceso funcionará con otros roles que no sean de Azure AD, como los roles de Exchange o SharePoint.

Solo recuerde que para usar **Grupos de acceso privilegiado** se necesitan licencias de Azure AD Premium 2 para los usuarios incluidos.

Tenga en cuenta que puede haber un retraso de tiempo entre convertirse en miembro del grupo y obtener acceso a los roles de seguridad y cumplimiento. Microsoft es consciente y está trabajando para solucionar los problemas.

⚠ Note

- Eligible users for the SharePoint administrator role, the Device administrator role, and any roles trying to access the Microsoft Security & Compliance Center might experience delays of up to a few hours after activating their role. We are working with those teams to fix the issues.

Referencias de Microsoft

Use grupos de Azure AD para administrar las asignaciones de roles: [Azure Active Directory | Documentos de Microsoft](#)

[Administrar grupos de acceso privilegiado en Privileged Identity Management \(PIM\)](#) | [Documentos de Microsoft](#)

[Add-RoleGroupMember \(ExchangePowerShell\) | Documentos de Microsoft](#)[« Anterior](#)[próximo »](#)

Mensajes recientes

- » [¿Sabe que ahora puede cargar sus acciones de mejora en Microsoft Purview Compliance Manager?](#)
- » [Cómo administrar las revisiones de acceso de invitados en Microsoft 365](#)
- » [Cómo realizar Teams y tareas de administración de usuarios sin salir de Teams](#)
- » [Cómo aplicar el acceso justo a tiempo a los roles de seguridad y cumplimiento](#)
- » [Cómo realizar un seguimiento de las actualizaciones de la página de Microsoft Docs en Microsoft To-do](#)

Etiquetas

[Cumplimiento \(1\)](#) [Gerente de Cumplimiento \(1\)](#) [datos \(1\)](#) [Correo electrónico \(1\)](#) [gobernanza \(1\)](#) [colaboración invitada \(1\)](#)[Invitados \(2\)](#) [Gestión del cambio \(1\)](#) [microsoft365 \(1\)](#) [Grupos de Microsoft 365 \(1\)](#) [ámbito de Microsoft \(1\)](#) [móvil \(3\)](#)[permisos \(1\)](#) [**Automatización de energía \(5\)**](#) [PowerShell \(1\)](#) [Informes \(2\)](#)[Charla de equipos \(1\)](#) [**Gobernanza de equipos \(6\)**](#)[Reuniones de equipos \(2\)](#)

Archivo

- » [agosto 2022](#)
- » [junio 2022](#)
- » [abril 2022](#)
- » [marzo 2022](#)
- » [febrero 2022](#)
- » [enero 2022](#)
- » [diciembre 2021](#)
- » [noviembre 2021](#)
- » [octubre 2021](#)
- » [mayo 2021](#)
- » [abril 2021](#)

- » [marzo 2021](#)
- » [febrero 2021](#)
- » [enero 2021](#)
- » [octubre 2020](#)

Descargo De Responsabilidad Política De Privacidad



© 2022 por Nikki Chapple. Reservados todos los derechos.