TREND MICRO
Cloud App Security

Aprovisionamiento de Microsoft Teams Chat

Cloud App Security analiza contenidos y archivos que los empleados envían en chats privados con otros usuarios (uno a uno o uno a muchos). Los archivos de chat privados se almacenan en la carpeta OneDrive del remitente. Si también ha aprovisionado una cuenta de servicio de OneDrive, cuando el usuario envía o carga un archivo se selecciona como objetivo de política respectivamente, Cloud App Security aplica las políticas correspondientes para Teams Chat y OneDrive a este archivo.

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

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

Dado que los modelos de licencia de Microsoft para las API de Teams imponen restricciones de uso y requisitos de licencia en las llamadas de API, debe usar su propia aplicación registrada con Azure AD y seleccionar un modelo de licencia aplicable al aprovisionar Teams Chat. Para obtener detalles sobre los modelos de licencia, consulte la documentación de Microsoft .

La siguiente tabla resume los modelos de licencia y la protección de Cloud App Security admitida en cada modelo.

Modelo	Requisitos de licencia y pago	Protección de seguridad de aplicaciones en la nube compatible
Modelo A	• Una licencia apropiada de Microsoft 365 E5 • Pago a Microsoft cuando el uso de la API supera el límite superior	• Escanea mensajes y archivos. • Bloquear o pasar mensajes y archivos al detectar riesgos.

Modelo	Requisitos de licencia y pago	Protección de seguridad de aplicaciones en la nube compatible
Modelo B	• Pago a Microsoft por cada llamada a la API • No se requiere licencia	• Escanea mensajes y archivos. • Pasar mensajes y archivos al detectar riesgos. No se admite el bloqueo de mensajes o archivos.
Modo de evaluación	No se requiere licencia ni pago	• Escanea mensajes y archivos. • Bloquear o pasar mensajes y archivos al detectar riesgos. Como este modelo proporciona llamadas API limitadas, Cloud App Security puede escanear y tomar medidas solo en una cantidad limitada de mensajes y archivos.

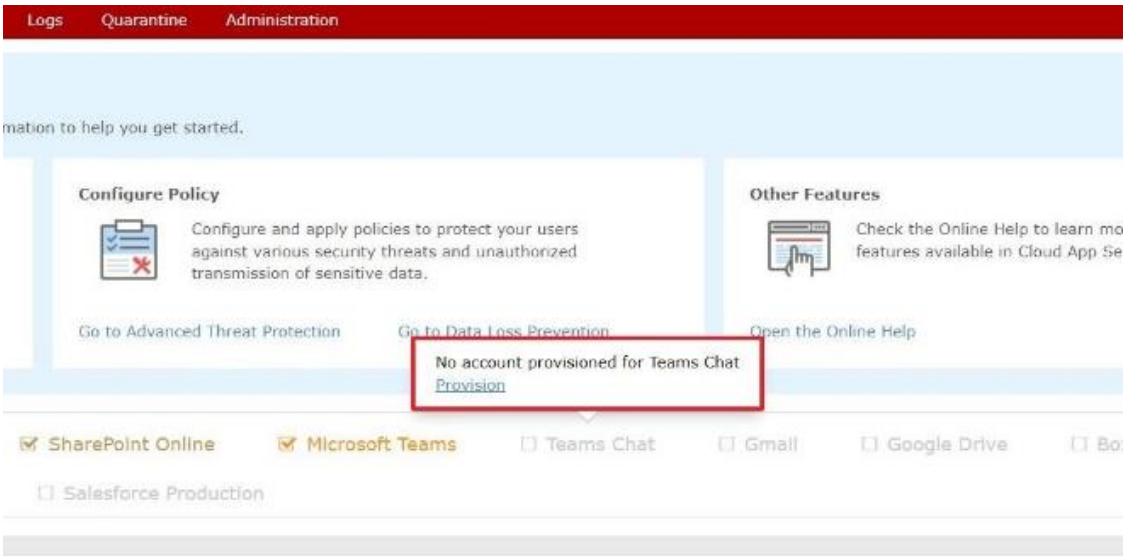
Si ya aprovisionó Teams Chat de la manera anterior sin crear su propia aplicación, se aplica el modo de evaluación. Trend Micro recomienda que actualice el aprovisionamiento para tener acceso a todos los modelos de licencias y la protección continua de Cloud App Security realizando lo siguiente:

Vaya a **Administración** > **Cuenta de servicio** , busque su cuenta de servicio de Teams Chat, haga clic en **Proteger** con su propia aplicación y complete el aprovisionamiento consultando las operaciones de este tema.

Para aprovisionar una cuenta de servicio para Teams Chat desde la consola web de Cloud App Security:

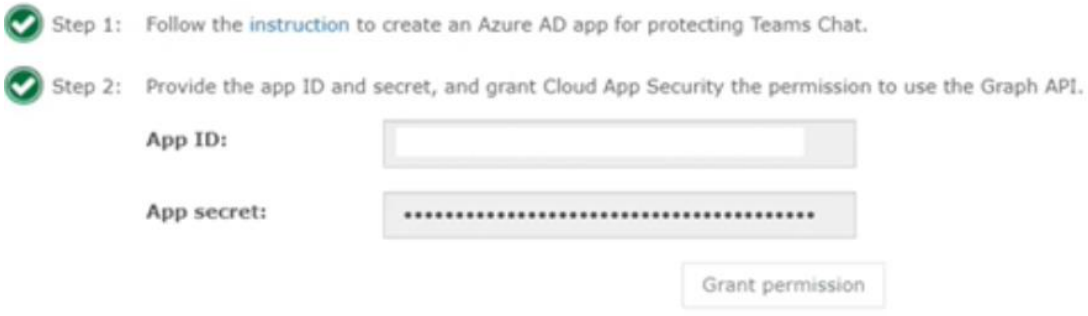
Inicie sesión en la consola de administración de Cloud App Security.

Pase el cursor sobre Teams Chat y haga clic en **Aprovisionar**.



Cree una aplicación en Azure AD para proteger Teams Chat.
Para obtener más información, consulte [Creación de una aplicación de Azure AD para Teams Chat Protection]() .

Especifique el ID y el secreto de la aplicación y haga clic en **Conceder permiso**.

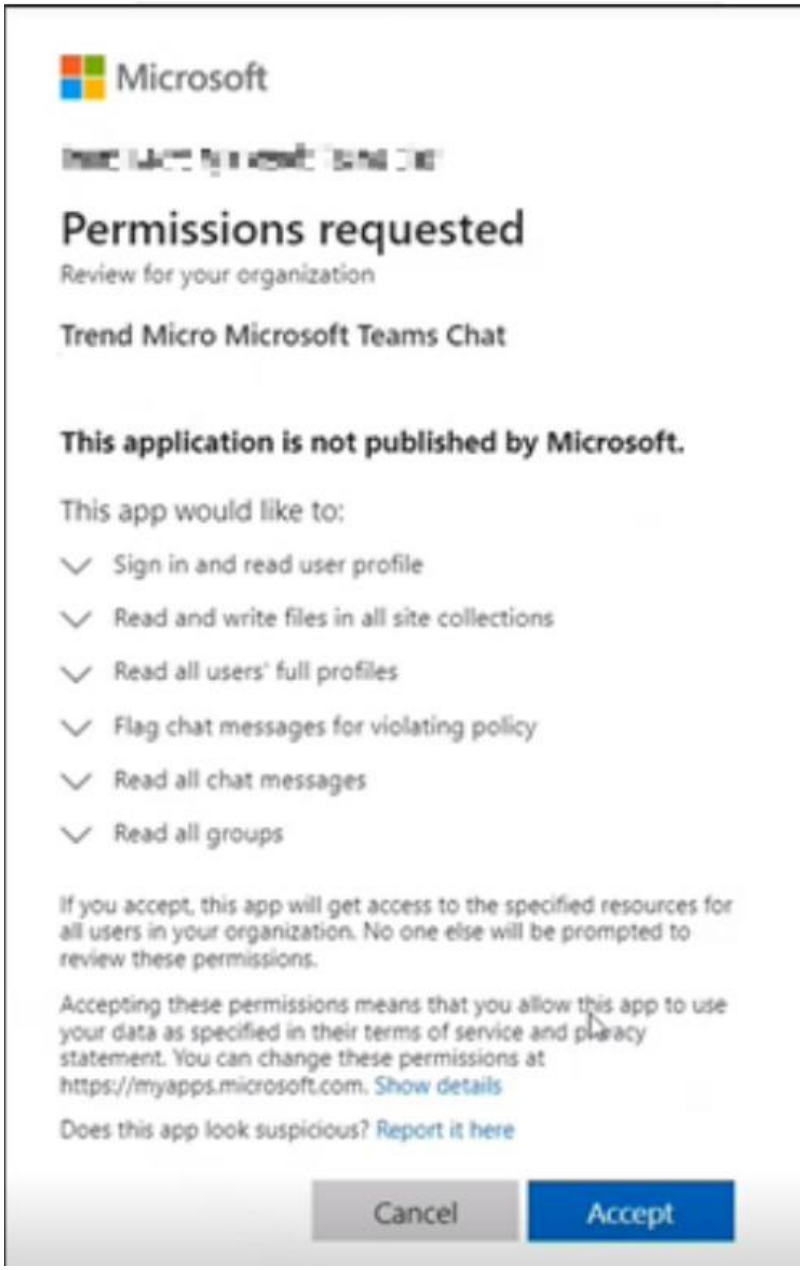


Si por algún motivo el token de acceso deja de ser válido después del aprovisionamiento, vaya a **Administración** > **Cuenta de servicio** para crear un nuevo token de acceso para la cuenta de servicio. Para obtener más información, consulte [Cuenta de servicio]() .

Si el secreto deja de ser válido o desea cambiar a otra aplicación después del aprovisionamiento, vaya a **Administración** > **Cuenta de servicio**, ubique su cuenta de servicio de Teams Chat y haga clic en **Actualizar secreto o Cambiar aplicación** para comenzar a reemplazar el secreto o cambiar a otra aplicación. El procedimiento posterior es el mismo que el aprovisionamiento descrito en este tema.

Especifique sus credenciales de administrador global de Office 365 y haga clic en **Iniciar sesión**.

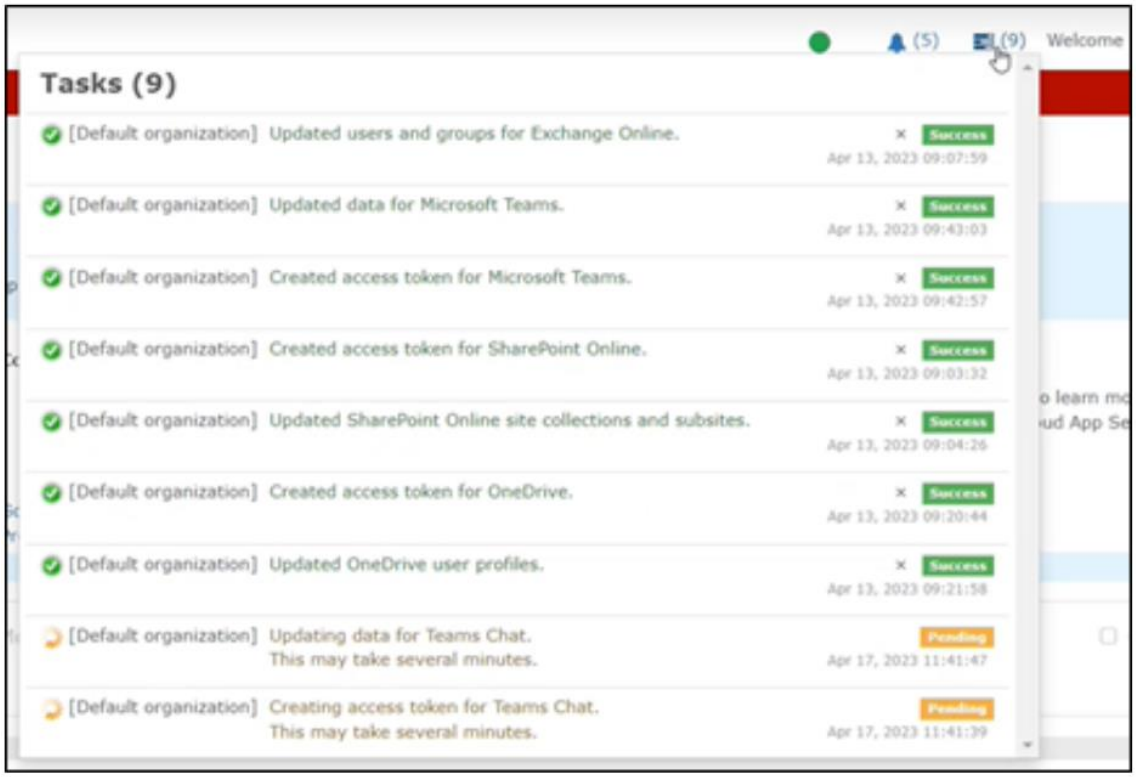
Haga clic en **Aceptar** para otorgar a Cloud App Security el permiso para usar Graph API para acceder a los datos de servicio relacionados con Teams Chat.



Vuelva a la consola de administración de Cloud App Security y seleccione un modelo de licencia de Microsoft.

Para cambiar el modo de protección después del aprovisionamiento, consulte Configuración del modelo de licencias de Microsoft para Teams Chat .

Haga clic en Listo. Cloud App Security luego actualiza los datos de Teams Chat en su organización. El tiempo requerido depende de la cantidad de datos que tenga en Teams Chat.



Pase el cursor sobre el ícono del anillo en la esquina superior derecha de la consola de administración.
Si aparece el mensaje *Teams Chat protected* en la pantalla de notificaciones, el aprovisionamiento se realizó correctamente.