



MONTEVIDEO COMM® Tecnología para tus proyectos

TREND MICRO Cloud App Security

Aprovisionamiento de Microsoft Teams



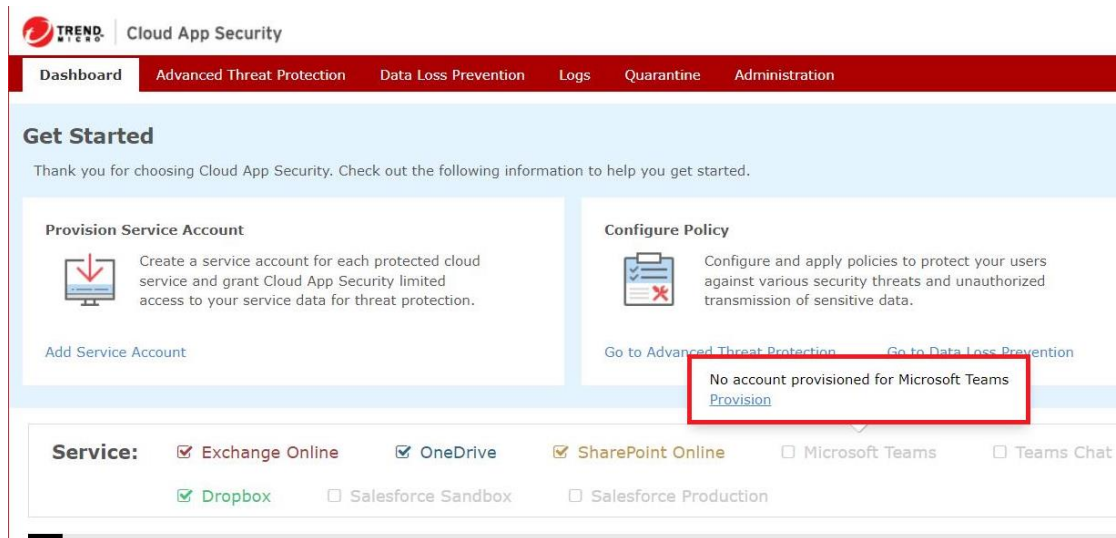
Aprovisione una cuenta de servicio para Microsoft Teams (Teams) para permitir que Cloud App Security ejecute protección avanzada contra amenazas y análisis de prevención de pérdida de datos en archivos en equipos protegidos.

Cloud App Security protege los servicios de Teams y Chat en Microsoft Teams por separado.

Cloud App Security analiza los archivos que los empleados comparten en los canales del equipo, que se almacenan en SharePoint. Si también ha provisionado una cuenta de servicio de SharePoint Online, cuando el sitio de SharePoint y el equipo correspondiente a un archivo se seleccionan como objetivo de política respectivamente, Cloud App Security aplica políticas para Microsoft Teams (Teams) a este sitio a menos que el sitio no alcance cualquier política para Microsoft Teams.

Para provisionar una cuenta de servicio para Microsoft Teams desde la consola web de Cloud App Security:

1. Inicie sesión en la consola de administración de Cloud App Security.
2. Pase el cursor sobre Microsoft Teams y haga clic en **Aprovisionar**.





- Haga clic en el enlace **Haga clic aquí** en el Paso 1. Esto abrirá una pantalla de inicio de sesión de Microsoft.

Provision Service Account for Microsoft Teams ×

Step 1: Grant Cloud App Security the permission to use the Graph API to access your Teams related service data. [Click here](#)

Step 2: Grant Cloud App Security the permission to use the SharePoint Client Object Modal API to access your Teams related service data. [Click here](#)

Step 3: Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning on your teams. [Learn more.](#)

Step 4: Click Done

[Done](#)

- Especifique sus credenciales de administrador global de Office 365 y haga clic en **Iniciar sesión**.
- Haga clic en **Aceptar** para otorgar a Cloud App Security el permiso para usar Graph API para acceder a todos los dominios bajo el arrendatario asociado con el Administrador global especificado.

Microsoft

Permissions requested
Review for your organization

Trend Micro Cloud App Security
[Trend Micro Incorporate](#)

This app would like to:

- Sign in and read user profile
- Read directory data
- Read all groups
- Read and write mail in all mailboxes
- Read all hidden memberships
- Use Exchange Web Services with full access to all mailboxes

If you accept, this app will get access to the specified resources for all users in your organization. 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](#)

Does this app look suspicious? [Report it here](#)

[Cancel](#) [Accept](#)



6. Vuelva a la consola de administración de Cloud App Security, como se indica, luego haga clic en el enlace **Haga clic aquí** en el Paso 2. Esto abrirá la pantalla de autorización de Microsoft Teams.

Provision Service Account for Microsoft Teams ×

✔ Step 1: Grant Cloud App Security the permission to use the Graph API to access your Teams related service data. [Click here](#)


Step 2: Grant Cloud App Security the permission to use the SharePoint Client Object Modal API to access your Teams related service data. [Click here](#)

Step 3: Follow the instructions to grant Cloud App Security permissions to receive notifications from Microsoft for real-time scanning on your teams. [Learn more](#).


Step 4: Click Done

[Done](#)

7. Haga clic en **Aceptar** para otorgar a Cloud App Security el permiso para acceder a los recursos en todos los sitios de Microsoft Teams.



Permissions requested
Review for your organization

Trend Micro Cloud App Security
[Trend Micro Incorporate](#) 

This app would like to:

- ✓ Sign in and read user profile
- ✓ Read directory data
- ✓ Read all groups
- ✓ Read and write mail in all mailboxes
- ✓ Read all hidden memberships
- ✓ Use Exchange Web Services with full access to all mailboxes

If you accept, this app will get access to the specified resources for all users in your organization. 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](#)

Does this app look suspicious? [Report it here](#)

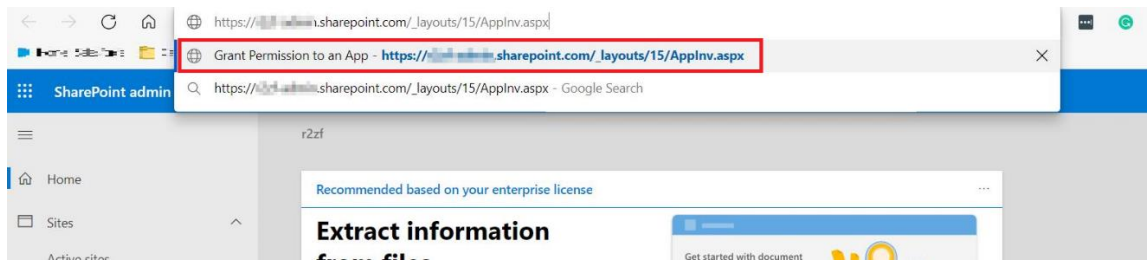
[Cancel](#) [Accept](#)

- Vuelva a la consola de administración de Cloud App Security como se indica. Tome nota de la ID de la aplicación que se muestra.

- Realice los siguientes pasos para otorgar permisos de Cloud App Security para recibir notificaciones de Microsoft sobre cualquier cambio en los archivos en sus sitios de Microsoft Teams.
 - Inicie sesión en el [centro de administración de Microsoft 365](#) con su cuenta de administrador global.
 - Vaya a **Centros de administración > SharePoint** desde la navegación de la izquierda. Aparece la página del centro de administración de SharePoint.

3. Cambie la URL del centro de administración de SharePoint a {sharepoint_admin_site}/_layouts/15/AppInv.aspx en la barra de direcciones.

Por ejemplo, cambie https://example-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/home a https://example-admin.sharepoint.com/_layouts/15/AppInv.aspx.



4. En la pantalla que aparece, ingrese la Id. de la aplicación asignada (del Paso 8) en el campo **Id. de la aplicación** y luego haga clic en **Buscar**. El campo Título se rellena automáticamente.

The screenshot shows the 'Grant Permission to an App' form. At the top, there are 'Create' and 'Cancel' buttons. The form is divided into two main sections: 'App Id and Title' and 'App's Permission Request XML'. In the 'App Id and Title' section, the 'App Id' field is highlighted with a red box, and a 'Lookup' button is positioned below it. Below the 'App Id' field are fields for 'Title', 'App Domain', and 'Redirect URL'. The 'App's Permission Request XML' section contains a large text area for entering XML code. At the bottom of the form, there are 'Create' and 'Cancel' buttons.

El Id. de la aplicación se puede encontrar en la Cuenta autorizada correspondiente en **Administración > Cuenta de servicio**.



5. En el campo **Dominio de la aplicación**, ingrese "tmcas.trendmicro.com".
6. Ingrese {Cloud App Security_admin_site}/provision.html en el campo **URL de redireccionamiento** según su sitio de servicio.
Por ejemplo, si la URL de su consola de administración de Cloud App Security en la barra de direcciones es "https://admin-eu.tmcas.trendmicro.com" después de iniciar sesión, ingrese https://admin-eu.tmcas.trendmicro.com /provision.html en el campo **URL de redirección** .
7. Copie y pegue la siguiente información en el campo **XML de solicitud de permiso**:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
```

```
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="Administrar" />
```

```
</AppPermissionRequests>
```

Create **Cancel**

App Id and Title
The app's identity and its title.

App Id: **Lookup**

Title:

App Domain:
Example: "www.contoso.com"

Redirect URL:
Example: "https://www.contoso.com/default.aspx"

App's Permission Request XML
The permission required by the app.

Permission Request XML:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="Administrar" />
</AppPermissionRequests>
```

Create **Cancel**

10. Vuelva a la consola de administración de Cloud App Security y haga clic en **Enviar**. Cloud App Security luego actualiza los datos de Microsoft Teams en su organización. El tiempo requerido depende de la cantidad de datos que tenga en Microsoft Teams.
11. En la esquina superior derecha de la consola de gestión, desplace el cursor sobre el icono de campana y confirme si el aprovisionamiento se realizó correctamente. Si aparece el mensaje "Microsoft Teams protected". aparece en la pantalla de Notificaciones, el aprovisionamiento es exitoso.

The screenshot displays the Trend Micro Cloud App Security dashboard. On the left, the 'Get Started' section includes a 'Provision Service Account' card with instructions and a list of services: Exchange Online, OneDrive, Dropbox, and Salesforce Sandbox. On the right, a 'Notifications (8)' panel is open, showing a list of status messages. The notification 'Microsoft Teams protected.' is highlighted with a red box, indicating successful provisioning. Other notifications include SharePoint Online, OneDrive, and Dropbox protection, as well as failures for Box and Google Drive, and an optional notification for Azure Rights Management.

Notification	Status	Timestamp
[Default organization] SharePoint Online protected.	Success	Jan 06, 2022 23:57:35
[Default organization] OneDrive protected.	Success	Jan 07, 2022 00:15:14
[Default organization] Failed to provision for Box because personal accounts are not supported. Retry	Failure	Dec 30, 2021 23:50:03
[Default organization] Dropbox protected.	Success	Dec 29, 2021 23:18:18
[Default organization] Google Drive not protected. Provision for Google Drive	Required	
[Default organization] Create an account for Azure Rights Management (Azure RMS) protected file scanning.	Optional	
[Default organization] Exchange Online protected.	Success	Jan 06, 2022 23:26:10
[Default organization] Microsoft Teams protected.	Success	Jan 07, 2022 00:27:24