

Contents

Documentación sobre External Identities

Información general

Comparación entre soluciones para External Identities

¿Qué es el acceso de usuarios invitados de B2B?

¿Qué es Azure AD B2C?

Novedades de la documentación

Guías de inicio rápido

Incorporación de usuarios invitados en el portal

Incorporación de usuarios invitados con PowerShell

Tutoriales

Invitación masiva a usuarios invitados mediante PowerShell

Invitación masiva a usuarios invitados mediante Azure Portal

Aplicación de la autenticación multifactor en usuarios invitados

Ejemplos

Ejemplos de registro de autoservicio para usuarios invitados

Ejemplos de Code y Azure PowerShell

Conceptos

Precios de identidades externas

Procedimientos recomendados de B2B

Uso compartido externo de B2B y Office 365

Canje de invitación

Correo electrónico de invitación

Descripción del usuario de B2B

Asignación de notificaciones de usuario de B2B

Token de usuario de B2B

Acceso condicional para B2B

B2B para organizaciones híbridas

Proveedores de identidades para External Identities

Registro de autoservicio de flujos de usuario (versión preliminar)

[Registro de autoservicio de conectores de API \(versión preliminar\)](#)

[Administración de derechos de Azure AD](#)

[Limitaciones actuales](#)

[Guías paso a paso](#)

[Configuración de valores de colaboración externa](#)

[Invitar a usuarios externos](#)

[Adición de usuarios de B2B por los administradores](#)

[Adición de usuarios de B2B por los trabajadores de la información](#)

[Invitación a usuarios internos a B2B](#)

[Permiso o bloqueo de invitaciones](#)

[Incorporación de usuarios B2B sin invitación](#)

[API de invitación y personalización](#)

[Federación con proveedores de identidades](#)

[Federación de Google](#)

[Federación de Facebook](#)

[Federación directa](#)

[Ejemplo de federación directa con AD FS](#)

[Autenticación con código de acceso de un solo uso](#)

[Registro de autoservicio para usuarios invitados \(versión preliminar\)](#)

[Incorporación de un flujo de usuario de registro de autoservicio](#)

[Definición de atributos personalizados](#)

[Personalización del lenguaje del flujo de usuario](#)

[Adición de un conector de API](#)

[Adición de un sistema de aprobación personalizado](#)

[Administración de cuentas de usuario invitado](#)

[Adición de un usuario B2B a un rol](#)

[Grupos dinámicos y usuarios de B2B](#)

[Descripción del usuario de B2B](#)

[Restablecimiento del estado de canje](#)

[B2B para las aplicaciones integradas de Azure AD](#)

[Administración del acceso de invitado en una organización híbrida](#)

[Concesión a los usuarios locales de acceso a las aplicaciones en la nube](#)

[Concesión a los usuarios B2B de acceso a las aplicaciones locales](#)

[Salir de una organización](#)

[Informes y auditoría](#)

[Solución de problemas de B2B](#)

[Referencia](#)

[API del administrador de invitaciones](#)

[Recursos](#)

[Preguntas más frecuentes](#)

[Obtención de soporte técnico](#)

[Foro de comentarios de Azure](#)

[Azure Roadmap](#)

[Página de preguntas y respuestas de Microsoft](#)

[Precios](#)

[Calculadora de precios](#)

[Actualizaciones del servicio](#)

[Stack Overflow](#)

[Vídeos](#)

¿Qué son External Identities de Azure Active Directory?

18/02/2021 • 9 minutes to read • [Edit Online](#)

Mediante External Identities de Azure AD, puede facilitar a personas ajenas a una organización el acceso a sus aplicaciones y recursos, además de permitirles iniciar sesión con la identidad que prefieran. Los asociados, distribuidores, proveedores y otros usuarios invitados pueden "traer sus propias identidades". Tanto si tienen una identidad digital corporativa o emitida por una entidad gubernamental, como si tienen una identidad social no administrada, como Google o Facebook, pueden usar sus propias credenciales para iniciar sesión. El proveedor de identidades administra la identidad del usuario externo y el usuario administra el acceso a sus aplicaciones con Azure AD para mantener protegidos los recursos.

Escenarios de External Identities

Azure AD External Identities se centra menos en la relación de un usuario con su organización y más en la forma en que un usuario quiere iniciar sesión en sus aplicaciones y recursos. Dentro de este marco, Azure AD admite varios escenarios, desde la colaboración de negocio a negocio (B2B) a la administración de accesos para aplicaciones orientadas a consumidores, clientes o ciudadanos (negocio a cliente, o B2C).

- **Uso compartido de aplicaciones y recursos con usuarios externos (colaboración B2B)** . Invite a usuarios externos a su propio inquilino como usuarios "invitados" a los que puede asignar permisos (para autorización) al tiempo que les permite usar sus credenciales existentes (para autenticación). Los usuarios inician sesión en los recursos compartidos con un proceso sencillo de invitación y canje con su cuenta profesional o educativa o con cualquier cuenta de correo electrónico. También puede usar la [administración de derechos de Azure AD](#) para configurar directivas que [administren el acceso para los usuarios externos](#). Y ahora, con la disponibilidad de los [flujos de registro de usuarios en modo de autoservicio \(versión preliminar\)](#), puede permitir que los usuarios externos se registren por sí mismos en las aplicaciones. La experiencia se puede personalizar para permitir el registro con una identidad profesional, educativa o de redes sociales (como Google o Facebook). También puede recopilar información sobre el usuario durante el proceso de registro. Para obtener más información, consulte la [Documentación de Azure AD B2B](#).
- **Cree recorridos del usuario con una solución de administración de identidades de marca blanca para aplicaciones orientadas a consumidores y clientes (Azure AD B2C)** . Si es un negocio o un desarrollador que crea aplicaciones orientadas a clientes, puede escalar a millones de consumidores, clientes o ciudadanos mediante Azure AD B2C. Los desarrolladores pueden usar Azure AD como sistema completo de administración de identidades y acceso de cliente (CIAM) para sus aplicaciones. Los clientes pueden iniciar sesión con una identidad ya establecida (como Facebook o Gmail). Con Azure AD B2C, puede personalizar y controlar el modo en que los clientes se suscriben, inician sesión y administran sus perfiles al usar las aplicaciones. Para obtener más información, consulte la [Documentación de Azure AD B2C](#).

Comparación de las soluciones de External Identities

En la tabla siguiente se proporciona una comparación detallada de los escenarios que se pueden habilitar con Azure AD External Identities.

	COLABORACIÓN DE USUARIO EXTERNO (B2B)	ACCESO A APLICACIONES ORIENTADAS A CONSUMIDORES O CLIENTES (B2C)
Escenario principal	Colaboración mediante aplicaciones de Microsoft (Microsoft 365, Teams, etc.) o sus propias aplicaciones (aplicaciones SaaS, aplicaciones personalizadas, etc.).	Administración de identidades y acceso para aplicaciones SaaS o personalizadas modernas (no aplicaciones propias de Microsoft).
Destinado a	Colaborar con socios comerciales de organizaciones externas como proveedores o asociados. Los usuarios aparecen como usuarios invitados en el directorio. Estos usuarios pueden tener TI administrado o no.	Clientes de su producto. Estos usuarios se administran en un directorio de Azure AD independiente.
Se admiten proveedores de identidades	Los usuarios externos pueden colaborar mediante cuentas profesionales, cuentas educativas, cualquier dirección de correo electrónico, proveedores de identidades basados en SAML y WS-Fed, Gmail y Facebook.	Usuarios consumidores con cuentas de aplicaciones locales (cualquier dirección de correo electrónico o nombre de usuario), diversas identidades admitidas de redes sociales y usuarios con identidades corporativas o emitidas por una entidad gubernamental mediante la federación directa.
Administración de usuarios externos	Los usuarios externos se administran en el mismo directorio que los empleados, pero normalmente se les etiqueta como usuarios invitados. Los usuarios invitados pueden administrarse del mismo modo que los empleados, pueden agregarse a los mismos grupos, etc.	Los usuarios externos se administran en el directorio de Azure AD B2C. Se administran de manera independiente del directorio de asociados y de empleados de la organización (si existe).
Inicio de sesión único (SSO)	se admite SSO en todas las aplicaciones conectadas a Azure AD. Por ejemplo, puede proporcionar acceso a Microsoft 365, o bien a aplicaciones locales y a otras aplicaciones SaaS como Salesforce o Workday.	Se admite el inicio de sesión único para aplicaciones propiedad de los clientes dentro de los inquilinos de Azure AD B2C. No se admite el inicio de sesión único en Microsoft 365 ni en otras aplicaciones SaaS de Microsoft.
Directiva de seguridad y cumplimiento	los administra la organización anfitriona o que realiza la invitación (por ejemplo, con directivas de acceso condicional).	Las administra la organización mediante el acceso condicional y Identity Protection.
Personalización de marca	se utiliza la marca de la organización anfitriona o que realiza la invitación.	Personalización de marca totalmente personalizable por aplicación u organización.
Modelo de facturación	Los precios de las identidades externas se basan en los usuarios activos mensuales (MAU). (Consulte también: Detalles de la configuración B2B)	Los precios de las identidades externas se basan en los usuarios activos mensuales (MAU). (Consulte también: Detalles de la configuración B2C)
Más información	Entrada de blog , Documentación	página de producto , documentación

Proteja y administre los clientes y asociados más allá de los límites organizacionales con Azure AD External Identities.

Acerca de las aplicaciones multiinquilino

Si va a proporcionar una aplicación como servicio y no desea administrar las cuentas de usuario de los clientes, es probable que una aplicación multiinquilino sea la opción más adecuada. Al desarrollar aplicaciones para otros inquilinos de Azure AD, puede dirigirse a usuarios de una única organización (inquilino único) o usuarios de cualquier organización que ya tenga un inquilino de Azure AD (aplicaciones multiinquilino). Los registros de aplicaciones en Azure AD son de inquilino único de forma predeterminada, pero puede hacer que el registro sea multiinquilino. Usted mismo registra una vez la aplicación multiinquilino en su propia instancia de Azure AD. Pero, después, cualquier usuario de Azure AD de cualquier organización puede usar la aplicación sin ningún trabajo adicional por su parte. Para más información, consulte [Administración de identidades en aplicaciones multiinquilino, Guía de procedimientos](#).

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Acerca de Azure AD B2C](#)

¿Qué es el acceso de usuarios invitados en Azure Active Directory B2B?

18/02/2021 • 7 minutes to read • [Edit Online](#)

La colaboración de negocio a negocio (B2B) de Azure Active Directory (Azure AD) es una característica de External Identities que le permite invitar a los usuarios invitados a colaborar con una organización. La colaboración B2B le permite compartir de forma segura las aplicaciones y los servicios de una empresa con los usuarios invitados de cualquier otra organización, al tiempo que mantiene el control sobre sus propios datos corporativos. Trabaje de forma segura con asociados externos, grandes o pequeños, incluso si no tienen Azure AD o un departamento de TI. Un proceso de invitación y canje sencillo permite a los asociados usar sus propias credenciales para acceder a los recursos de su empresa. Los desarrolladores pueden usar las API de negocio a negocio de Azure AD para personalizar el proceso de invitación o escribir aplicaciones como los portales de suscripción de autoservicio. Para obtener información sobre las licencias y los precios relacionados con los usuarios invitados, consulte [Precios de Azure Active Directory](#).

IMPORTANT

- **A partir del 4 de enero de 2021**, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa Google Federation o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).
- **A partir del 31 de marzo de 2021**, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

Colaboración con cualquier asociado mediante sus identidades

Con Azure AD B2B, el asociado utiliza su propia solución de administración de identidades, así que no hay ninguna sobrecarga administrativa externa para su organización. Los usuarios invitados inician sesión en las aplicaciones y los servicios con sus propias identidades profesionales, educativas o sociales.

- El socio utiliza sus propias identidades y credenciales; Azure AD no es necesario.
- No es necesario administrar las cuentas externas o las contraseñas.
- No es necesario sincronizar las cuentas o administrar los ciclos de vida de las cuentas.

Facilidad de la invitación a los usuarios invitados desde el portal de Azure AD

Como administrador, puede agregar fácilmente usuarios invitados a su organización en Azure Portal.

- [Cree un usuario invitado](#) en Azure AD, de forma similar a cómo se agrega un nuevo usuario.
- Asigne los usuarios invitados a las aplicaciones o los grupos.
- Envíe una invitación por correo electrónico que contenga un vínculo de canje o enviar un vínculo directo a una aplicación que desee compartir.

New user

Microsoft

Identity

Email address * ✓

Personal message

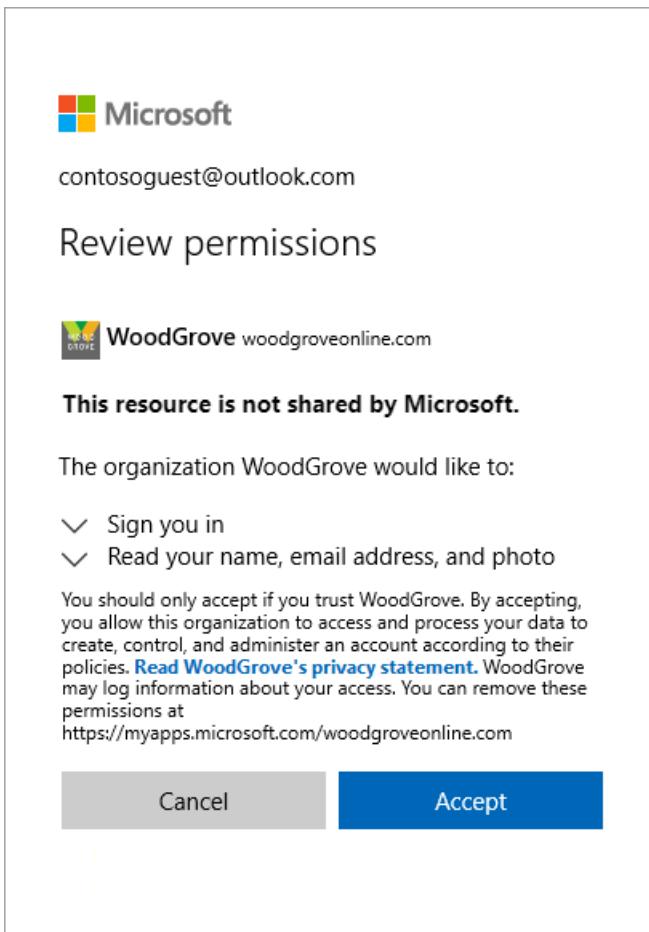
Hello! We're excited to have you with us on the new project.

Accept this invitation and you'll get access to all the apps that you need. Let me know if you have any questions.

Thanks,
Tami Weiss, Contoso administrator

Invite

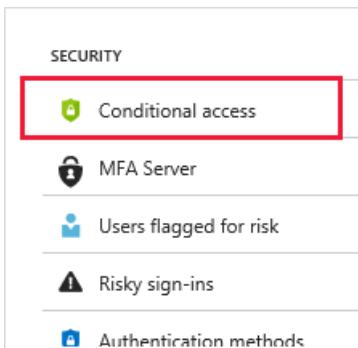
- Los usuarios invitados siguen unos [pasos de canje](#) sencillos para iniciar sesión.



Uso de directivas para compartir de forma segura sus aplicaciones y servicios

Puede usar las directivas de autorización para proteger el contenido corporativo. Las directivas de acceso condicional, como la autenticación multifactor, se pueden aplicar:

- En el nivel de inquilino.
- En el nivel de aplicación.
- A usuarios invitados específicos para proteger los datos y las aplicaciones empresariales.



Permitir que los propietarios de aplicaciones y grupos administren sus propios usuarios invitados

Puede delegar la administración de usuarios invitados a los propietarios de aplicaciones para que puedan agregar usuarios invitados directamente a cualquier aplicación que deseen compartir, ya sea una aplicación de Microsoft o no.

- Los administradores configuran la administración de aplicaciones y grupos de autoservicio.
- Los usuarios no administradores usan su [panel de acceso](#) para agregar usuarios invitados a aplicaciones o grupos.

The screenshot shows the 'Access Panel Applications' page in the Azure portal. It lists various applications such as Box, Concur, G Suite, Groups, GoToMeeting, Jive, Lucidchart, Salesforce, Security & Compli..., and Store. The 'Salesforce' application card is selected, showing options like 'Open' and 'Manage app'. The 'Manage app' button is highlighted with a red box.

Personalización de la experiencia de incorporación de usuarios invitados de B2B

Incorpore a los asociados externos de manera personalizada según las necesidades de su organización.

- Use la [administración de derechos de Azure AD](#) para configurar directivas que [administren el acceso para los usuarios externos](#).
- Use la [API de invitación de colaboración B2B](#) para personalizar las experiencias de incorporación.

Integración con proveedores de identidades

Azure AD admite proveedores de identidades externos (como Facebook), cuentas de Microsoft, Google o proveedores de identidades empresariales. Puede configurar la federación con proveedores de identidades para que los usuarios externos puedan iniciar sesión con sus cuentas empresariales o sociales existentes en lugar de

crear una nueva cuenta solo para la aplicación. Obtenga más información sobre los proveedores de identidades para External Identities.

The screenshot shows the 'External Identities | All identity providers' page. On the left, there's a sidebar with links like 'Get started', 'All identity providers' (which is selected), 'External collaboration settings', 'Diagnose and solve problems', 'Self-service sign up', 'Custom user attributes (Preview)', 'User flows (Preview)', 'Lifecycle management', and 'Terms of use'. The main area has a search bar at the top right with 'Google', 'Facebook', 'New SAML/WS-Fed IdP', and a 'Got feedback?' link. Below that is a note about invited users. Then, there are sections for 'Social identity providers' (with 'Facebook' listed) and 'SAML/WS-Fed identity providers' (with a search bar). At the bottom, there are columns for 'Domain', 'Protocol', and 'Issuer'.

Creación de un flujo de usuario de registro de autoservicio (versión preliminar)

Con un flujo de usuario de registro de autoservicio, puede crear una experiencia de registro para los usuarios externos que quieran tener acceso a sus aplicaciones. Como parte del flujo de registro, puede proporcionar opciones para diferentes proveedores de identidades sociales o empresariales y recopilar información sobre el usuario. Obtenga información sobre el [registro de autoservicio y cómo configurarlo](#).

También puede usar [conectores de API](#) para integrar los flujos de usuarios de registro de autoservicio con sistemas en la nube externos. Puede conectarse con flujos de trabajo de aprobación personalizados, realizar la comprobación de identidades, validar la información proporcionada por el usuario, etc.

The screenshot shows the 'User flows' management interface. On the left, there's a sidebar with 'Overview' (selected), 'Settings' (with 'Identity providers' and 'User attributes' options), 'Customize' (with 'Page layouts' and 'Languages' options), 'Use' (with 'Applications' option), and a 'Delete' button. The main area has a feedback message. Below that are sections for 'Settings' (with 'Identity providers' showing 'Azure Active Directory Sign up' and 'Facebook') and 'Customize' (with 'Page layouts' set to 'Classic').

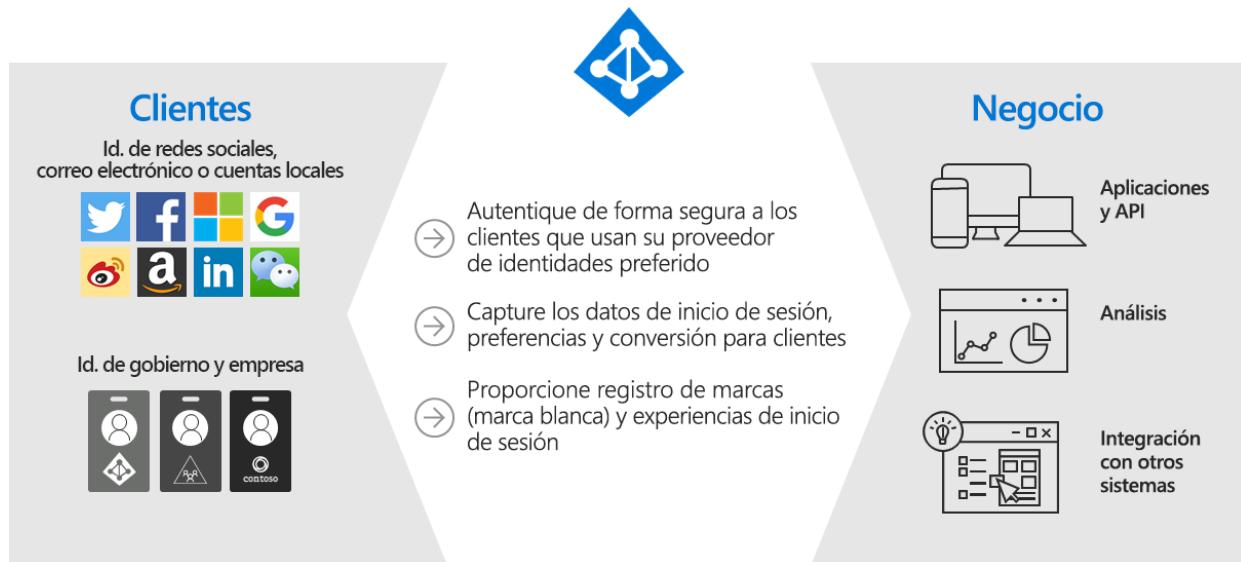
Pasos siguientes

- [Precios de identidades externas](#)
- [Aregar usuarios invitados de colaboración B2B en el portal](#)
- [Información sobre el proceso de canje de invitaciones](#)

¿Qué es Azure Active Directory B2C?

18/02/2021 • 11 minutes to read • [Edit Online](#)

Azure Active Directory B2C proporciona la identidad de negocio a cliente como servicio. Los clientes usan las identidades de la cuenta de redes sociales, corporativa o local preferidas para acceder al inicio de sesión único para sus aplicaciones y API.

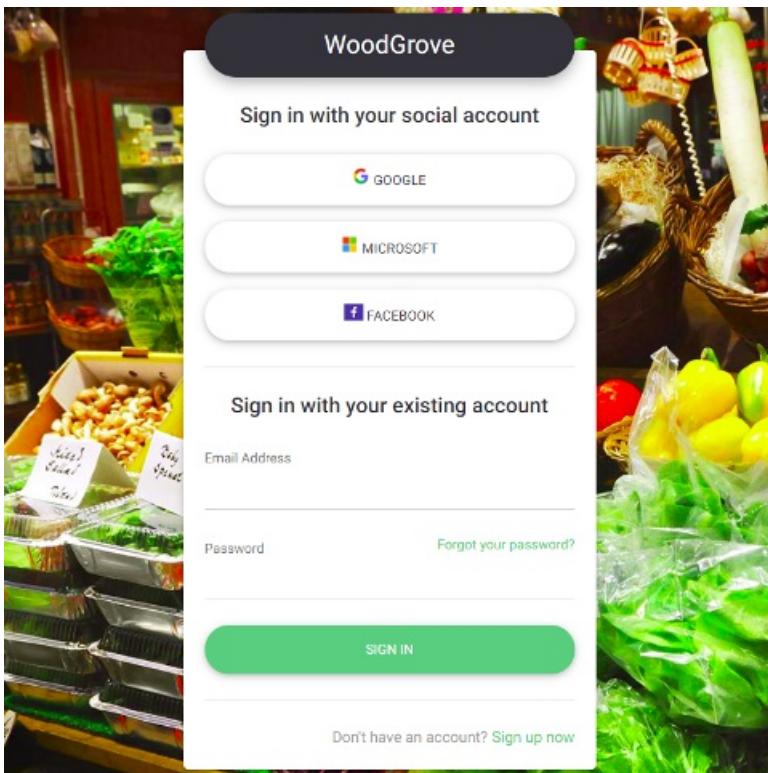


Azure Active Directory B2C (Azure AD B2C) es una solución de administración de acceso de identidades de clientes (CIAM) capaz de admitir millones de usuarios y miles de millones de autenticaciones al día. Se encarga del escalado y la seguridad de la plataforma de autenticación, de la supervisión y del control automático de amenazas, como la denegación de servicio, la difusión de contraseñas o los ataques por fuerza bruta.

Solución de identidad de marca personalizada

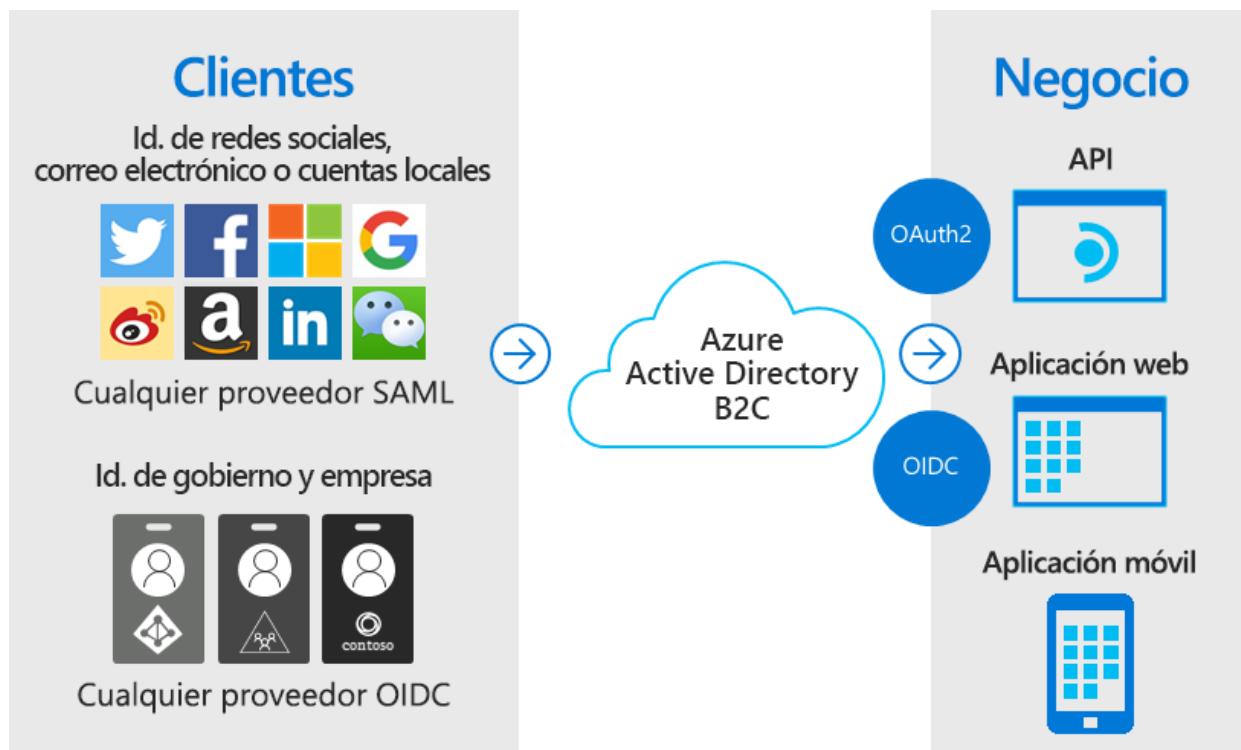
Azure AD B2C es una solución de autenticación de marca blanca. Puede personalizar toda la experiencia del usuario con su marca para que se fusionen sin problemas con las aplicaciones web y móviles.

Personalice todas las páginas mostradas por Azure AD B2C cuando los usuarios se registren, inicien sesión y modifiquen su información de perfil. Personalice el HTML, CSS y JavaScript en los recorridos del usuario para que la experiencia de Azure AD B2C tenga la apariencia de una parte nativa de la aplicación.



Acceso de inicio de sesión único con una identidad proporcionada por el usuario

Azure AD B2C utiliza protocolos de autenticación basados en estándares, como OpenID Connect, OAuth 2.0 y SAML. Se integra con la mayoría de las aplicaciones modernas y el software comercial.

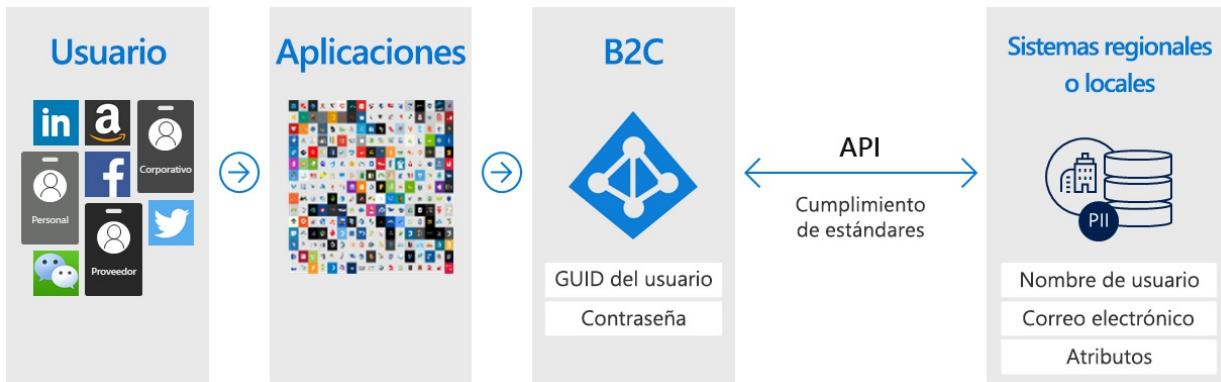


Al actuar como la entidad de autenticación central de las aplicaciones web, las aplicaciones móviles y las API, Azure AD B2C le permite crear una solución de inicio de sesión único (SSO) para todas ellas. Centralice la recopilación de información de perfiles de usuario y preferencias, y capture el análisis detallado sobre el comportamiento de inicio de sesión y la conversión de registros.

Integración con almacenes de usuarios externos

Azure AD B2C proporciona un directorio que puede contener 100 atributos personalizados por usuario. Sin embargo, también puede integrarse con sistemas externos. Por ejemplo, use Azure AD B2C para la autenticación, pero delegue en una base de datos externa de administración de relaciones con el cliente (CRM) o de fidelización de clientes como el origen de veracidad para los datos de los clientes.

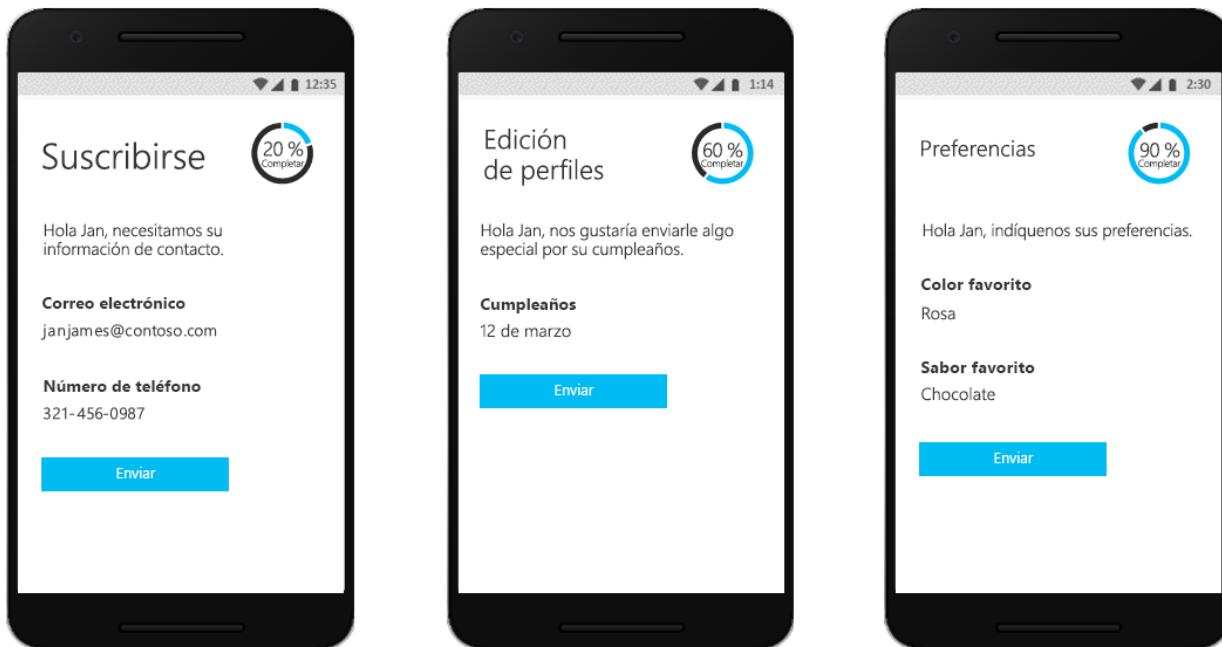
Otro escenario de almacenamiento de usuarios externo consiste en que Azure AD B2C se encargue de la autenticación de la aplicación, pero se integre con un sistema externo que almacena el perfil de usuario o los datos personales. Por ejemplo, para satisfacer los requisitos de residencia de datos, como las directivas de almacenamiento de datos regionales o locales.



Azure AD B2C puede facilitar la recopilación de la información del usuario durante el registro o la edición de perfiles y, a continuación, colocar los datos en el sistema externo. Después, durante las autenticaciones futuras, Azure AD B2C puede recuperar los datos del sistema externo y, si es necesario, incluirlos como parte de la respuesta del token de autenticación que envía a la aplicación.

Generación de perfiles progresiva

Otra opción de recorrido del usuario incluye la generación de perfiles progresiva. La generación de perfiles progresiva permite a los clientes completar rápidamente la primera transacción mediante la recopilación de una cantidad mínima de información. Posteriormente, se recopilarán gradualmente más datos de perfil del cliente en los inicios de sesión futuros.



Comprobación y prueba de identidades de terceros

Use Azure AD B2C para facilitar la comprobación de identidades y su prueba mediante la recopilación de datos

de usuario y, después, pasarlos a un sistema de terceros para realizar la validación, la puntuación de confianza y la aprobación para la creación de cuentas de usuario.



Estas son solo algunas de las cosas que puede hacer con Azure AD B2C como plataforma de identidad de negocio a cliente. Las siguientes secciones de esta información general le guiarán por una aplicación de demostración que usa Azure AD B2C. También va a pasar directamente a una [introducción general técnica más detallada de Azure AD B2C](#).

Ejemplo: WoodGrove Groceries

[WoodGrove Groceries](#) es una aplicación web activa creada por Microsoft para mostrar varias características de Azure AD B2C. En las siguientes secciones se van a revisar algunas de las opciones de autenticación proporcionadas por Azure AD B2C al sitio web de WoodGrove.

Información general empresarial

WoodGrove es una tienda de comestibles en línea que vende comestibles tanto a clientes individuales como a clientes empresariales. Los clientes empresariales compran los comestibles en nombre de la empresa u organizaciones que administran.

Opciones de inicio de sesión

WoodGrove Groceries ofrece varias opciones de inicio de sesión basadas en la relación que tienen sus clientes con la tienda:

- Los clientes **individuales** pueden registrarse o iniciar sesión con cuentas individuales, como un proveedor de identidades de redes sociales o una dirección de correo electrónico y una contraseña.
- Los clientes **empresariales** pueden registrarse o iniciar sesión con las credenciales de empresa.
- Los **asociados** y proveedores son usuarios que suministran a la tienda de comestibles productos para su venta. La identidad del asociado la proporciona [Azure Active Directory B2B](#).

WoodGrove Groceries

Sign in

Language
Choose language

Individual customers
Order your fresh groceries with WoodGrove Groceries and our friendly drivers will deliver your grocery shopping to your home door.

Business customers
Order your fresh groceries with WoodGrove Groceries and our friendly drivers will deliver your grocery shopping to your office door.

Business partners
Manage your local produce in our inventory so we can deliver your fresh groceries to our customers.

[SIGN IN WITH YOUR PERSONAL ACCOUNT](#)

[SIGN UP WITH YOUR PERSONAL ACCOUNT](#)

[SIGN IN WITH YOUR WORK ACCOUNT](#)

[SIGN UP WITH YOUR WORK ACCOUNT](#)

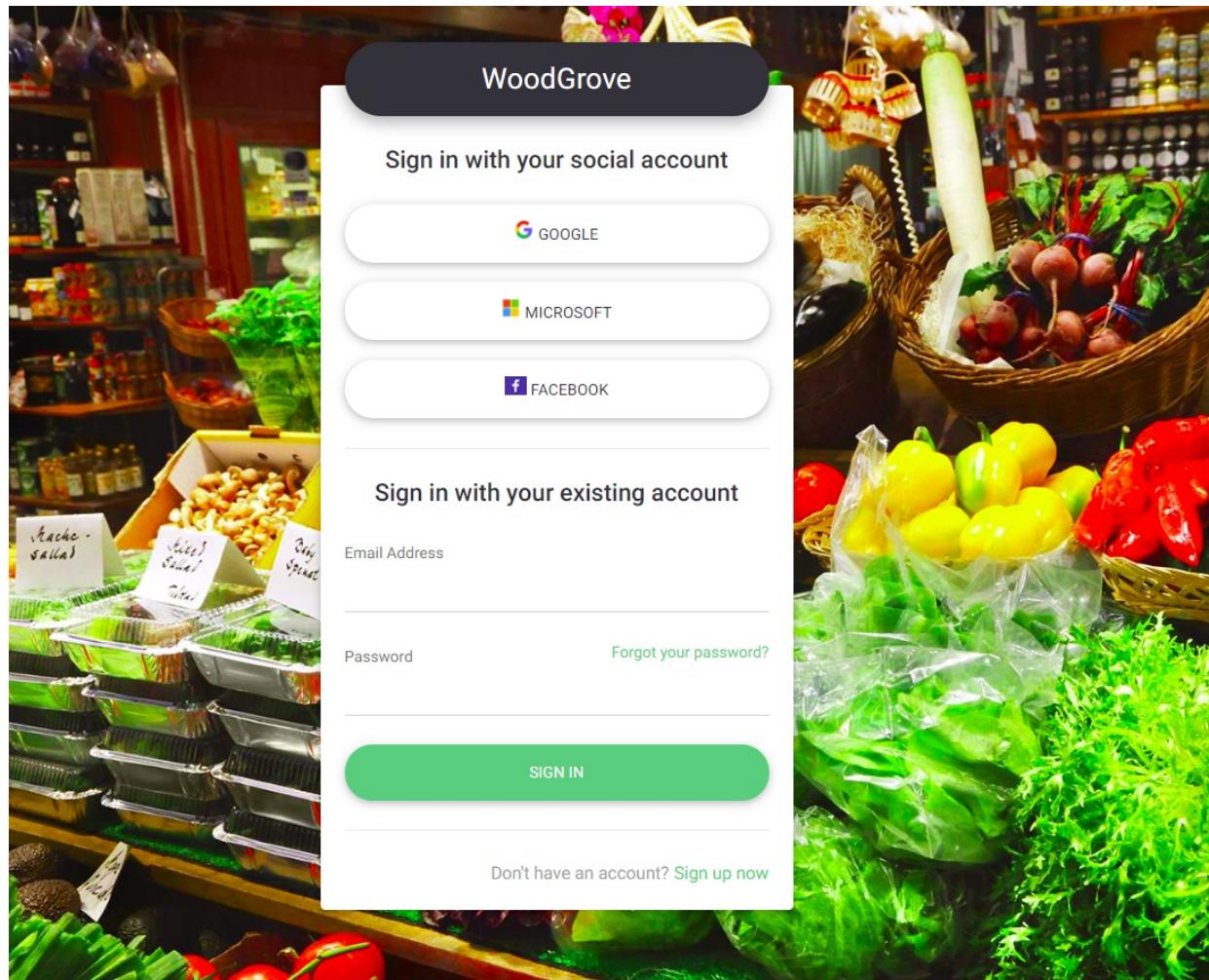
[SIGN IN WITH YOUR SUPPLIER ACCOUNT](#)

[SIGN UP TO BE A WOODGROVE SUPPLIER](#)



Autenticación de clientes individuales

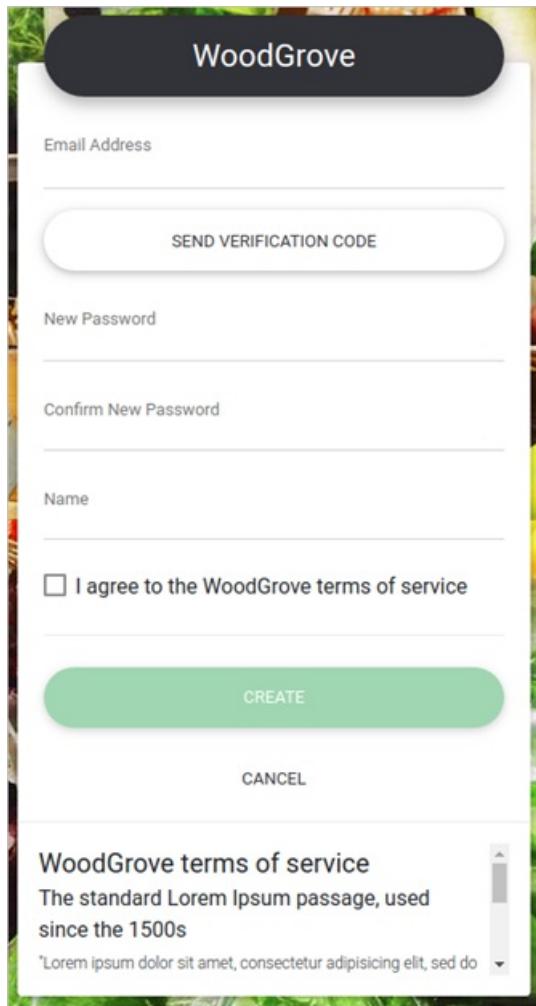
Cuando un cliente selecciona **Inicie sesión con su cuenta personal**, se le redirige a una página de inicio de sesión personalizada hospedada por Azure AD B2C. Puede ver en la siguiente imagen que hemos personalizado la interfaz de usuario para que se parezca al sitio web de WoodGrove Groceries. Los clientes de WoodGrove no deberían notar que la experiencia de autenticación está hospedada y protegida por Azure AD B2C.



WoodGrove permite a sus clientes registrarse e iniciar sesión con sus cuentas de Google, Facebook o Microsoft como proveedor de identidades. O bien, pueden registrarse con su dirección de correo electrónico y una

contraseña para crear lo que se denomina una *cuenta local*.

Cuando un cliente selecciona **Regístrate con su cuenta personal** y, después, **Registrarse ahora**, se le presenta una página de registro personalizada.



Después de escribir una dirección de correo electrónico y seleccionar **Enviar código de verificación**, Azure AD B2C le envía el código. Cuando escriba el código, seleccione **Verificar código** y, después, escriba la otra información en el formulario, que también debe aceptar los términos de servicio.

Al hacer clic en el botón **Crear**, Azure AD B2C redirige al usuario al sitio web de WoodGrove Groceries. Cuando se redirige, Azure AD B2C pasa un token de autenticación de OpenID Connect a la aplicación web de WoodGrove. El usuario ya ha iniciado sesión y está preparado, y su nombre para mostrar aparece en la esquina superior derecha para indicar que está conectado.

A screenshot of the WoodGrove Groceries website's header. It features the brand name "WoodGrove Groceries" on the left, a "Catálogo" button in the center, a "Carro" (Cart) icon with the number "0" to its left, and a user profile dropdown menu on the right showing the name "Ellen Adams - Cliente individual". Below the header is a dark navigation bar with the "Catálogo" button on the left and a "Buscar" (Search) input field on the right.

Autenticación de los clientes empresariales

Cuando un cliente selecciona una de las opciones en **Business customers** (Clientes empresariales), el sitio web de WoodGrove Groceries invoca una directiva de Azure AD B2C diferente a la de los clientes individuales.

Esta directiva presenta al usuario una opción para usar sus credenciales corporativas para el registro y el inicio de sesión. En el ejemplo de WoodGrove, se pide a los usuarios que inicien sesión con cualquier cuenta profesional o educativa. Esta directiva usa una [aplicación de Azure AD multiinquilino](#) y el punto de conexión de Azure AD `/common` para federar Azure AD B2C con cualquier cliente de Microsoft 365 del mundo.

Autenticación de asociados

El vínculo **Sign in with your supplier account** (Inicie sesión con su cuenta de proveedor) usa la funcionalidad de colaboración de Azure Active Directory B2B. Azure AD B2B es una familia de características de Azure Active Directory para administrar las identidades de los asociados. Esas identidades se pueden federar desde Azure Active Directory para el acceso a aplicaciones protegidas mediante Azure AD B2C.

Para más información sobre Azure AD B2B, consulte [¿Qué es el acceso de usuarios invitados en Azure Active Directory B2B?](#).

Pasos siguientes

Ahora que tiene una idea de lo que es Azure AD B2C y algunos de los escenarios en los que puede ayudar, profundice un poco más en sus características y aspectos técnicos.

[Información general técnica de Azure AD B2C >](#)

Identidades externas de Azure Active Directory: Novedades

18/02/2021 • 4 minutes to read • [Edit Online](#)

Estas son las novedades en la documentación de las identidades externas de Azure Active Directory. En este artículo se enumeran los documentos nuevos que se han agregado y los que han tenido actualizaciones importantes en los últimos tres meses. Para conocer las novedades del servicio de identidades externas, consulte [Novedades de Azure Active Directory](#).

Enero de 2021

Artículos actualizados

- [Permitir o bloquear invitaciones a los usuarios de B2B de organizaciones específicas](#)
- [¿Cómo pueden los usuarios de la organización invitar a usuarios invitados a una aplicación?](#)

Diciembre de 2020

Artículos actualizados

- [Preguntas más frecuentes acerca de la colaboración B2B de Azure Active Directory](#)
- [Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B](#)
- [Proveedores de identidades para External Identities](#)
- [Canje de invitación de colaboración B2B de Azure Active Directory](#)
- [Adición de un conector de API a un flujo de usuario](#)
- [Adición de un flujo de trabajo de aprobaciones personalizado al registro de autoservicio](#)
- [Solución de problemas de colaboración B2B de Azure Active Directory](#)
- [¿Qué es el acceso de usuarios invitados en Azure Active Directory B2B?](#)
- [Procedimientos recomendados de Azure Active Directory B2B](#)
- [Habilitación de la colaboración externa B2B y administración de quién puede invitar a otros usuarios](#)
- [Autenticación con código de acceso de un solo uso por correo electrónico](#)

Noviembre de 2020

Artículos actualizados

- [Uso compartido externo de Microsoft 365 y colaboración B2B de Azure Active Directory \(Azure AD\)](#)
- [Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube mediante la colaboración B2B de Azure AD](#)
- [Propiedades de un usuario de colaboración B2B de Azure Active Directory](#)

Octubre de 2020

Artículos actualizados

- [Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B](#)
- [¿Cómo pueden los usuarios de la organización invitar a usuarios invitados a una aplicación?](#)
- [Permitir o bloquear invitaciones a los usuarios de B2B de organizaciones específicas](#)
- [Preguntas más frecuentes acerca de la colaboración B2B de Azure Active Directory](#)

- [Documentación sobre External Identities](#)
- [Canje de invitación de colaboración B2B de Azure Active Directory](#)
- [Adición de un flujo de trabajo de aprobaciones personalizado al registro de autoservicio](#)
- [¿Qué son External Identities de Azure Active Directory?](#)
- [Adición de un conector de API a un flujo de usuario](#)

Septiembre de 2020

Artículos actualizados

- [Elementos del correo electrónico de invitación para la colaboración B2B: Azure Active Directory](#)
- [Solución de problemas de colaboración B2B de Azure Active Directory](#)
- [Modelo de facturación para Azure AD for External Identities](#)
- [Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B](#)

Agosto de 2020

Artículos nuevos

- [Modelo de facturación para Azure AD for External Identities](#)

Artículos actualizados

- [Habilitación de la colaboración externa B2B y administración de quién puede invitar a otros usuarios](#)
- [Adición de un conector de API a un flujo de usuario](#)
- [Adición de un flujo de trabajo de aprobaciones personalizado al registro de autoservicio](#)

Inicio rápido: Incorporación de usuarios invitados a su directorio en Azure Portal

18/02/2021 • 6 minutes to read • [Edit Online](#)

Puede invitar a alguien para colaborar con su organización incorporándolo a su directorio como usuario invitado. A continuación, puede enviar una invitación por correo electrónico que contenga un vínculo de canje o enviar un vínculo directo a una aplicación que desea compartir. Los usuarios invitados inician sesión con su identidad profesional, educativa o social. Junto con este inicio rápido, puede obtener más información sobre cómo agregar usuarios invitados [en Azure Portal](#), a través de [PowerShell](#) o de forma masiva.

En este inicio rápido, agregará un nuevo usuario invitado al directorio de Azure AD a través de Azure Portal, enviará una invitación y verá la apariencia del proceso de canje de la invitación del usuario invitado.

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

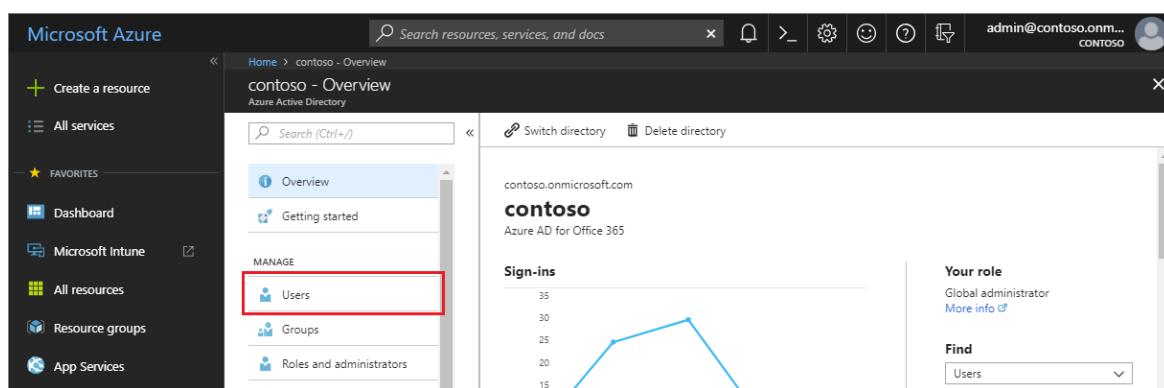
Requisitos previos

Para completar el escenario de este tutorial, necesita:

- Un rol que le permite crear usuarios en el directorio de inquilino, como el rol de administrador global o cualquiera de los roles de directorio de administrador limitado.
- Una cuenta de correo electrónico válida que puede agregar a su directorio de inquilino y que puede usar para recibir el correo electrónico de invitación de prueba.

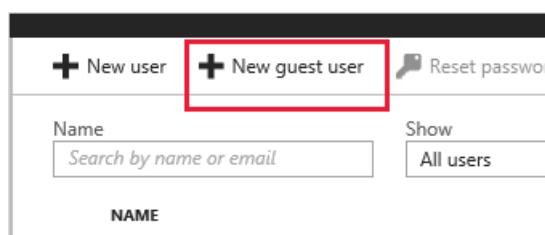
Incorporación de un nuevo usuario invitado en Azure AD

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En el panel izquierdo, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Usuarios**.



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with options like 'Create a resource', 'All services', 'FAVORITES' (which includes 'Dashboard', 'Microsoft Intune', 'All resources', 'Resource groups', and 'App Services'), and 'Create a resource'. The main content area is titled 'contoso - Overview' under 'Azure Active Directory'. It features a search bar at the top right. Below the search bar, there are sections for 'Overview' (with a blue background), 'Getting started', and 'MANAGE' (with a red box around the 'Users' option). To the right, there's a 'Sign-ins' chart showing activity over time, and a 'Your role' section indicating 'Global administrator'. At the bottom right, there's a 'Find' bar set to 'Users'.

4. Seleccione **Nuevo usuario invitado**.



The screenshot shows the 'New user' creation form. At the top, there are two buttons: '+ New user' and '+ New guest user' (which is highlighted with a red box). Below these are fields for 'Name' (with a placeholder 'Search by name or email') and 'Show' (with a dropdown menu showing 'All users'). At the bottom, there's a large input field labeled 'NAME'.

5. En la página **Nuevo usuario**, seleccione **Invitar usuario** y, después, agregue la información del usuario invitado.

- **Nombre**. Nombre y apellidos del nuevo usuario.
- **Dirección de correo (obligatorio)**. La dirección de correo del usuario invitado.
- **Mensaje personal (opcional)** Incluye un mensaje de bienvenida personal al usuario invitado.
- **Grupos**: Puede agregar al usuario invitado a uno o varios de los grupos existentes, o puede hacerlo después.
- **Rol del directorio**. Si necesita permisos administrativos de Azure AD para el usuario, puede agregarlos a un rol de Azure AD.

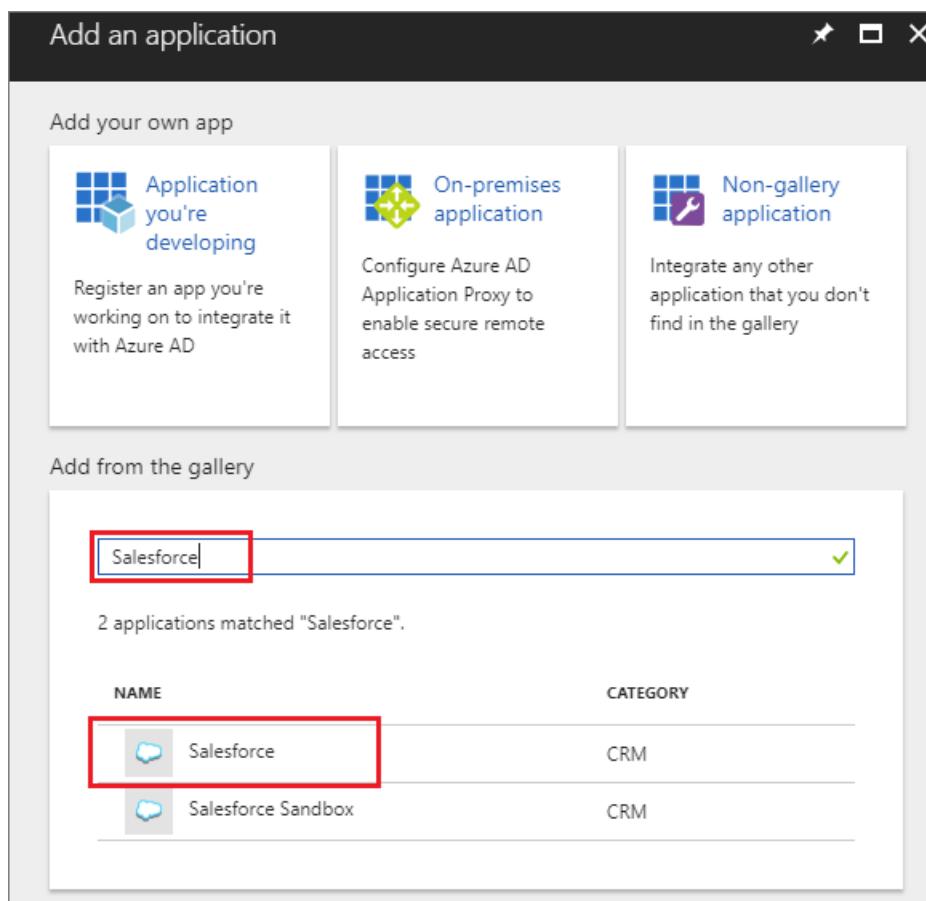
6. Seleccione **Invitar** para enviar automáticamente la invitación al usuario invitado. Aparece una notificación en la esquina superior derecha con el mensaje **Usuario invitado correctamente**.

7. Después de enviar la invitación, la cuenta de usuario se agrega automáticamente al directorio como invitado.

Asignación de una aplicación al usuario invitado

Agregue la aplicación de Salesforce a su inquilino de prueba y asigne el usuario invitado de prueba a la aplicación.

1. Inicie sesión en Azure Portal como administrador de Azure AD.
2. En el panel izquierdo, seleccione **Aplicaciones empresariales**.
3. Seleccione **Nueva aplicación**.
4. En **Agregar desde la galería**, busque **Salesforce** y después selecciónelo.



5. Seleccione **Agregar**.

6. En **Administrar**, seleccione **Inicio de sesión único** y, en **Modo de inicio de sesión único**, seleccione

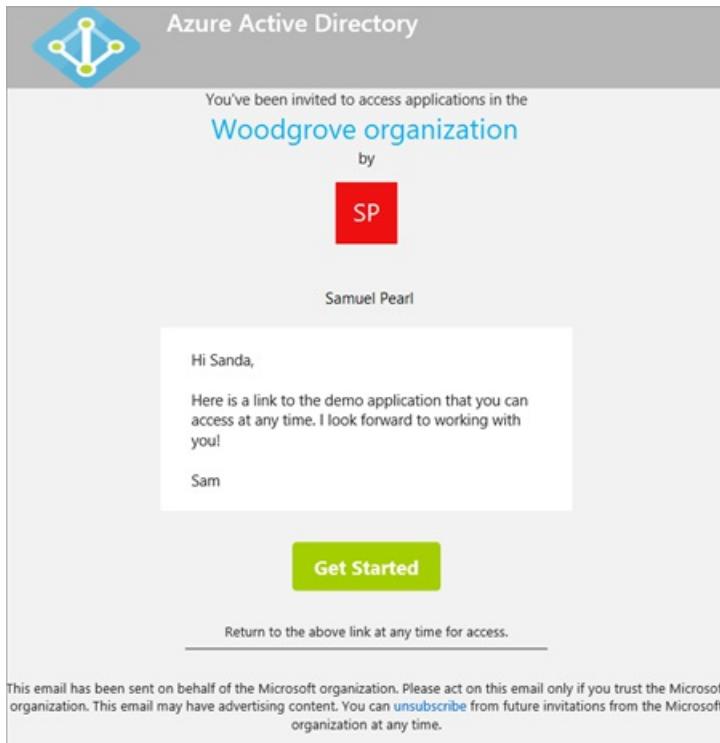
Inicio de sesión con contraseña y haga clic en **Guardar**.

7. En **Administrar**, seleccione **Usuarios y grupos** > **Agregar usuario** > **Usuarios y grupos**.
8. Utilice el cuadro de búsqueda para buscar el usuario de prueba (si es necesario) y seleccione el usuario de prueba en la lista. Despues, haga clic en **Seleccionar**.
9. Seleccione **Asignar**.

Aceptar la invitación

Ahora inicie sesión como usuario invitado para ver la invitación.

1. Inicie sesión en la cuenta de correo electrónico del usuario invitado de prueba.
2. En su Bandeja de entrada, busque el correo electrónico "Está invitado".



3. En el cuerpo del correo electrónico, seleccione **Comenzar**. Se abre una página **Revisar permisos** en el explorador.



contosoguest@outlook.com

Review permissions



WoodGrove woodgroveonline.com

This resource is not shared by Microsoft.

The organization WoodGrove would like to:

- ✓ Sign you in
- ✓ Read your name, email address, and photo

You should only accept if you trust WoodGrove. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. [Read WoodGrove's privacy statement](#). WoodGrove may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/woodgroveonline.com>

Cancel

Accept

4. Seleccione **Aceptar**. Se abre el panel de acceso, donde se enumeran las aplicaciones a las que el usuario invitado puede acceder.

Limpieza de recursos

Cuando ya no sea necesario, elimine el usuario invitado de prueba y la aplicación de prueba.

1. Inicie sesión en Azure Portal como administrador de Azure AD.
2. En el panel izquierdo, seleccione Azure Active Directory.
3. En **Administrar**, seleccione **Aplicaciones empresariales**.
4. Abra la aplicación **Salesforce** y luego seleccione **Eliminar**.
5. En el panel izquierdo, seleccione Azure Active Directory.
6. En **Administrar**, seleccione **Usuarios**.
7. Seleccione el usuario de prueba y después **Eliminar usuario**.

Pasos siguientes

En este tutorial, creó un usuario invitado en Azure Portal y envió una invitación para compartir aplicaciones. Después pudo ver el proceso de canje desde la perspectiva del usuario de prueba y verificó que la aplicación aparecía en el panel de acceso del usuario invitado. Para más información sobre cómo agregar usuarios invitados para la colaboración, vea [Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#).

Inicio rápido: Incorporación de un usuario invitado con PowerShell

18/02/2021 • 5 minutes to read • [Edit Online](#)

Hay muchas maneras de invitar a los asociados externos a sus aplicaciones y servicios con la colaboración de Azure Active Directory B2B. En el tutorial anterior, vimos cómo agregar usuarios invitados directamente en el portal de administración de Azure Active Directory. También puede usar PowerShell para agregar usuarios invitados, uno a uno o de forma masiva. En este tutorial, usará el comando `New-AzureADMSInvitation` para agregar un usuario invitado a su inquilino de Azure.

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Prerrequisitos

Instalación del último módulo de AzureADPreview

Asegúrese de que instala la última versión de Azure AD PowerShell para el módulo Graph (AzureADPreview).

En primer lugar, compruebe qué módulos ha instalado. Abra Windows PowerShell como un usuario con privilegios elevados (Ejecutar como administrador) y ejecute el comando siguiente:

```
Get-Module -ListAvailable AzureAD*
```

Si se muestra el módulo AzureADPreview sin ningún mensaje que indica que hay una versión posterior, significa que está listo. De lo contrario, en función de la salida, realice una de las siguientes acciones:

- Si no se devuelve ningún resultado, ejecute el siguiente comando para instalar el módulo AzureADPreview:

```
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureAD en los resultados, ejecute los comandos siguientes para instalar el módulo AzureADPreview:

```
Uninstall-Module AzureAD  
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureADPreview en los resultados, pero recibe un mensaje que indica que hay una versión posterior, ejecute los comandos siguientes para actualizar el módulo:

```
Uninstall-Module AzureADPreview  
Install-Module AzureADPreview
```

Puede que reciba un mensaje que indica que está instalando el módulo desde un repositorio de confianza. Esto se produce si el repositorio de PSGallery no se ha establecido previamente como un repositorio de confianza. Presione Y para instalar el módulo.

Obtención de una cuenta de correo electrónico de prueba

Necesita una cuenta de correo electrónico de prueba a la que poder enviar la invitación. La cuenta debe estar

fueras de su organización. Puede usar cualquier tipo de cuenta, incluida una cuenta social como una dirección de gmail.com o outlook.com.

Inicio de sesión en su inquilino

Ejecute el siguiente comando para conectarse al dominio del inquilino:

```
Connect-AzureAD -TenantDomain "<Tenant_Domain_Name>"
```

Por ejemplo, `Connect-AzureAD -TenantDomain "contoso.onmicrosoft.com"`.

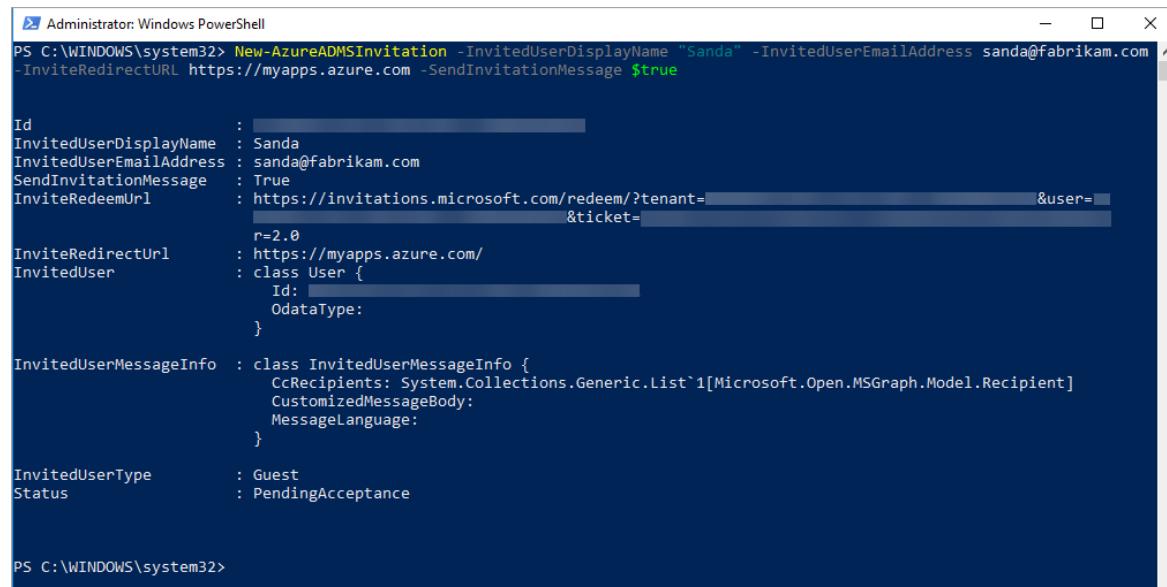
Cuando se le solicite, escriba las credenciales.

Envío de una invitación

1. Para enviar una invitación a su cuenta de correo electrónico de prueba, ejecute el siguiente comando de PowerShell (reemplace "Sanda" y `sanda@fabrikam.com` por la dirección de correo electrónico y el nombre de la cuenta de correo electrónico de prueba):

```
New-AzureADMSInvitation -InvitedUserDisplayName "Sanda" -InvitedUserEmailAddress sanda@fabrikam.com -  
InviteRedirectURL https://myapps.microsoft.com -SendInvitationMessage $true
```

2. El comando envía una invitación a la dirección de correo electrónico especificada. Consulte la salida, que debería ser similar a la siguiente:



```
PS C:\WINDOWS\system32> New-AzureADMSInvitation -InvitedUserDisplayName "Sanda" -InvitedUserEmailAddress sanda@fabrikam.com -  
-InviteRedirectURL https://myapps.azure.com -SendInvitationMessage $true

Id : [REDACTED]
InvitedUserDisplayName : Sanda
InvitedUserEmailAddress : sanda@fabrikam.com
SendInvitationMessage : True
InviteRedeemUrl : https://invitations.microsoft.com/redeem/?tenant=[REDACTED]&user=[REDACTED]&ticket=[REDACTED]&r=2.0
InviteRedirectUrl : https://myapps.azure.com/
InvitedUser : class User {
    Id : [REDACTED]
    OdataType:
}

InvitedUserMessageInfo : class InvitedUserMessageInfo {
    CcRecipients: System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.Recipient]
    CustomizedMessageBody:
    MessageLanguage:
}

InvitedUserType : Guest
Status : PendingAcceptance

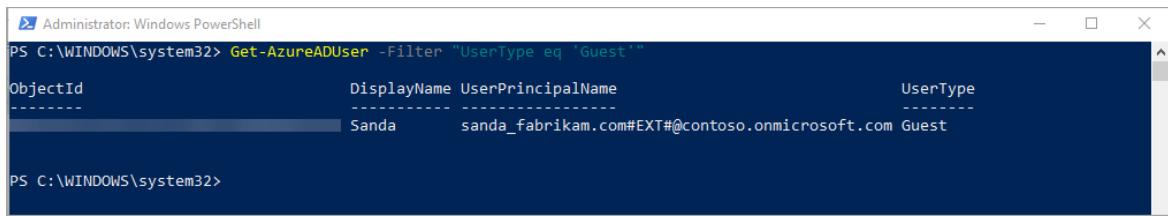
PS C:\WINDOWS\system32>
```

Verificación de la existencia del usuario en el directorio

1. Para verificar que se agregó el usuario invitado a Azure AD, ejecute el siguiente comando:

```
Get-AzureADUser -Filter "UserType eq 'Guest'"
```

2. Consulte la salida para asegurarse de que el usuario invitado aparece en la lista, con un nombre principal de usuario (UPN) con el formato `emailaddress#EXT#@domain`. Por ejemplo, `sanda_fabrikam.com#EXT#@contoso.onmicrosoft.com`, donde contoso.onmicrosoft.com es la organización desde la que se enviaron las invitaciones.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-AzureADUser -Filter "UserType eq 'Guest'"
ObjectID          DisplayName UserPrincipalName          UserType
-----          -----
Sanda           sanda_fabrikam.com#EXT#@contoso.onmicrosoft.com Guest

PS C:\WINDOWS\system32>
```

Limpieza de recursos

Cuando ya no sea necesaria, puede eliminar la cuenta de usuario de prueba del directorio. Ejecute el siguiente comando para eliminar una cuenta de usuario:

```
Remove-AzureADUser -ObjectId "<UPN>"
```

Por ejemplo: `Remove-AzureADUser -ObjectId "sanda_fabrikam.com#EXT#@contoso.onmicrosoft.com"`

Pasos siguientes

En este tutorial, invitó y agregó a un único usuario invitado a su directorio con PowerShell. A continuación, obtenga información sobre cómo invitar a usuarios en masa mediante PowerShell.

[Tutorial: Invitación en masa a usuarios de colaboración de Azure AD B2B](#)

Tutorial: Uso de PowerShell para invitar en bloque a usuarios de colaboración de Azure AD B2B

18/02/2021 • 6 minutes to read • [Edit Online](#)

Si usas la colaboración de Azure Active Directory (Azure AD) B2B para trabajar con asociados externos, puede invitar a varios usuarios a su organización al mismo tiempo. En este tutorial, obtendrá información sobre cómo usar PowerShell para enviar invitaciones de forma masiva a usuarios externos. En particular, haga lo siguiente:

- Prepare un archivo de valores separados por comas (.csv) con la información de usuario.
- Ejecute un script de PowerShell para enviar invitaciones.
- Verifique si los usuarios se agregaron al directorio.

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Prerrequisitos

Instalación del último módulo de AzureADPreview

Asegúrese de que instala la última versión de Azure AD PowerShell para el módulo Graph (AzureADPreview).

En primer lugar, compruebe qué módulos ha instalado. Abra Windows PowerShell como un usuario con privilegios elevados (Ejecutar como administrador) y ejecute el comando siguiente:

```
Get-Module -ListAvailable AzureAD*
```

En función de la salida, realice una de las siguientes acciones:

- Si no se devuelve ningún resultado, ejecute el siguiente comando para instalar el módulo AzureADPreview:

```
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureAD en los resultados, ejecute los comandos siguientes para instalar el módulo AzureADPreview:

```
Uninstall-Module AzureAD
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureADPreview en los resultados, pero recibe un mensaje que indica que hay una versión posterior, ejecute los comandos siguientes para actualizar el módulo:

```
Uninstall-Module AzureADPreview
Install-Module AzureADPreview
```

Puede recibir un mensaje que indica que está instalando el módulo desde un repositorio de confianza. Esto se produce si el repositorio de PSGallery no se ha establecido previamente como un repositorio de confianza. Presione Y para instalar el módulo.

Obtención de cuentas de correo electrónico de prueba

Necesita dos o más cuentas de correo electrónico de prueba a las que poder enviar las invitaciones. Las cuentas deben estar fuera de su organización. Puede usar cualquier tipo de cuenta, incluidas las cuentas sociales como las direcciones de gmail.com o outlook.com.

Preparación del archivo .csv

En Microsoft Excel, cree un archivo .csv con la lista de nombres de usuarios invitados y las direcciones de correo electrónico. Asegúrese de incluir los encabezados de columna **Nombre** e **InvitedUserEmailAddress**.

Por ejemplo, cree una hoja de cálculo con el formato siguiente:

	A	B
1	Name	InvitedUserEmailAddress
2	Lucy Stokes	lstokes@fabrikam.com
3	FirstName LastName	username@outlook.com
4	FirstName LastName	username@gmail.com
5		

Guarde el archivo como **C:\BulkInvite\Invitations.csv**.

Si no tiene Excel, puede crear un archivo .csv en cualquier editor de texto como el Bloc de notas. Separe cada valor con una coma y cada fila con una línea nueva.

Inicio de sesión en su inquilino

Ejecute el siguiente comando para conectarse al dominio del inquilino:

```
Connect-AzureAD -TenantDomain "<Tenant_Domain_Name>"
```

Por ejemplo, `Connect-AzureAD -TenantDomain "contoso.onmicrosoft.com"`.

Cuando se le solicite, escriba las credenciales.

Envío de invitaciones en masa

Para enviar las invitaciones, ejecute el siguiente script de PowerShell (donde `c:\bulkinvite\invitations.csv` es la ruta de acceso al archivo .csv):

```
$invitations = import-csv c:\bulkinvite\invitations.csv

$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo

$messageInfo.customizedMessageBody = "Hello. You are invited to the Contoso organization."

foreach ($email in $invitations)
{
    New-AzureADMSInvitation `

        -InvitedUserEmailAddress $email.InvitedUserEmailAddress `

        -InvitedUserDisplayName $email.Name `

        -InviteRedirectUrl https://myapps.microsoft.com `

        -InvitedUserMessageInfo $messageInfo `

        -SendInvitationMessage $true
}
```

El script enviará una invitación a las direcciones de correo electrónico del archivo Invitations.csv. Debería ver una salida similar a la siguiente para cada usuario:

```
Id : 
InvitedUserDisplayName : 
InvitedUserEmailAddress : 
SendInvitationMessage : True
InviteRedeemUrl : https://invitations.microsoft.com/redeem/?tenant= &user= &ticket= &ver=2.0
InviteRedirectUrl : https://myapps.azure.com/
InvitedUser : class User {
    Id: 
    OdataType: 
}

InvitedUserMessageInfo : class InvitedUserMessageInfo {
    CcRecipients: System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.Recipient]
    CustomizedMessageBody: Hello. You are invited to the Contoso organization.
    MessageLanguage: 
}

InvitedUserType : Guest
Status : PendingAcceptance
```

Verificación de la existencia de los usuarios en el directorio

Para verificar que se agregaron los usuarios invitados a Azure AD, ejecute el siguiente comando:

```
Get-AzureADUser -Filter "UserType eq 'Guest'"
```

Debería ver los usuarios invitados en la lista, con un nombre principal de usuario (UPN) con el formato *direccióndecorreoelectrónico #EXT#@dominio*. Por ejemplo, *lstokes_fabrikam.com#EXT#@contoso.onmicrosoft.com*, donde contoso.onmicrosoft.com es la organización desde la que se enviaron las invitaciones.

Limpieza de recursos

Cuando ya no sean necesarias, puede eliminar las cuentas de usuario de prueba del directorio. Ejecute el siguiente comando para eliminar una cuenta de usuario:

```
Remove-AzureADUser -ObjectId "<UPN>"
```

Por ejemplo: `Remove-AzureADUser -ObjectId "lstokes_fabrikam.com#EXT#@contoso.onmicrosoft.com"`

Pasos siguientes

En este tutorial, ha enviado invitaciones en masa a usuarios invitados fuera de la organización. A continuación, obtenga información sobre cómo funciona el proceso de canje de la invitación.

[Obtenga información sobre el proceso de canje de la invitación de colaboración de Azure AD B2B](#)

Tutorial: Invitación en masa a usuarios de colaboración de Azure AD B2B

18/02/2021 • 8 minutes to read • [Edit Online](#)

Si usas la colaboración de Azure Active Directory (Azure AD) B2B para trabajar con asociados externos, puedes invitar a varios usuarios a su organización al mismo tiempo. En este tutorial aprenderá a usar Azure Portal para enviar invitaciones de forma masiva a usuarios externos. En particular, haga lo siguiente:

- Use **Invitar usuarios en bloque** para preparar un archivo de valores separados por comas (.csv) con la información del usuario y las preferencias de invitación.
- Cargue el archivo .csv en Azure AD.
- Verifique si los usuarios se agregaron al directorio.

Antes de comenzar, si no tiene una cuenta de Azure Active Directory, [cree una gratuita](#).

Nociones sobre la plantilla CSV

Descargue y rellene la plantilla CSV de carga masiva para ayudarle a invitar correctamente a los usuarios invitados de Azure AD de forma masiva. La plantilla CSV que descargue podría parecerse a este ejemplo:

Row 1 must be preserved as-is, and the version number is always required.	
A	B
1	version:v1.0
2	Email address to invite [inviteeEmail] Required
3	Example: lstokes@fabrikam.com
4	Redirection url [inviteRedirectURL] ReS https://myapps.azure.com

Preserve the column headings as-is in row 2. Column headings indicate acceptable values and whether they're required. Don't add additional columns.

Use the entries in row 3 as examples. Remove the row's contents and replace the examples with your entries.

Estructura de la plantilla CSV

Las filas de una plantilla CSV descargada son las siguientes:

- **Número de versión:** la primera fila, que contiene el número de versión, debe estar incluida en el archivo CSV de carga.
- **Encabezados de columna:** el formato de los encabezados de columna es <*Nombre del elemento*> [nombreDePropiedad] <*Required (Obligatorio)* o en blanco>. Por ejemplo, **Email address to invite [inviteeEmail] Required**. Algunas versiones anteriores de la plantilla podrían tener ligeras variaciones.
- **Fila de ejemplos:** en la plantilla se incluye una fila de ejemplos de valores válidos para cada columna. Debe quitar la fila de ejemplos y reemplazarla por sus propias entradas.

Instrucciones adicionales

- Las dos primeras filas de la plantilla de carga no se deben eliminar ni modificar, o no se podrá procesar la carga.
- Las columnas necesarias se enumeran en primer lugar.
- No se recomienda agregar nuevas columnas a la plantilla. Cualquier columna adicional que agregue se omitirá y no se procesará.

- Se recomienda que descargue la versión más reciente de la plantilla CSV tan a menudo como sea posible.

Prerrequisitos

Necesita dos o más cuentas de correo electrónico de prueba a las que poder enviar las invitaciones. Las cuentas deben estar fuera de su organización. Puede usar cualquier tipo de cuenta, incluidas las cuentas sociales como las direcciones de gmail.com o outlook.com.

Invitación en bloque a usuarios

1. Inicie sesión en Azure Portal con una cuenta que sea la del administrador de usuarios de la organización.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Usuarios > Invitar en bloque**.
4. En la página **Invitar usuarios en bloque**, seleccione **Descargar** para obtener una plantilla .csv válida con las propiedades de la invitación.

5. Abra la plantilla .csv y agregue una línea por cada usuario invitado. Los valores obligatorios son:

- **Dirección de correo electrónico para enviar la invitación:** el usuario que recibirá una invitación.
- **URL de redireccionamiento:** la dirección URL a la que se reenviará al usuario invitado después de que acepte la invitación.

	A	B	C	D
1	version:v1.0			
2	Email address to invite [inviteeEmail] Required	Redirection url [inviteRedirectURL]	ReSend invitation message (true)	Customized invitation message [customize]
3	Example: istokes@fabrikam.com	https://myapps.azure.com	TRUE	Welcome to the Contoso organization!
4				

NOTE

No use comas en **Mensaje de invitación personalizado**, porque impedirán que el mensaje se analice correctamente.

6. Guarde el archivo.
7. En la página **Invitar usuarios en bloque**, en **Cargue el archivo csv**, vaya al archivo. Al seleccionarlo, comienza su validación.
8. Cuando finalice la validación del contenido del archivo, aparecerá el mensaje **Archivo cargado correctamente**. Si hay errores, debe corregirlos para poder enviar el trabajo.
9. Cuando el archivo supere la validación, seleccione **Enviar** para iniciar la operación masiva de Azure que agrega las invitaciones.
10. Para ver el estado del trabajo, seleccione **Haga clic aquí para ver el estado de cada operación**. O bien, puede seleccionar **Resultados de la operación masiva** en la sección **Actividad**. Para más

información sobre cada elemento de línea dentro de la operación en bloque, seleccione los valores de las columnas **Número de elementos correctos**, **Número de errores** o **Total de solicitudes**. Si se produjeron errores, se mostrarán sus motivos.

The screenshot shows the 'Users - Bulk operation results' page in the Azure Active Directory portal. The left sidebar includes options like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Activity', 'Sign-ins', 'Audit logs', and 'Bulk operation results'. The 'Bulk operation results' option is selected. The main area displays a table with one row for 'testinvite.csv'. The columns include 'FILE NAME', 'UPLOAD TIME', 'COMPLETION TIME', 'STATUS', '# SUCCESS', '# FAILURE', 'TOTAL REQUESTS', 'ADMIN UPLOADED', and 'TYPE'. The status is 'Completed with errors', with 2 successes, 1 failure, and 3 total requests. The admin uploaded is 'useradmin@contoso.com' and the type is 'user invite'. There is also a feedback message at the top: 'Got a second? We would love your feedback on Bulk operations'.

11. Cuando el trabajo finalice, verá una notificación indicando que la operación masiva se realizó correctamente.

Verificación de usuarios invitados en el directorio

Compruebe en Azure Portal o mediante PowerShell que los usuarios invitados que ha agregado existen en el directorio.

Visualización de los usuarios invitados en Azure Portal

1. Inicie sesión en Azure Portal con una cuenta que sea la del administrador de usuarios de la organización.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Usuarios**.
4. En **Mostrar**, seleccione **Solo usuarios invitados** y compruebe que los usuarios que ha agregado aparecen en la lista.

Visualización de los usuarios invitados con PowerShell

Ejecute el siguiente comando:

```
Get-AzureADUser -Filter "UserType eq 'Guest'"
```

Debería ver los usuarios invitados en la lista, con un nombre principal de usuario (UPN) con el formato *direccióndecorreoelectrónico#EXT#@dominio*. Por ejemplo, *lstokes_fabrikam.com#EXT#@contoso.onmicrosoft.com*, donde contoso.onmicrosoft.com es la organización desde la que se enviaron las invitaciones.

Limpieza de recursos

Cuando ya no necesite las cuentas de usuario de prueba del directorio de Azure Portal, puede eliminarlas desde la página Usuarios; para ello, active la casilla situada junto al usuario invitado y, a continuación, seleccione **Eliminar**.

También puede ejecutar el siguiente comando de PowerShell para eliminar una cuenta de usuario:

```
Remove-AzureADUser -ObjectId "<UPN>"
```

Por ejemplo: `Remove-AzureADUser -ObjectId "lstokes_fabrikam.com#EXT#@contoso.onmicrosoft.com"`

Pasos siguientes

En este tutorial, ha enviado invitaciones en masa a usuarios invitados fuera de la organización. A continuación,

obtenga información sobre cómo funciona el proceso de canje de la invitación.

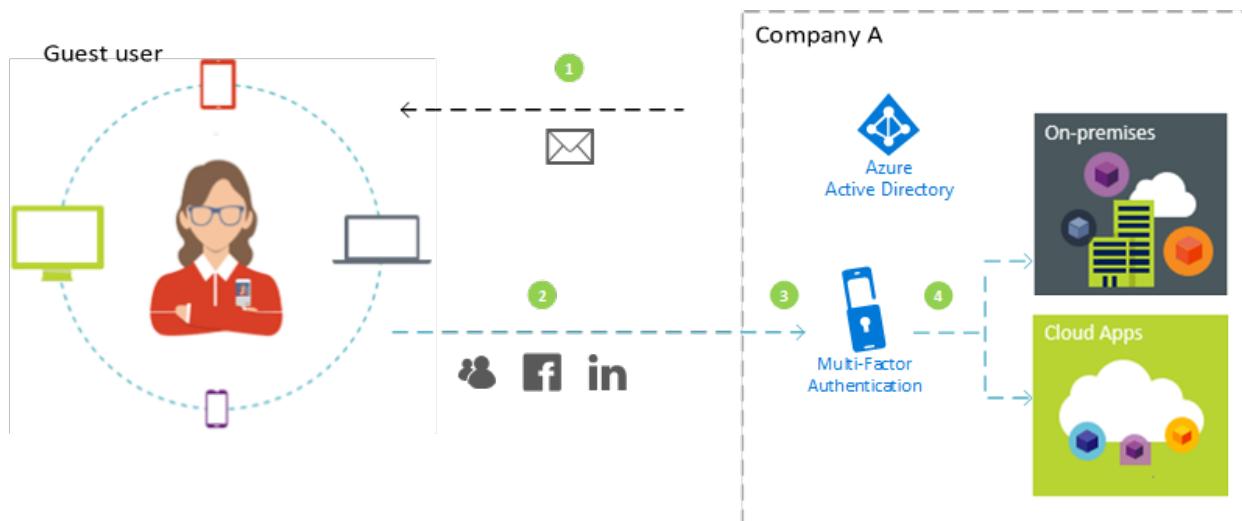
[Obtenga información sobre el proceso de canje de la invitación de colaboración de Azure AD B2B](#)

Tutorial: Aplicación de la autenticación multifactor para usuarios invitados de B2B

18/02/2021 • 9 minutes to read • [Edit Online](#)

Al colaborar con los usuarios externos invitados de B2B, es una buena idea proteger sus aplicaciones con directivas de autenticación multifactor (MFA). Después, los usuarios externos necesitarán más de un nombre de usuario y una contraseña para acceder a los recursos. En Azure Active Directory (Azure AD), puede lograr este objetivo con una directiva de acceso condicional que precisa de MFA para el acceso. Las directivas de MFA se pueden exigir en el nivel de inquilino, aplicación o usuario invitado individual, del mismo modo que pueden habilitarse para miembros de la organización.

Ejemplo:



1. Un administrador o un empleado de la empresa A invita a un usuario invitado para usar una aplicación local o en la nube que está configurada para requerir MFA para el acceso.
2. El usuario invitado inicia sesión con su identidad profesional, educativa o social.
3. Al usuario se le pide que complete un desafío de MFA.
4. El usuario configura su MFA con la empresa A y elegir su opción de MFA. El usuario puede tener acceso a la aplicación.

En este tutorial, aprenderá lo siguiente:

- Probar la experiencia de inicio de sesión antes de la configuración de MFA.
- Crear una directiva de acceso condicional que requiere MFA para acceder a una aplicación en la nube en su entorno. En este tutorial, vamos a usar la aplicación de administración de Microsoft Azure para ilustrar el proceso.
- Use la herramienta What If para simular el inicio de sesión con MFA.
- Pruebe la directiva de acceso condicional.
- Limpie el usuario de prueba y la directiva.

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Prerequisites

Para completar el escenario de este tutorial, necesita:

- **Acceder a la edición Azure AD Premium**, que incluye funcionalidades de directiva de acceso condicional. Para exigir MFA, debe crear una directiva de acceso condicional de Azure AD. Tenga en cuenta que siempre se aplican directivas de MFA en su organización, independientemente de si el asociado tiene funcionalidades de MFA. Si configura MFA para su organización, debe asegurarse de que haya suficientes licencias de Azure AD Premium para sus usuarios invitados.
- **Una cuenta válida de correo electrónico externa** que puede agregar a su directorio de inquilino como un usuario invitado y usarla para iniciar sesión. Si no sabe cómo crear una cuenta de invitado, vea [Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#).

Creación de un usuario invitado de prueba en Azure AD

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En el panel izquierdo, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Usuarios**.
4. Seleccione **Nuevo usuario invitado**.

The screenshot shows the Azure portal interface with the URL https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/AllUsers. On the left, there's a sidebar with 'Create a resource', 'All services', 'FAVORITES', and 'Function Apps'. The main content area is titled 'Users - All users' under 'contoso - Azure Active Directory'. It shows a list of users with columns for NAME, USER NAME, USER TYPE, and SOURCE. At the top right of this list, there are buttons for '+ New user' and '+ New guest user', with '+ New guest user' being highlighted by a red box. Below these buttons are search fields for 'Name' and 'Show'.

5. En **Nombre de usuario**, escriba la dirección de correo electrónico del usuario externo. Opcionalmente, puede incluir un mensaje de bienvenida.

The screenshot shows the 'New Guest User' dialog. At the top, it says 'New Guest User' and 'microsoft'. Below that is an information icon with the text: 'This user will be added as a Guest. Click here to learn more.' A red box highlights the 'User name' input field, which contains 'contosoguest1@outlook.com'. Below the input field is a message input field with the placeholder 'Include a personal message with the invitation'. At the bottom, there's a large blue 'Invite' button.

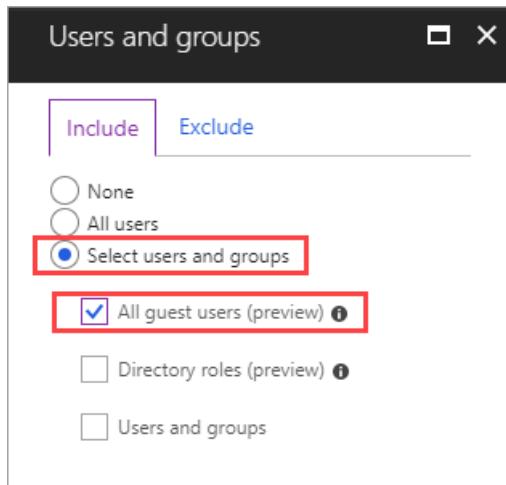
6. Seleccione **Invitar** para enviar automáticamente la invitación al usuario invitado. Aparece un mensaje **Usuario invitado correctamente**.
7. Despues de enviar la invitación, la cuenta de usuario se agrega automáticamente al directorio como invitado.

Probar la experiencia de inicio de sesión antes de la configuración de MFA

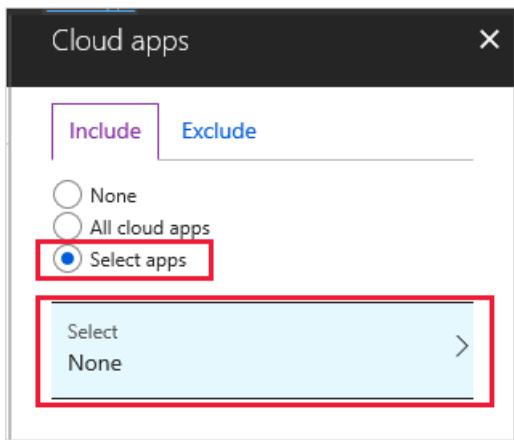
1. Use la contraseña y el nombre de usuario invitado para iniciar sesión en [Azure Portal](#).
2. Tenga en cuenta que podrá acceder a Azure Portal solo con sus credenciales de inicio de sesión. No se requiere la autenticación adicional.
3. Cierre la sesión.

Creación de una directiva de acceso condicional que requiere MFA

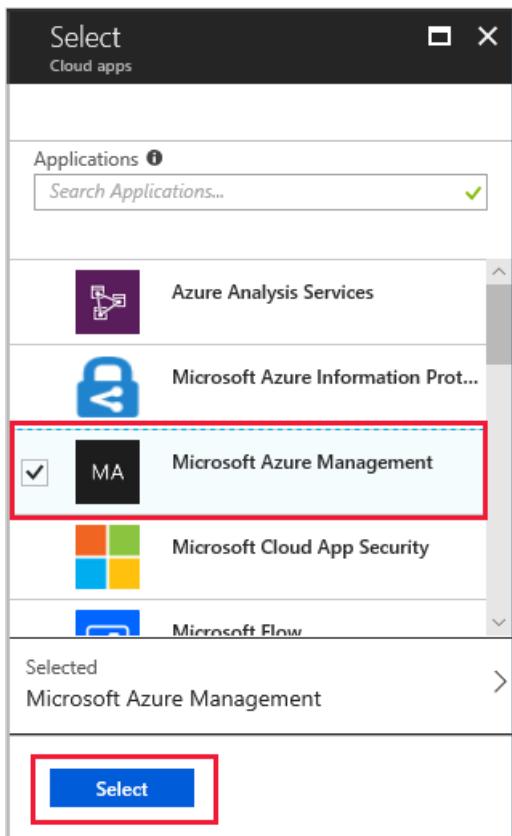
1. Inicie sesión en [Azure Portal](#) como administrador de seguridad o administrador de acceso condicional.
2. En Azure Portal, seleccione **Azure Active Directory**.
3. En la página **Azure Active Directory**, en la sección **Seguridad**, seleccione **Acceso condicional**.
4. En la página **Acceso condicional**, en la barra de herramientas de la parte superior, seleccione **Nueva directiva**.
5. En la página **Nuevo**, en el cuadro de texto **Nombre**, escriba **Requerir MFA para acceder al portal de B2B**.
6. En la sección **Asignaciones**, seleccione **Usuarios y grupos**.
7. En la página **Usuarios y grupos**, elija **Seleccionar usuarios y grupos** y luego seleccione **Todos los usuarios invitados (versión preliminar)**.



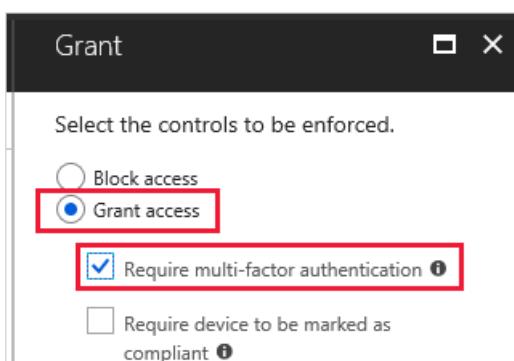
8. Seleccione **Listo**.
9. En la página **Nuevo**, en la sección **Asignaciones**, seleccione **Aplicaciones en la nube**.
10. En la página **Aplicaciones en la nube**, haga clic en **Seleccionar aplicaciones** y después haga clic en **Seleccionar**.



11. En la página **Seleccionar**, elija **Administración de Microsoft Azure** y después haga clic en **Seleccionar**.



12. En la página **Aplicaciones en la nube**, seleccione **Listo**.
13. En la página **Nuevo**, en la sección **Controles de acceso**, seleccione **Conceder**.
14. En la página **Conceder**, elija **Conceder acceso**, marque la casilla **Requerir autenticación multifactor** y luego haga clic en **Seleccionar**.



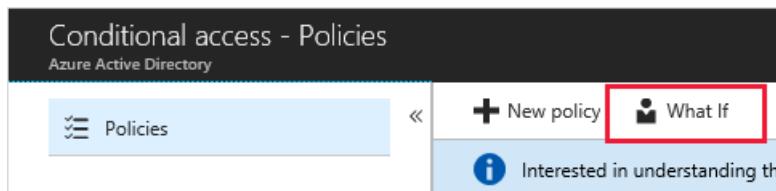
15. En **Habilitar directiva**, seleccione **Activar**.



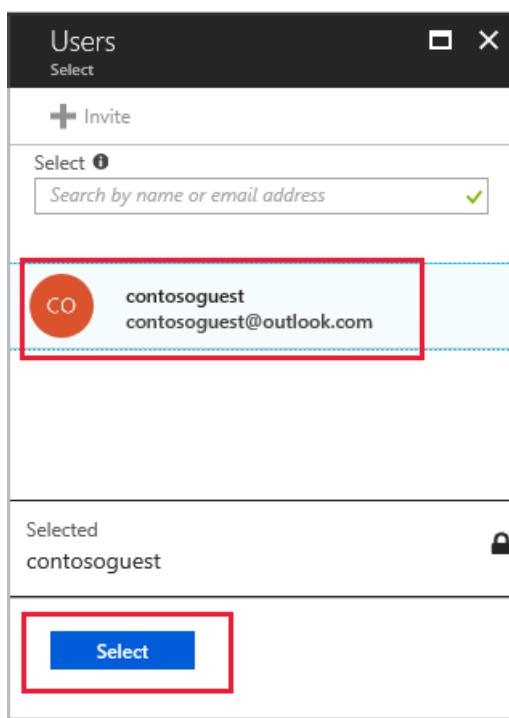
16. Seleccione Crear.

Uso de la opción What If para simular el inicio de sesión

1. En la página Acceso condicional - Directivas, seleccione **What If**.

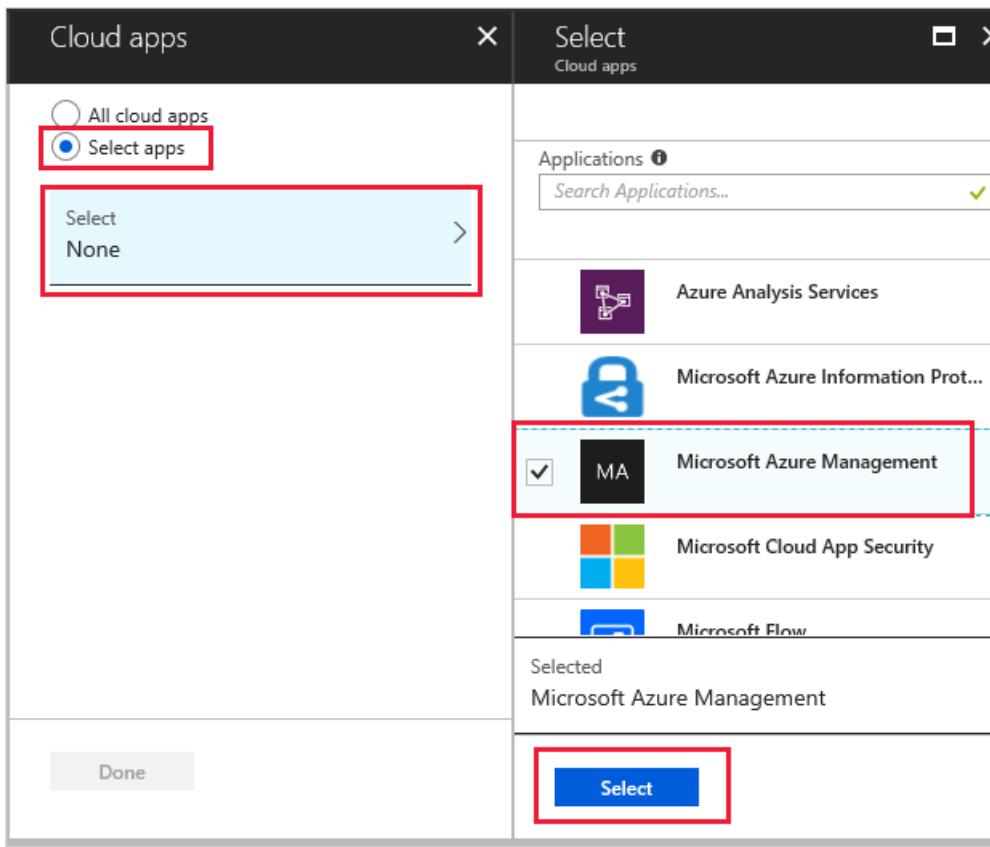


2. Seleccione **Usuario**, elija el usuario invitado de prueba y después haga clic en **Seleccionar**.



3. Seleccione **Aplicaciones en la nube**.

4. En la página **Aplicaciones en la nube**, haga clic en **Seleccionar aplicaciones** y después haga clic en **Seleccionar**. En la lista de aplicaciones, seleccione **Administración de Microsoft Azure** y luego haga clic en **Seleccionar**.



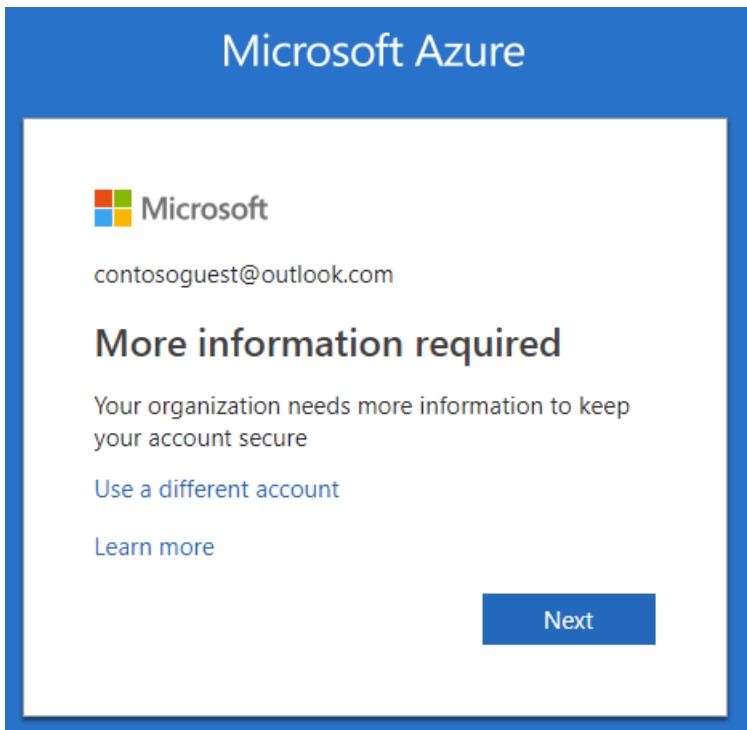
5. En la página **Aplicaciones en la nube**, seleccione **Listo**.
6. Seleccione **What If** y verifique que la nueva directiva aparece en **Resultados de evaluación** en la pestaña **Directivas que se aplicarán**.

This screenshot shows the 'What If' evaluation results page. At the top, there are 'What If' and 'Reset' buttons. Below them is a section titled 'Evaluation result' with tabs for 'Policies that will apply' (selected) and 'Policies that will not apply'. The main table has columns for 'POLICY NAME' and 'GRANT CONTROLS'. One row shows 'Require MFA for Azure portal access' and 'Require multi-factor authentication'.

POLICY NAME	GRANT CONTROLS
Require MFA for Azure portal access	Require multi-factor authentication

Prueba de la directiva de acceso condicional

1. Use la contraseña y el nombre de usuario invitado para iniciar sesión en [Azure Portal](#).
2. Debería ver una solicitud para los métodos de autenticación adicionales. Tenga en cuenta que la directiva puede tardar algún tiempo en aplicarse.



3. Cierre la sesión.

Limpieza de recursos

Cuando ya no sean necesarios, elimine el usuario de prueba y la directiva de acceso condicional de prueba.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En el panel izquierdo, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Usuarios**.
4. Seleccione el usuario de prueba y después **Eliminar usuario**.
5. En el panel izquierdo, seleccione **Azure Active Directory**.
6. En **Seguridad**, seleccione **Acceso condicional**.
7. En la lista **Nombre de la directiva**, seleccione el menú contextual (...) de la directiva de prueba y después seleccione **Eliminar**. Seleccione **Sí** para confirmar la acción.

Pasos siguientes

En este tutorial, ha creado una directiva de acceso condicional que requiere que los usuarios invitados usen MFA al iniciar sesión en una de las aplicaciones en la nube. Para más información sobre cómo agregar usuarios invitados para la colaboración, vea [Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#).

Ejemplos de registro de autoservicio de identidades externas

18/02/2021 • 2 minutes to read • [Edit Online](#)

En las tablas siguientes se proporcionan vínculos a ejemplos de código para aprovechar las API web en los flujos de usuario de registro de autoservicio mediante [conectores de API](#).

Guías de inicio rápido de Azure Functions para conectores de API

MUESTRA	DESCRIPCIÓN
.NET Core	Este ejemplo de Azure Functions con .NET Core muestra cómo limitar los registros a dominios de inquilino específicos y validar la información proporcionada por el usuario.
Node.js	Este ejemplo de Azure Functions con Node.js muestra cómo limitar los registros a dominios de inquilino específicos y validar la información proporcionada por el usuario.
Python	Este ejemplo de Azure Functions con Python muestra cómo limitar los inicios de sesión a dominios de inquilino específicos y validar la información proporcionada por el usuario.

Flujos de trabajo de aprobación personalizados

MUESTRA	DESCRIPCIÓN
Flujo de trabajo de aprobación manual	Este ejemplo muestra un flujo de trabajo de aprobación de un extremo a otro para administrar la creación de cuentas de usuario invitado en el registro de autoservicio

Verificación de identidad

MUESTRA	DESCRIPCIÓN
IDology	En este ejemplo se muestra cómo comprobar una identidad de usuario como parte de su suscripción de autoservicio mediante un conector de API para integrarse con IDology.
Experian	En este ejemplo se muestra cómo comprobar una identidad de usuario como parte de su registro de autoservicio mediante un conector de API para integrarse con Experian.

Ejemplos de código y PowerShell para la colaboración B2B de Azure Active Directory

18/02/2021 • 5 minutes to read • [Edit Online](#)

Ejemplo de PowerShell

Puede invitar de forma masiva a usuarios externos a una organización desde direcciones de correo electrónico que ha almacenado en un archivo CSV.

1. Prepare el archivo: cree un archivo CSV y asígnele el nombre invitations.csv. En este ejemplo, el archivo se guarda en C:\data y contiene la información siguiente:

NOMBRE	INVITEDUSEREMAILADDRESS
Invitado de B2B de Gmail	b2binvitee@gmail.com
Invitado de B2B de Outlook	b2binvitee@outlook.com

2. Obtenga la última versión de Azure AD PowerShell para usar los nuevos cmdlets: debe instalar el módulo de Azure AD PowerShell actualizado, que puede descargar de la [página de la versión del módulo de Powershell](#).

3. Inicie sesión en el espacio.

```
$cred = Get-Credential  
Connect-AzureAD -Credential $cred
```

4. Ejecución del cmdlet de PowerShell

```
$invitations = import-csv C:\data\invitations.csv  
$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo  
$messageInfo.customizedMessageBody = "Hey there! Check this out. I created an invitation through  
PowerShell"  
foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress  
$email.InvitedUserEmailAddress -InvitedUserDisplayName $email.Name -InviteRedirectUrl  
https://wingtiptoysonline-dev-ed.my.salesforce.com -InvitedUserMessageInfo $messageInfo -  
SendInvitationMessage $true}
```

Este cmdlet enviará una invitación a la dirección de correo electrónico de invitations.csv. Algunas características adicionales de este cmdlet son las siguientes:

- Texto personalizado en el mensaje de correo electrónico
- Inclusión de un nombre para mostrar de los usuarios invitados
- Envío de mensajes en copias o supresión de mensajes de correo electrónico por completo

Código de ejemplo

En este ejemplo se muestra cómo llamar a la API de invitación, en el modo de solo de aplicación, para obtener la URL de pago del recurso al que va a invitar al usuario B2B. El objetivo consiste en enviar un correo electrónico de invitación personalizado. El correo electrónico se puede redactar con un cliente HTTP, lo que le permite

personalizar su aspecto y enviarlo a través de Microsoft Graph API.

```
namespace SampleInviteApp
{
    using System;
    using System.Linq;
    using System.Net.Http;
    using System.Net.Http.Headers;
    using Microsoft.IdentityModel.Clients.ActiveDirectory;
    using Newtonsoft.Json;
    class Program
    {
        /// <summary>
        /// Microsoft Graph resource.
        /// </summary>
        static readonly string GraphResource = "https://graph.microsoft.com";

        /// <summary>
        /// Microsoft Graph invite endpoint.
        /// </summary>
        static readonly string InviteEndPoint = "https://graph.microsoft.com/v1.0/invitations";

        /// <summary>
        /// Authentication endpoint to get token.
        /// </summary>
        static readonly string EstsLoginEndpoint = "https://login.microsoftonline.com";

        /// <summary>
        /// This is the tenantid of the tenant you want to invite users to.
        /// </summary>
        private static readonly string TenantID = "";

        /// <summary>
        /// This is the application id of the application that is registered in the above tenant.
        /// The required scopes are available in the below link.
        /// https://developer.microsoft.com/graph/docs/api-reference/v1.0/api/invitation_post
        /// </summary>
        private static readonly string TestAppClientId = "";

        /// <summary>
        /// Client secret of the application.
        /// </summary>
        private static readonly string TestAppClientSecret = @"";

        /// <summary>
        /// This is the email address of the user you want to invite.
        /// </summary>
        private static readonly string InvitedUserEmailAddress = @"";

        /// <summary>
        /// This is the display name of the user you want to invite.
        /// </summary>
        private static readonly string InvitedUserDisplayName = @"";

        /// <summary>
        /// Main method.
        /// </summary>
        /// <param name="args">Optional arguments</param>
        static void Main(string[] args)
        {
            Invitation invitation = CreateInvitation();
            SendInvitation(invitation);
        }

        /// <summary>
        /// Create the invitation object.
        /// </summary>
        /// <returns>Returns the invitation object.</returns>
```

```

private static Invitation CreateInvitation()
{
    // Set the invitation object.
    Invitation invitation = new Invitation();
    invitation.InvitedUserDisplayName = InvitedUserDisplayName;
    invitation.InvitedUserEmailAddress = InvitedUserEmailAddress;
    invitation.InviteRedirectUrl = "https://www.microsoft.com";
    invitation.SendInvitationMessage = true;
    return invitation;
}

/// <summary>
/// Send the guest user invite request.
/// </summary>
/// <param name="invitation">Invitation object.</param>
private static void SendInvitation(Invitation invitation)
{
    string accessToken = GetAccessToken();

    HttpClient httpClient = GetHttpClient(accessToken);

    // Make the invite call.
    HttpContent content = new StringContent(JsonConvert.SerializeObject(invitation));
    content.Headers.Add("ContentType", "application/json");
    var postResponse = httpClient.PostAsync(InviteEndPoint, content).Result;
    string serverResponse = postResponse.Content.ReadAsStringAsync().Result;
    Console.WriteLine(serverResponse);
}

/// <summary>
/// Get the HTTP client.
/// </summary>
/// <param name="accessToken">Access token</param>
/// <returns>Returns the Http Client.</returns>
private static HttpClient GetHttpClient(string accessToken)
{
    // setup http client.
    HttpClient httpClient = new HttpClient();
    httpClient.Timeout = TimeSpan.FromSeconds(300);
    httpClient.DefaultRequestHeaders.Authorization = new AuthenticationHeaderValue("Bearer",
    accessToken);
    httpClient.DefaultRequestHeaders.Add("client-request-id", Guid.NewGuid().ToString());
    Console.WriteLine(
        "CorrelationID for the request: {0}",
        httpClient.DefaultRequestHeaders.GetValues("client-request-id").Single());
    return httpClient;
}

/// <summary>
/// Get the access token for our application to talk to Microsoft Graph.
/// </summary>
/// <returns>Returns the access token for our application to talk to Microsoft Graph.</returns>
private static string GetAccessToken()
{
    string accessToken = null;

    // Get the access token for our application to talk to Microsoft Graph.
    try
    {
        AuthenticationContext testAuthContext =
            new AuthenticationContext(string.Format("{0}/{1}", EstsLoginEndpoint, TenantID));
        AuthenticationResult testAuthResult = testAuthContext.AcquireTokenAsync(
            GraphResource,
            new ClientCredential(TestAppClientId, TestAppClientSecret)).Result;
        accessToken = testAuthResult.AccessToken;
    }
    catch (AdalException ex)
    {
        Console.WriteLine("An exception was thrown while fetching the token: {0}.". ex);
    }
}

```

```
        throw;
    }

    return accessToken;
}

/// <summary>
/// Invitation class.
/// </summary>
public class Invitation
{
    /// <summary>
    /// Gets or sets display name.
    /// </summary>
    public string InvitedUserDisplayName { get; set; }

    /// <summary>
    /// Gets or sets display name.
    /// </summary>
    public string InvitedUserEmailAddress { get; set; }

    /// <summary>
    /// Gets or sets a value indicating whether Invitation Manager should send the email to
    InvitedUser.
    /// </summary>
    public bool SendInvitationMessage { get; set; }

    /// <summary>
    /// Gets or sets invitation redirect URL
    /// </summary>
    public string InviteRedirectUrl { get; set; }
}
}
```

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)

Modelo de facturación para Azure AD for External Identities

18/02/2021 • 5 minutes to read • [Edit Online](#)

Los precios de Azure Active Directory (Azure AD) for External Identities se basan en los usuarios activos mensuales (MAU), que es el recuento de usuarios únicos con actividad de autenticación dentro de un mes natural. Este modelo de facturación se aplica tanto a la colaboración de usuarios invitados (B2B) de Azure AD como a los [inquilinos de Azure AD B2C](#). La facturación de MAU le ayuda a reducir los costos al ofrecer un nivel gratis y precios flexibles y predecibles. En este artículo obtendrá información sobre la facturación de MAU y la vinculación de los inquilinos de Azure AD a una suscripción.

IMPORTANT

Este artículo no contiene detalles de precios. Para conocer la información más reciente sobre la facturación por uso y los precios, consulte [Precios de Azure Active Directory](#).

¿Qué tengo que hacer?

Para aprovechar las ventajas de la facturación de MAU, el inquilino de Azure AD debe estar vinculado a una suscripción de Azure.

SI EL INQUILINO ES:	NECESITA:
Un inquilino de Azure AD ya vinculado a una suscripción	No haga nada. Al usar las características de identidades externas para colaborar con los usuarios invitados, se le facturará automáticamente mediante el modelo de MAU.
Un inquilino de Azure AD no vinculado aún a una suscripción	Vincule el inquilino de Azure AD a una suscripción para activar la facturación de MAU.

Acerca de la facturación de usuarios activos mensuales (MAU)

En el inquilino de Azure AD, el uso de la colaboración de usuarios invitados se factura en función del número de usuarios invitados únicos con actividad de autenticación dentro de un mes natural. Este modelo reemplaza el modelo de facturación con una relación 1:5, que permitía hasta cinco usuarios invitados para cada licencia Premium de Azure AD del inquilino. Cuando el inquilino está vinculado a una suscripción y usa las características de identidades externas para colaborar con los usuarios invitados, se le facturará automáticamente mediante el modelo de facturación basado en MAU.

El plan de tarifa que se aplica a los usuarios invitados se basa en el plan de tarifa más alto asignado al inquilino de Azure AD. Por ejemplo, si el plan de tarifa más alto del inquilino es Azure AD Premium P1, también se aplica a los usuarios invitados el plan de tarifa Premium P1. Si el plan de tarifa más alto es Azure AD Free, se le pedirá que actualice a un plan de tarifa Premium al intentar usar las características Premium para los usuarios invitados.

Vinculación del inquilino de Azure AD a una suscripción

Se debe vincular un inquilino de Azure AD a una suscripción de Azure para una facturación adecuada y el acceso a las características. Si el directorio todavía no tiene una suscripción a la que se pueda vincular, tendrá la oportunidad de agregar una durante este proceso.

1. Inicie sesión en [Azure Portal](#) con una cuenta de Azure a la que se haya asignado al menos el rol [Colaborador](#) dentro de la suscripción o un grupo de recursos dentro de la suscripción.
2. Seleccione el directorio que desee vincular: En la barra de herramientas de Azure Portal, seleccione el ícono de **Directorio + suscripción** y, luego, seleccione el directorio.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Home, Dashboard, All services, and Favorites. The main area is titled 'Azure services' and contains icons for Create a resource, Azure Active Directory, Azure AD B2C, Resource groups, App Services, Storage accounts, SQL databases, and All services. Below this is a 'Recent resources' table:

NAME	TYPE
contosob2c.onmicrosoft.com	B2C Tenant
contosob2cRG	Resource group
contosostorage	Storage account
vm01	Virtual machine
vm01PublicIP	Public IP address
vm01VMNic	Network interface
contoso-vnet	Virtual network
vm01NSG	Network security group
contosoRG	Resource group

To the right, a 'Directory + subscription' blade is open. It shows a 'Default subscription filter' set to 'contoso.onmicrosoft.com'. Under 'Switch directory', there's a search bar and a list of directories. One entry, 'Fabrikam', is highlighted with a red box. The full list includes:

- Favorites
- All Directories
- A to Z

Search
Fabrikam
Fabrikam.onmicrosoft.com
12345678-1234-1234-1234-123456789012
Default Directory
contoso.onmicrosoft.com
00000000-0000-0000-0000-000000000000

3. En **Servicios de Azure**, seleccione **Azure Active Directory**.
4. En el menú de la izquierda, seleccione **External Identities**.
5. En **Suscripciones**, seleccione **Suscripciones vinculadas**.
6. En la lista de inquilinos, active la casilla situada junto al inquilino y, a continuación, seleccione **Vinculación de la suscripción**.



External Identities | Linked subscriptions

Fabrikam Corporation - Azure Active Directory

 Search (Ctrl+ /)

<<

[Link subscription](#)[Edit](#)[Got feedback?](#)[Get started](#)[All identity providers](#)[External collaboration settings](#)[Diagnose and solve problems](#)

Self-service sign up

[Custom user attributes \(Preview\)](#)[All API connectors \(Preview\)](#)[User flows \(Preview\)](#)

Subscriptions

[Linked subscriptions](#)

Lifecycle management

[Tenants](#)

Tenant	Directory type
<input checked="" type="checkbox"/> Fabrikam Corporation	Azure AD

Azure AD External Identities is priced on a Monthly Active User (MAU) per month.

Your tenant's subscription

Please link an Azure subscription to this tenant to continue receiving updates.

7. En el panel Vinculación de una suscripción, seleccione una **suscripción** y un **grupo de recursos**. Luego, seleccione **Aplicar**.

NOTE

Si no aparecen suscripciones, puede [asociar una suscripción al inquilino](#). También puede agregar una nueva suscripción seleccionando el vínculo . Si aún no tiene una suscripción, puede [crear una aquí](#) .

Link a subscription

X

Azure AD External Identities is priced on a Monthly Active User (MAU) basis, ensuring you only pay for what you use. Your first 50,000 MAU are free.

Associate a subscription for External Identities. You will not be billed until your usage exceeds 50,000 MAU.

Subscription *

Visual Studio Enterprise Subscription

Resource group *

ContosoRG

Billing unit

Monthly active users (MAU)

Apply

Después de completar estos pasos, la suscripción de Azure se factura según los detalles del Contrato Enterprise o de Azure Direct, si procede.

Pasos siguientes

Para obtener la información de precios más reciente, consulte [Precios de Azure Active Directory](#).

Procedimientos recomendados de Azure Active Directory B2B

18/02/2021 • 8 minutes to read • [Edit Online](#)

Este artículo contiene recomendaciones y procedimientos recomendados para la colaboración de negocio a negocio (B2B) en Azure Active Directory (Azure AD).

IMPORTANT

A partir de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de inquilinos y cuentas de Azure AD no administrada ("virales" o "Just-In-Time") para escenarios de colaboración B2B. En ese momento, la característica de código de acceso de un solo uso por correo electrónico se activará para todos los inquilinos existentes, y se habilitará de forma predeterminada para los nuevos. Vamos a habilitar la característica de código de acceso de un solo uso por correo electrónico, ya que proporciona un método eficaz de autenticación de reserva para usuarios invitados. No obstante, puede deshabilitar esta característica si prefiere no utilizarla. Para más información, consulte [Autenticación con código de acceso de un solo uso por correo electrónico](#).

Recomendaciones de B2B

RECOMENDACIÓN	COMENTARIOS
Para una experiencia de inicio de sesión óptima, realice la federación con proveedores de identidades.	Siempre que sea posible, realice la federación directamente con los proveedores de identidades, para permitir que los usuarios invitados inicien sesión en las aplicaciones y recursos compartidos sin tener que crear cuentas de Microsoft (MSA) o cuentas de Azure AD. Puede usar la característica de federación de Google para permitir que los usuarios invitados de B2B inicien sesión con sus cuentas de Google. O bien, puede usar la característica de federación directa (versión preliminar) para configurar la federación directa con cualquier organización cuyo proveedor de identidades (IdP) admite los protocolos SAML 2.0 o WS-FED.
Uso de la característica de código de acceso de un solo uso por correo electrónico para invitados B2B que no se pueden autenticar por otros medios.	La característica de código de acceso de un solo uso por correo electrónico autentica los usuarios invitados de B2B cuando no pueden autenticarse por otros medios, como Azure AD, una cuenta de Microsoft (MSA) o la federación de Google. Cuando el usuario invitado canjea una invitación o accede a un recurso compartido, puede solicitar un código temporal, que se envía a su dirección de correo electrónico. A continuación, escribe este código para continuar con el inicio de sesión.
Adición de personalización de marca a la página de inicio de sesión	Puede personalizar la página de inicio de sesión de forma que resulte más intuitiva para los usuarios invitados de B2B. Consulte cómo agregar personalización de marca de la empresa en las páginas de inicio de sesión y del Panel de acceso .

RECOMENDACIÓN	COMENTARIOS
Agregue la declaración de privacidad a la experiencia de canje del usuario invitado de B2B.	Puede agregar la dirección URL de la declaración de privacidad de la organización al proceso de canje de invitación por primera vez, de modo que un usuario invitado deba dar su consentimiento a los términos de privacidad para continuar. Consulte Incorporación de información de privacidad de su organización en Azure Active Directory .
Use la característica de invitación en bloque (versión preliminar) para invitar a varios usuarios de B2B al mismo tiempo.	Invite a varios usuarios a su organización al mismo tiempo mediante la característica en versión preliminar de invitación en bloque de Azure Portal. Esta característica permite cargar un archivo CSV para crear usuarios invitados de B2B y enviar invitaciones en bloque. Consulte el tutorial para invitar en bloque a usuarios de B2B .
Aplique directivas de acceso condicional para Multi-Factor Authentication (MFA).	Se recomienda aplicar las directivas de MFA en las aplicaciones que desee compartir con los usuarios de B2B de asociados. De este modo, MFA se aplicará de forma coherente en las aplicaciones del inquilino, independientemente de si la organización asociada usa MFA. Consulte Acceso condicional para usuarios de colaboración B2B .
Si va a aplicar directivas de acceso condicional basado en el dispositivo, use listas de exclusión para permitir el acceso a los usuarios de B2B.	Si la organización tiene habilitadas directivas de acceso condicional basado en el dispositivo, los dispositivos de los usuarios invitados de B2B se bloquearán porque no están administrados por su organización. Puede crear listas de exclusión que contengan usuarios de asociados específicos para excluirlos de la directiva de acceso condicional basado en el dispositivo. Consulte Acceso condicional para usuarios de colaboración B2B .
Use una dirección URL específica del inquilino cuando proporcione vínculos directos a los usuarios invitados de B2B.	Como alternativa a la invitación por correo electrónico, puede darle al invitado un vínculo directo a la aplicación o al portal. Este vínculo directo debe ser específico del cliente, por lo que debe incluir un identificador de inquilino o dominio comprobado, de manera que el invitado se pueda autenticar en el inquilino donde se encuentra la aplicación compartida. Consulte Experiencia de invitación de colaboración B2B de Azure Active Directory .
Al desarrollar una aplicación, utilice UserType para determinar la experiencia del usuario invitado.	Si está desarrollando una aplicación y desea proporcionar diferentes experiencias para usuarios de inquilinos y usuarios invitados, use la propiedad UserType. La notificación UserType no está incluida actualmente en el token. Las aplicaciones deben usar Microsoft Graph API para consultar el usuario en el directorio y obtener su valor de UserType.
Cambio la propiedad UserType <i>solo</i> si cambia la relación del usuario con la organización.	Aunque es posible usar PowerShell para convertir la propiedad UserType de un usuario de miembro a invitado (y viceversa), solo debe cambiar esta propiedad si cambia la relación del usuario con la organización. Consulte Propiedades de un usuario de colaboración B2B de Azure Active Directory .

Pasos siguientes

[Habilitación de la colaboración externa B2B y administración de quién puede invitar a otros usuarios](#)

Uso compartido externo de Microsoft 365 y colaboración B2B de Azure Active Directory (Azure AD)

18/02/2021 • 5 minutes to read • [Edit Online](#)

En el uso compartido externo de Microsoft 365 y la colaboración B2B de Azure AD (OneDrive, SharePoint Online, grupos unificados, etc.), la autenticación de los usuarios externos se realiza mediante Azure AD B2B.

¿En qué se diferencia Azure AD B2B del uso compartido externo de SharePoint Online?

OneDrive y SharePoint Online tiene un administrador de invitaciones independiente. La compatibilidad con el uso compartido externo en OneDrive o SharePoint Online comenzó antes que Azure AD desarrollara su compatibilidad. Con el tiempo, el uso compartido externo de OneDrive o SharePoint Online ha acumulado varias características y muchos millones de usuarios que usan el patrón de uso compartido integrado del producto. Sin embargo, existen algunas diferencias sutiles entre cómo funciona el uso compartido externo de OneDrive y SharePoint Online y la colaboración B2B de Azure AD. Puede aprender más sobre el uso compartido externo de OneDrive o SharePoint Online en [Información general sobre el uso compartido externo](#). En general, el proceso difiere de Azure AD B2B de las siguientes maneras:

- OneDrive y SharePoint Online agregan usuarios al directorio después de que los usuarios han canjeado sus invitaciones. Por lo tanto, antes del canje, el usuario no se muestra en el portal de Azure AD. Si, mientras tanto, un usuario recibe una invitación de otro sitio, se genera una nueva invitación. Sin embargo, cuando se usa la colaboración B2B de Azure AD, los usuarios se agregan inmediatamente cuando se les invita por lo que se muestran en todas partes.
- La experiencia de canje en OneDrive y SharePoint Online parece diferente de la experiencia de colaboración B2B de Azure AD. Después de que un usuario canjea una invitación, las experiencias se asemejan.
- Los usuarios invitados a la colaboración B2B de Azure AD se pueden seleccionar en los cuadros de diálogo de uso compartido de OneDrive y SharePoint Online. Los usuarios invitados a OneDrive y SharePoint Online también se muestran en Azure AD después de que canjean sus invitaciones.
- Los requisitos de concesión de licencia son diferentes. Para más información sobre licencias, consulte [Concesión de licencias de Azure AD External Identities](#) y la [introducción al uso compartido externo de SharePoint Online](#). Para administrar el uso compartido externo en OneDrive o SharePoint Online con la colaboración B2B de Azure AD, establezca la configuración de uso compartido externo de OneDrive o SharePoint Online en **Allow sharing only with the external users that already exist in your organization's directory** (Permitir uso compartido solo con los usuarios externos que ya existan en el directorio de la organización). Los usuarios pueden acceder a los sitios compartidos externamente y elegir entre colaboradores externos que haya agregado el administrador. El administrador puede agregar los colaboradores externos a través de la API de invitación de colaboración B2B.

The screenshot shows the SharePoint admin center interface. On the left, there's a navigation bar with links like 'site collections', 'infopath', 'user profiles', 'bcs', and 'term store'. The main content area is titled 'Sharing outside your organization' with the sub-instruction 'Control how users share content with people outside your organization.' Below this, there are four options for sharing with external users:

- Don't allow sharing outside your organization
- Allow sharing only with the external users that already exist in your organization's directory
- Allow users to invite and share with authenticated external users
- Allow sharing to authenticated external users and using anonymous access links

The second option is highlighted with a red box.

Después de habilitar el uso compartido externo, la posibilidad de buscar usuarios invitados existentes en el selector de personas de SharePoint Online (SPO) está desactivada de manera predeterminada para así coincidir con el comportamiento heredado.

Para habilitarla, use la configuración "ShowPeoplePickerSuggestionsForGuestUsers" en el nivel de inquilino y colección de sitios. Para configurarla, use los cmdlets Set-SPOTenant y Set-SPOSite, que permiten que los miembros busquen a todos los usuarios invitados existentes en el directorio. Los cambios en el ámbito del inquilino no afectan los sitios de SPO que ya se aprovisionaron.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Incorporación de usuarios de colaboración B2B a un rol](#)
- [Delegación de las invitaciones de colaboración B2B](#)
- [Grupos dinámicos y colaboración B2B](#)
- [Solución de problemas de colaboración B2B de Azure Active Directory](#)

Experiencia de invitación de colaboración B2B de Azure Active Directory

18/02/2021 • 15 minutes to read • [Edit Online](#)

En este artículo se describen las maneras en las que los usuarios invitados pueden acceder a los recursos y el proceso de consentimiento que se encuentran. Si envía un correo electrónico de invitación al invitado, la invitación incluye un vínculo que este puede canjear para acceder a la aplicación o al portal. El correo electrónico de invitación es solo uno de los modos de acceso de los invitados a los recursos. Como alternativa, puede agregar invitados a su directorio y proporcionarles un vínculo directo al portal o a la aplicación que desee compartir. Independientemente del método que usen, la primera vez se les guiará por un proceso de consentimiento. Este proceso garantiza que los invitados acepten los términos de privacidad y los [términos de uso](#) que haya configurado.

Al agregar un usuario invitado al directorio, la cuenta de este tiene un estado de consentimiento (visible en PowerShell) que se establece inicialmente en **PendingAcceptance**. Esta configuración permanece hasta que el invitado acepta la invitación, la política de privacidad y los términos de uso. Después de eso, el estado de consentimiento cambia a **Accepted** y las páginas de consentimiento dejan de aparecer para el invitado.

IMPORTANT

- **A partir del 4 de enero de 2021**, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa Google Federation o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).
- **A partir del 31 de marzo de 2021**, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

Canje a través del correo electrónico de invitación

Al agregar un usuario invitado al directorio [mediante Azure Portal](#), se envía un correo electrónico de invitación al invitado. También puede enviar correos electrónicos de invitación cuando [use PowerShell](#) para agregar usuarios invitados al directorio. Esta es una descripción de la experiencia del invitado cuando canjea el vínculo del correo electrónico.

1. El invitado recibe un [correo electrónico de invitación](#) que se envía desde **Microsoft Invitations**.
2. El invitado selecciona **Aceptar invitación** en el correo electrónico.
3. El invitado usará sus propias credenciales para iniciar sesión en el directorio. Si el invitado no tiene una cuenta que se pueda federar al directorio y la característica [código de acceso de un solo uso \(OTP\)](#) de correo electrónico no está habilitada, se solicita al invitado que cree una cuenta [MSA](#) personal o una [cuenta de autoservicio de Azure AD](#). Consulte [Flujo de canje de invitación](#) para más información.
4. Al invitado se le guiará por la [experiencia de consentimiento](#) que se describe a continuación.

Canje a través de un vínculo directo

Como alternativa a la invitación por correo electrónico, puede darle al invitado un vínculo directo a la aplicación o al portal. Primero debe agregar el usuario invitado a su directorio mediante [Azure Portal](#) o [PowerShell](#). Puede

usar cualquiera de las [maneras personalizables para implementar las aplicaciones para los usuarios](#), incluidos los vínculos de inicio de sesión en directo. Cuando un invitado usa un vínculo directo en lugar de la invitación por correo electrónico, también se le guía por la experiencia de consentimiento inicial.

IMPORTANT

El vínculo directo debe ser específico del inquilino. En otras palabras, debe incluir un identificador de inquilino o dominio comprobado de manera que el invitado se puede autenticar en el inquilino donde se encuentra la aplicación compartida. Una dirección URL típica, como <https://myapps.microsoft.com>, no funcionará para un invitado, ya que redirige al inquilino principal para la autenticación. Estos son algunos ejemplos de vínculos directos con el contexto del inquilino:

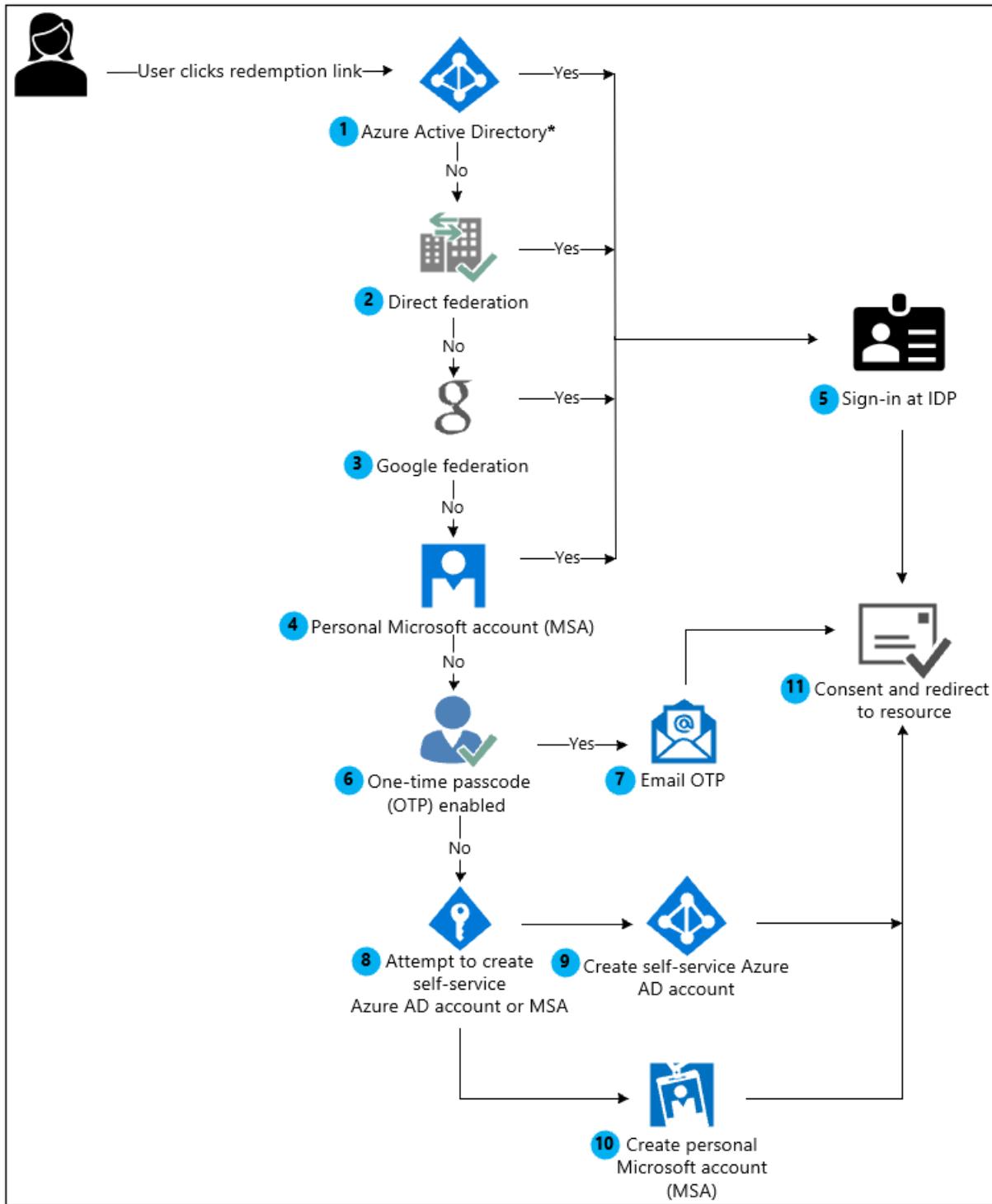
- Panel de acceso de aplicaciones: https://myapps.microsoft.com/?tenantid=<tenant_id>
- Panel de acceso de aplicaciones para un dominio comprobado: https://myapps.microsoft.com/<;verified_domain>
- Azure Portal: https://portal.azure.com/<tenant_id>
- Aplicación individual: consulte cómo usar un [vínculo de inicio de sesión en directo](#)

En algunos casos se recomienda el correo electrónico de invitación en lugar del vínculo directo. Si estos casos especiales son importantes para su organización, se recomienda que invite a los usuarios mediante métodos que aún envíen el correo electrónico de invitación:

- El usuario no tiene una cuenta de Azure AD, MSA o de correo electrónico en una organización federada. A menos que use la característica de código de acceso de un solo uso, el invitado deberá canjear la invitación por correo electrónico para que se le guíe para crear una MSA.
- A veces, el objeto de usuario invitado puede no tener una dirección de correo electrónico debido a un conflicto con un objeto de contacto (por ejemplo, un objeto de contacto de Outlook). En este caso, el usuario debe hacer clic en la dirección URL de canje en el correo electrónico de invitación.
- El usuario puede iniciar sesión con un alias de la dirección de correo electrónico a la que se invitó. (Un alias es una dirección de correo electrónico adicional asociada con una cuenta de correo electrónico). En este caso, el usuario debe hacer clic en la dirección URL de canje en el correo electrónico de invitación.

Flujo del canje de invitación

Cuando un usuario hace clic en el vínculo **Aceptar invitación** de un [correo electrónico de invitación](#), Azure AD canjea automáticamente la invitación basándose en el flujo de canje, del modo que se muestra a continuación:



*Si el nombre principal de usuario (UPN) del usuario coincide con una cuenta existente de Azure AD y de MSA personal, se le pedirá al usuario que elija la cuenta con la que desea realizar el canje.

1. Azure AD realiza la detección basada en usuarios para determinar si el usuario existe en un **inquilino de Azure AD existente**.
2. Si un administrador ha habilitado la **federación directa**, Azure AD comprueba si el sufijo de dominio del usuario coincide con el dominio de un proveedor de identidades SAML/WS-FED configurado y redirige al usuario al proveedor de identidades configurado previamente.
3. Si un administrador ha habilitado la **federación de Google**, Azure AD comprueba si el sufijo de dominio del usuario es gmail.com o googlemail.com y redirige al usuario a Google.
4. El proceso de canje comprueba si el usuario tiene una **cuenta de Microsoft (MSA)** personal existente.
5. Una vez identificado el **directorio principal** del usuario, el usuario se envía al proveedor de identidades

correspondiente para iniciar sesión.

6. Si en los pasos 1 a 4 no se encuentra el directorio principal del usuario al que se ha enviado la invitación, Azure AD determina si el inquilino que realiza la invitación tiene habilitada la característica de [código de acceso de un solo uso \(OTP\) de correo electrónico](#) para los invitados.
7. Si el [código de acceso de un solo uso de correo electrónico para invitados está habilitado](#), se envía un código de acceso al usuario por medio del correo electrónico de invitación. El usuario recuperará el código de acceso y lo escribirá en la página de inicio de sesión de Azure AD.
8. Si el código de acceso de un solo uso de correo electrónico para invitados está deshabilitado, Azure AD comprueba el sufijo de dominio para determinar si pertenece a una cuenta de consumidor. Si es así, se pedirá al usuario que cree una [cuenta Microsoft](#) personal. En caso contrario, se pedirá al usuario que cree una [cuenta de autoservicio de Azure AD](#).
9. Azure AD intenta crear una [cuenta de autoservicio de Azure AD](#) mediante la verificación del acceso al correo electrónico. Para realizar la comprobación de la cuenta, se envía un código al correo electrónico, código que el usuario debe recuperar y enviar a Azure AD. Sin embargo, si el inquilino del usuario al que se ha enviado la invitación está federado o si el campo AllowEmailVerifiedUsers está establecido en false en el inquilino del usuario invitado, este no puede completar el canje y el flujo da como resultado un error. Para más información, consulte [Solución de problemas de colaboración de Azure Active Directory B2B](#).
10. Se solicita al usuario que cree una [cuenta Microsoft \(MSA\)](#) personal.
11. Después de autenticarse en el proveedor de identidades correcto, se redirige al usuario a Azure AD para completar la [experiencia de consentimiento](#).

En el caso de canjes Just-in-Time (JIT), en los que el canje se realiza por medio de un vínculo de aplicación con inquilinos, no están disponibles los pasos del 8 al 10. Si un usuario alcanza el paso 6 y la característica de código de acceso de un solo uso de correo electrónico no está habilitada, recibe un mensaje de error y no puede canjear la invitación. Para evitar este error, los administradores deben [habilitar el código de acceso de un solo uso de correo electrónico](#) o asegurarse de que el usuario haga clic en un vínculo de invitación.

Experiencia de consentimiento para el invitado

Cuando un invitado iniciar sesión por primera vez para acceder a los recursos de una organización asociada, se le guía por las siguientes páginas.

1. El invitado debe revisar la página **Revisar permisos**, donde se describe la declaración de privacidad de la organización anfitriona. Para poder continuar, el usuario debe **Aceptar** el uso de su información de acuerdo con las directivas de privacidad de la organización anfitriona.



sam@outlook.com

Review permissions



This resource is not shared by Microsoft.

The organization Contoso would like to:

- ✓ Sign you in
- ✓ Read your name, email address, and photo

You should only accept if you trust Contoso. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. [Read Contoso's privacy statement](#). Contoso may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/contoso.com>

Cancel

Accept

NOTE

Para obtener información sobre cómo puede, como administrador de inquilinos, vincular con la declaración de privacidad de su organización, vea [Procedimiento: Incorporación de información de privacidad de su organización en Azure Active Directory](#).

2. Si se han configurado términos de uso, el invitado debe abrirlos y revisarlos y seleccionar Aceptar.

Access Panel Applications

Secure | https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOf...

Microsoft

Contoso LLC terms of use

In order to access Contoso LLC resources you must accept the terms of use.

Contoso Official Terms of Use >

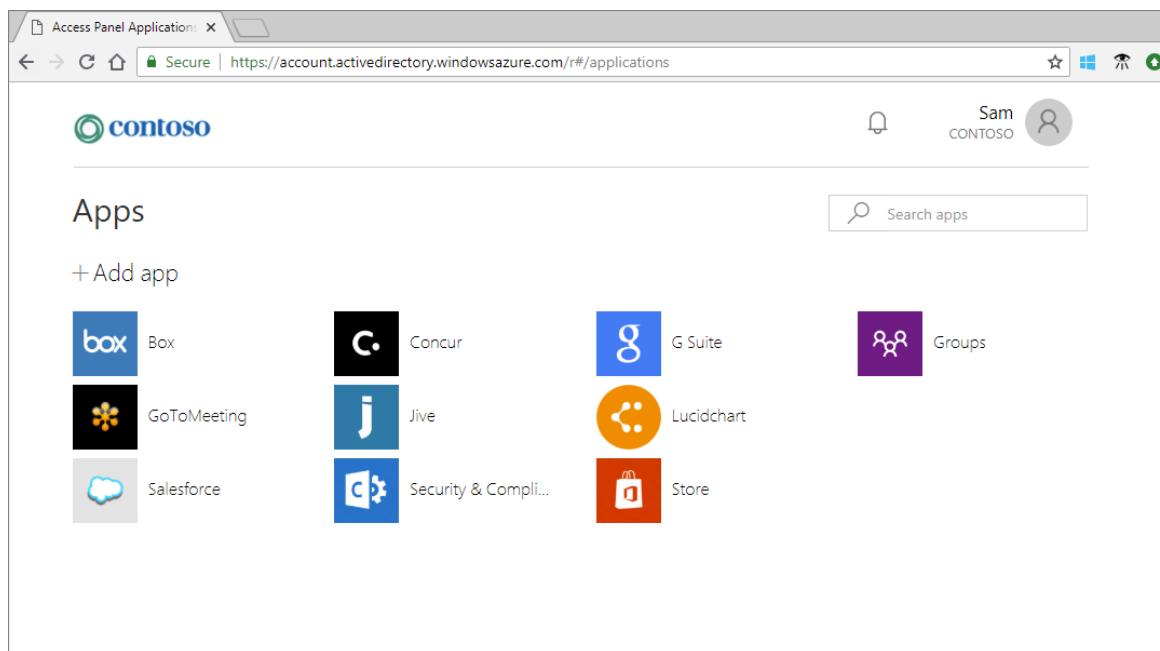
Choosing Accept means that you agree to all of the above terms of use.

Decline Accept

Privacy & cookies Terms of use Help Feedback ©2018 Microsoft

Puede configurar los Términos de uso en External Identities > Términos de uso.

3. A menos que se especifique otra cosa, al invitado se le redirige al panel de acceso a las aplicaciones, que enumera las aplicaciones a las que puede acceder.



En su directorio, el valor de **Invitación aceptada** cambia a Sí. Si se creó una MSA, el **Origen** del usuario muestra **Cuenta Microsoft**. Para más información sobre las propiedades de la cuenta de usuario invitado, consulte [Propiedades de un usuario de colaboración B2B de Azure Active Directory](#).

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#)
- [¿Cómo agregan los trabajadores de la información usuarios de colaboración B2B a Azure Active Directory?](#)
- [Incorporación de usuarios de colaboración B2B de Azure Active Directory con PowerShell](#)
- [Salir de una organización como usuario invitado](#)

Elementos del correo electrónico de invitación para la colaboración B2B: Azure Active Directory

18/02/2021 • 7 minutes to read • [Edit Online](#)

Los correos electrónicos de invitación son un componente fundamental para incorporar a los asociados como usuarios de colaboración B2B en Azure AD. Si bien [no es necesario que envíe un correo electrónico para invitar a alguien a usar la colaboración B2B](#), al hacerlo, se le proporciona al usuario toda la información que necesita para tomar una decisión sobre si aceptar la invitación. También le proporciona un vínculo al que siempre puede hacer referencia en el futuro cuando necesiten volver a los recursos.

The screenshot shows an email from Megan Bowen inviting April Montgomery to access applications within their organization. The email is from Microsoft Invitations on behalf of Contoso <invites@microsoft.com> and was sent on Tuesday, Oct 20 at 5:55 PM. It includes a warning about potential fraud and displays the organization's details (Contoso, contoso.com). A message from Megan Bowen states: "We're partnering a lot on this project, so I'm inviting you to access Contoso resources using your own username and password." Below the message is an 'Accept invitation' button. The footer contains privacy information and the Microsoft logo.

Explicación del correo electrónico

Se van a tratar algunos elementos del correo electrónico para saber cómo hacer el mejor uso de estas funcionalidades.

Asunto

El asunto del correo electrónico sigue este patrón:

<username> lo ha invitado a acceder a las aplicaciones de su organización.

Dirección De

Se usa un patrón similar a LinkedIn para la dirección De. Este patrón debe aclarar que, aunque el correo electrónico procede de invites@microsoft.com, la invitación viene de otra organización. El formato es: Microsoft Invitations`<tenantname>invites@microsoft.com` o invitaciones de Microsoft en nombre de `<tenantname>invites@microsoft.com`.

Responder a

En la respuesta al correo electrónico se indica el correo electrónico del invitador si está disponible, para que al responder al correo electrónico se vuelva a enviar un correo al invitador.

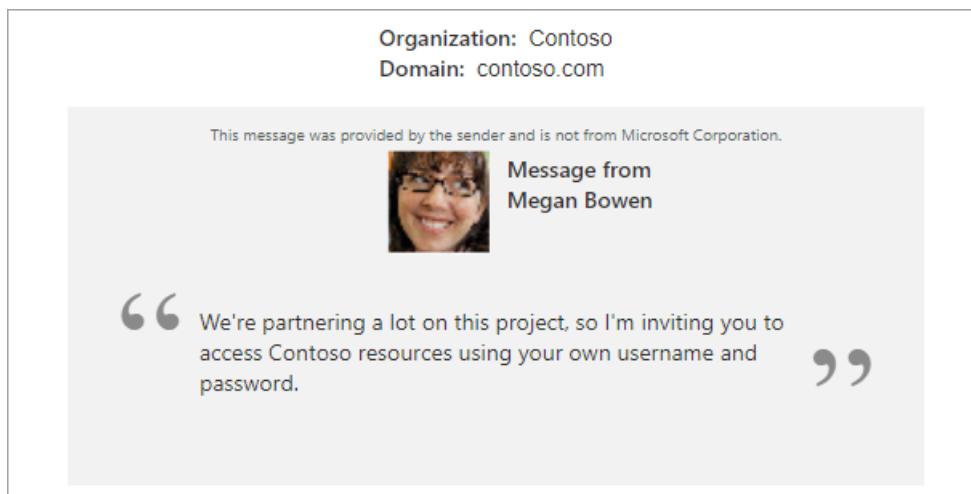
Advertencia de suplantación de identidad (phishing)

El correo electrónico comienza con una breve advertencia para el usuario sobre la suplantación de identidad (phishing) y lo alerta de que solo debe aceptar las invitaciones que espera. Es recomendable asegurarse de que los asociados a los que está invitando no se vean sorprendidos por su invitación, así es que es bueno que lo mencione con tiempo.

! Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

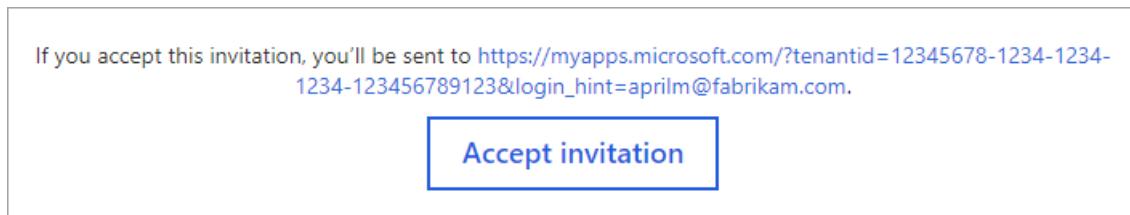
Información del invitador y mensaje de invitación

El correo electrónico incluye el nombre y el dominio principal asociados a la organización que envía la invitación. Esta información debe ayudar al invitado a tomar una decisión fundamentada sobre la aceptación de la invitación. Si el invitador incluye un mensaje como parte de su invitación cuando [invita a un usuario invitado al directorio, grupo o aplicación](#) o cuando [usa la API de invitación](#), el mensaje aparece resaltado en la sección principal del correo electrónico. También se incluye el nombre y la imagen de perfil del invitador, si se estableció. El mensaje mismo es un área de texto por lo que, por motivos de seguridad, no procesa etiquetas HTML.



Botón Aceptar y URL de redirecccionamiento

La sección siguiente del correo electrónico contiene información sobre adónde irá el invitado después de aceptar la invitación, así como un botón para hacerlo. En el futuro, el invitado siempre podrá usar este vínculo para volver directamente a los recursos.



Sección de pie de página

El pie de página contiene más información sobre la invitación que se envía. Siempre debe haber una opción para que el invitado bloquee las invitaciones futuras. Si la organización [estableció una declaración de privacidad](#), aquí debe aparecer el vínculo a dicha declaración. De lo contrario, una nota indica que la organización no ha establecido una declaración de privacidad.

[Block future invitations](#) from this organization.

This invitation email is from Contoso (contoso.com) and may include advertising content. Contoso has not provided a link to their privacy statement for you to review. Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the [Microsoft Privacy Statement](#).
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Bloqueo de una organización (cancelación de suscripción)

En la invitación de una organización, el pie de página contiene una opción para **bloquear las invitaciones futuras**. Un usuario invitado puede seleccionar este vínculo para bloquear cualquier invitación futura de la organización. Esta acción también agrega la organización a la lista de suscripciones canceladas del usuario en <https://invitations.microsoft.com/unsubscribe/manage>.

Visualización de las organizaciones que ha bloqueado

Un usuario invitado puede seguir estos pasos para ver o exportar las organizaciones que ha bloqueado:

1. Vaya a <https://invitations.microsoft.com/unsubscribe/manage>.
2. Escriba su correo electrónico y siga los pasos de inicio de sesión para la autenticación de código de acceso de un solo uso de correo electrónico.
3. Puede ver las organizaciones que ha bloqueado o exportar los nombres mediante copiar y pegar.

NOTE

Si desea permitir que una organización que ha bloqueado le invite de nuevo, puede elegir la organización y seleccionar **Siguiente**.

Cómo se determina el idioma

Las opciones siguientes determinan el idioma que el usuario invitado ve en el correo electrónico de invitación. Estas opciones de configuración se muestran en el siguiente orden de prioridad. Si una opción no está configurada, la siguiente de la lista será la que determine el idioma.

- La propiedad **messageLanguage** del objeto [guestUserMessageInfo](#), si se usa la API para crear una invitación.
- La propiedad **preferredLanguage** especificada en el [objeto de usuario](#) del invitado.
- El **idioma de notificación** establecido en las propiedades del inquilino principal del usuario invitado (solo para inquilinos de Azure AD).
- El **idioma de notificación** establecido en las propiedades del inquilino del recurso.

Si ninguna de estas opciones está configurada, el idioma se establece de forma predeterminada en inglés (EE. UU.).

Pasos siguientes

Consulte los siguientes artículos sobre la colaboración de B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [¿Cómo agregan los administradores de Azure Active Directory usuarios de colaboración B2B?](#)
- [¿Cómo agregan los trabajadores de la información usuarios de colaboración B2B?](#)
- [Canje de invitación de colaboración B2B](#)
- [Incorporación de usuarios de colaboración B2B sin invitación](#)

Propiedades de un usuario de colaboración B2B de Azure Active Directory

18/02/2021 • 13 minutes to read • [Edit Online](#)

En este artículo se describen las propiedades y los estados del objeto de usuario invitado B2B en Azure Active Directory (Azure AD) antes y después del canje de invitación. Un usuario de colaboración de negocio a negocio (B2B) de Azure AD es un usuario con UserType = Guest. Dicho usuario suele ser de una organización asociada y tiene, de forma predeterminada, privilegios limitados en el directorio de la invitación.

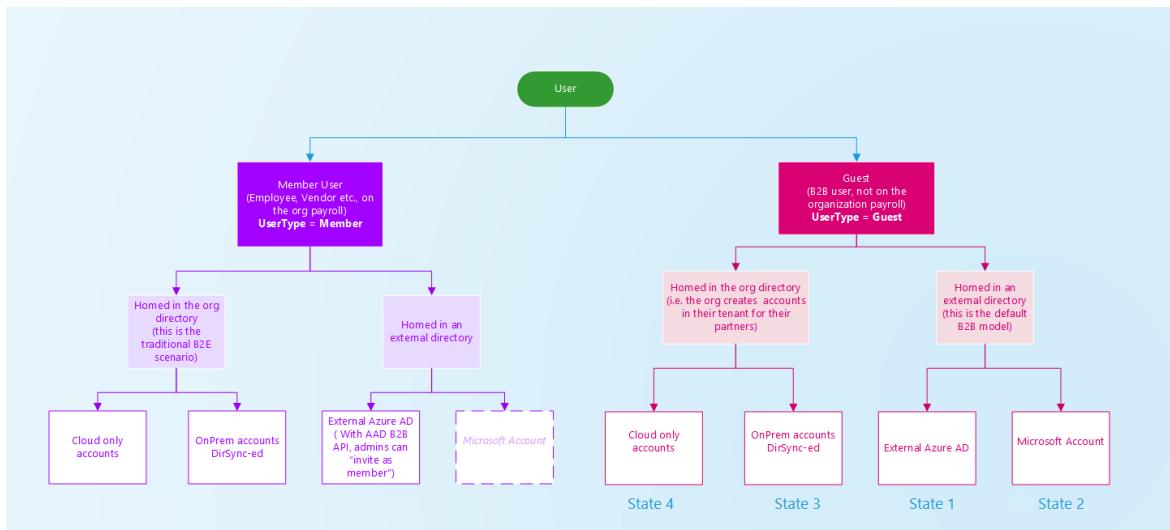
En función de las necesidades de la organización invitadora, un usuario de colaboración de B2B de Azure AD puede tener cualquiera de los siguientes estados de cuenta:

- Estado 1: alojado en una instancia externa de Azure AD y representado como un usuario invitado en la organización que invita. En este caso, el usuario de B2B inicia sesión con una cuenta de Azure AD que pertenece al inquilino invitado. Aunque la organización asociada no use Azure AD, se crea el usuario invitado en Azure AD. Los requisitos son que el usuario canjea su invitación y Azure AD comprueba su dirección de correo electrónico. Esta solución también se denomina inquilino Just-In-Time (JIT) o inquilino "viral".

IMPORTANT

A partir del 31 de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

- Estado 2: alojado en una cuenta Microsoft u otra cuenta y representado como usuario invitado en la organización host. En este caso, el usuario invitado inicia sesión con una cuenta de Microsoft o una cuenta social (google.com o similar). La identidad del usuario invitado se crea como una cuenta de Microsoft en el directorio de la organización que invita durante el canje de la oferta.
- Estado 3: alojado en la instancia de Active Directory local de la organización host y sincronizado con la instancia de Azure AD de la organización host. Puede usar Azure AD Connect para sincronizar las cuentas de asociado con la nube como usuarios B2B de Azure AD con UserType = Invitado. Vea [Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube](#).
- Estado 4: alojado en la instancia de Azure AD de la organización host con UserType = Invitado y credenciales que administra dicha organización.



Ahora, veamos cómo es un usuario de colaboración de B2B de Azure AD en Azure AD.

Antes del canje de la invitación

Las cuentas de estado 1 y estado 2 resultan de los usuarios invitados que invitan a colaborar con el uso de las propias credenciales de los usuarios invitados. Cuando se envía inicialmente la invitación al usuario invitado, se crea una cuenta en el directorio. Esta cuenta no tiene ninguna credencial asociada, ya que la autenticación la realiza el proveedor de identidades del usuario invitado. La propiedad **Origen** de la cuenta de usuario invitado del directorio se establece en **Usuario invitado**.

Name	First name	Last name
gsamooglegmail.com	---	---
User name	User type	Invitation accepted
gsamooglegmail.com	Guest	No
Object ID	Source	
8ea9cea8-1594-41bf...	Invited user	Resend invitation

Después del canje de la invitación

Una vez que el usuario invitado acepta la invitación, la propiedad **Origen** se actualiza según determine el proveedor de identidades del usuario invitado.

Para los usuarios invitados en estado 1, el **origen** es **Azure Active Directory externo**.

Home > Users - All users > Guest User1 - Profile

Guest User1 - Profile

User

Manage

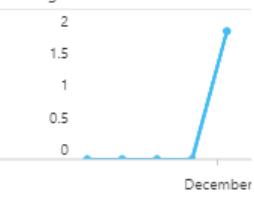
[Edit](#) [Reset password](#) [Delete](#)



Guest User1

guestuser1@fabrikam.com

User Sign-ins



Group memberships
0

Identity [edit](#)

Name	First name	Last name
Guest User1	---	---
User name	User type	Invitation accepted
guestuser1@fabrikam.com	Guest	Yes
Object ID	Source	
462cd2ac-018a-4194...	Edit	

Job info [edit](#)

Job title	Department	Manager
-----------	------------	---------

Para los usuarios invitados en estado 2, el origen es Cuenta Microsoft.

Home > Users - All users > gsamoogle - Profile

gsamoogle - Profile

User

Manage

[Edit](#) [Reset password](#) [Delete](#)



gsamoogle

gsamoogle@gmail.com

User Sign-ins



Group memberships
0

Identity [edit](#)

Name	First name	Last name
gsamoogle	---	---
User name	User type	Invitation accepted
gsamoogle@gmail.com	Guest	Yes
Object ID	Source	
8ea9cea8-1594-4...	Edit	

Job info [edit](#)

Job title	Department	Manager
-----------	------------	---------

Para los usuarios invitados en estado 3 y estado 4, la propiedad **Origen** se establece en Azure Active Directory o Windows Server Active Directory, como se describe en la siguiente sección.

Propiedades clave del usuario de colaboración de B2B de Azure AD

UserType

Esta propiedad indica la relación del usuario con el espacio host. Esta propiedad puede tener dos valores:

- Miembro: este valor indica un empleado de la organización host y un usuario en la plantilla de dicha organización. Por ejemplo, este usuario espera tener acceso solo a sitios internos. Este usuario no se considera como un colaborador externo.
- Invitado: Este valor indica un usuario que no se considera interno de la empresa, como un colaborador externo, un asociado o un cliente. No se espera que dicho usuario reciba una comunicación interna del CEO o que reciba beneficios de la empresa, por ejemplo.

NOTE

UserType no tiene relación alguna con la forma en que el usuario inicia sesión, el rol de directorio del usuario, etc.

Esta propiedad simplemente indica la relación del usuario con la organización host y permite a la organización exigir directivas que dependan de esta propiedad.

Para obtener detalles relacionados con los precios, consulte [Precios de Azure Active Directory](#).

Source

Esta propiedad indica la forma en que el usuario inicia sesión.

- Usuario invitado: este usuario ha recibido la invitación, pero aún no la ha canjeado.
- Azure Active Directory externo: este usuario está alojado en una organización externa y se autentica mediante una cuenta de Azure AD que pertenece a la otra organización. Este tipo de inicio de sesión corresponde al estado 1.
- Cuenta de Microsoft: el usuario está alojado en una cuenta de Microsoft y se autentica mediante una cuenta de Microsoft. Este tipo de inicio de sesión corresponde al estado 2.
- Windows Server Active Directory: este usuario inicia sesión desde una instancia de Active Directory local que pertenece a esta organización. Este tipo de inicio de sesión corresponde al estado 3.
- Azure Active Directory: este usuario se autentica mediante una cuenta de Azure AD que pertenece a esta organización. Este tipo de inicio de sesión corresponde al estado 4.

NOTE

Source y UserType son propiedades independientes. Un valor de Source no implica un valor concreto de UserType.

¿Se pueden agregar usuarios de B2B de Azure AD como miembros, en lugar de como invitados?

Normalmente, un usuario invitado y uno de B2B de Azure AD son sinónimos. Por tanto, de manera predeterminada los usuarios de colaboración de B2B de Azure AD se agregan como usuario con UserType = Guest. Sin embargo, en algunos casos, la organización asociada forma parte de una organización mayor a la que también pertenece la organización host. En ese caso, la organización host puede tratar a los usuarios de la organización asociada como miembros, en lugar de como invitados. Use las API del Administrador de invitaciones de B2B de Azure AD para agregar un usuario de la organización asociada a la organización host como miembro, o para invitarlo.

Filtro de usuarios invitados en el directorio

The screenshot shows the 'Users - All users' page in Microsoft Azure Active Directory. On the left, there's a sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Activity', 'Sign-ins', 'Audit logs', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area has buttons for 'New user', 'New guest user', 'Reset password', 'Delete user', 'Multi-Factor Authentication', and 'More'. A dropdown menu 'Show' is set to 'Guest users only'. The table lists six users:

NAME	USER NAME	USER TYPE	SOURCE
stdealer	stdealer@comcast.net	Guest	Microsoft Account
bryce	bryce@litwarecorp.com	Guest	Invited user
basarajesh	basarajesh@yahoo.com	Guest	Microsoft Account
Sanda	sanda@contoso.com	Guest	Azure Active Directory
Sarat Subramaniam	sarat@fabrikam.com	Guest	External Azure Active Directory
tjb2b	tjb2b@live.com	Guest	Invited user

Conversión de UserType

Es posible convertir UserType de miembro a invitado, y viceversa, mediante PowerShell. Sin embargo, la propiedad UserType representa la relación del usuario con la organización. Por tanto, debe cambiar esta propiedad solo si cambia la relación del usuario con la organización. Si cambia la relación del usuario, ¿se debe cambiar el nombre principal de usuario (UPN)? ¿Debe el usuario seguir teniendo acceso a los mismos recursos? ¿Debe asignarse un buzón de correo? No se recomienda cambiar el valor de UserType mediante el uso de PowerShell como una actividad atómica. Además, en caso de que esta propiedad se vuelva inmutable mediante PowerShell, no se recomienda depender de este valor.

Eliminación de limitaciones de usuarios invitados

Puede haber casos en los que desee ofrecer a los usuarios invitados privilegios más altos. Puede agregar un usuario invitado a cualquier rol e, incluso, eliminar las restricciones de usuario invitado predeterminadas en el directorio para concederle los mismos privilegios que a los miembros.

Se pueden desactivar las limitaciones predeterminadas para que un usuario invitado del directorio de la empresa tenga los mismos permisos que un usuario que sea miembro.

The screenshot shows the Microsoft - User settings page in the Azure Active Directory portal. The left sidebar has a search bar and a list of options: App registrations, App registrations (Preview), Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings (which is selected and highlighted in blue), Properties, and Notifications settings. Below these are two sections: Security (Identity Secure Score (Preview) and Conditional Access). The main pane has a 'Save' and 'Discard' button at the top. It contains several configuration sections: Enterprise applications (Manage how end users launch and view their applications), App registrations (Users can register applications: Yes or No), Administration portal (Restrict access to Azure AD administration portal: Yes or No), External users (Manage external collaboration settings), and Access panel (Manage settings for access panel preview features).

¿Puedo hacer visibles a los usuarios invitados en la lista global de direcciones de Exchange?

Sí. De forma predeterminada, los objetos de invitado no aparecen en la lista global de direcciones de la organización, pero puede usar Azure Active Directory PowerShell para que figuren. Para más información, consulte [¿Puedo hacer visibles los objetos de invitado de la lista global de direcciones?](#) en [Administración del acceso de invitados en grupos de Microsoft 365](#).

¿Puedo actualizar la dirección de correo electrónico de un usuario invitado?

Si un usuario invitado acepta su invitación y cambia posteriormente su dirección de correo electrónico, el nuevo correo electrónico no se sincroniza automáticamente con el objeto de usuario invitado en el directorio. La propiedad mail se crea a través de [Microsoft Graph API](#). Puede actualizar la propiedad de correo electrónico mediante Microsoft Graph API, el centro de administración de Exchange o [PowerShell de Exchange Online](#). El cambio se reflejará en el objeto de usuario invitado de Azure AD.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Tokens de usuario de colaboración B2B](#)
- [Asignación de notificaciones de usuario de colaboración B2B](#)

Asignación de notificaciones de usuario de colaboración B2B de Azure Active Directory

18/02/2021 • 2 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) admite la personalización de las notificaciones emitidas en el token SAML para los usuarios de colaboración B2B. Cuando un usuario se autentique en la aplicación, Azure AD emitirá un token SAML a la aplicación que contiene información (o notificaciones) sobre el usuario que lo identifica de forma única. De forma predeterminada, dicha información incluye el nombre de usuario, la dirección de correo electrónico, el nombre y los apellidos del usuario.

En [Azure Portal](#) puede ver o editar las notificaciones que se envían en el token SAML a la aplicación. Para acceder a la configuración, seleccione **Azure Active Directory > Aplicaciones empresariales >** la aplicación que está configurada para el inicio de sesión único > **Inicio de sesión único**. Consulte la configuración del token SAML en la sección **Atributos del usuario**.

The screenshot shows the 'User Attributes' section of the Azure portal. It includes a 'User Identifier' dropdown set to 'user.userprincipalname', a checked checkbox for 'View and edit all other user attributes', and a table of 'SAML Token Attributes' with four entries: givenname, surname, emailaddress, and name, each mapped to their respective Azure AD properties.

NAME	VALUE	NAMESPACE
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims ...
surname	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims ...
emailaddress	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims ...
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims ...

Hay dos razones posibles por las que puede que tenga que editar las notificaciones que se emiten en el token SAML:

1. La aplicación requiere un conjunto diferente de URI o valores de notificación.
2. La aplicación requiere que la notificación NameIdentifier tenga un valor que no sea el del nombre principal de usuario (UPN) almacenado en Azure AD.

Para más información acerca de cómo agregar y editar notificaciones, consulte [Personalización de las notificaciones emitidas en el token SAML para aplicaciones empresariales en Azure Active Directory](#).

Para los usuarios de colaboración B2B, por motivos de seguridad, se evita realizar la asignación de NameID y UPD entre inquilinos.

Pasos siguientes

- Para más información acerca de las propiedades de usuario de colaboración B2B, consulte [Propiedades de un usuario de colaboración B2B de Azure Active Directory](#).
- Para más información acerca de los tokens de usuario para los usuarios de colaboración B2B, consulte [Información sobre los tokens de usuario de la colaboración B2B de Azure Active Directory](#).

Información sobre los tokens de usuario de la colaboración B2B de Azure Active Directory

18/02/2021 • 2 minutes to read • [Edit Online](#)

Si le interesa conocer el aspecto del token de un usuario de colaboración B2B, estos son los detalles del token de portador y el contenido del token para un invitado de Azure Active Directory (Azure AD) y un invitado de una cuenta de Microsoft en el inquilino de recursos (para el identificador de inquilino: 04dcc6ab-388a-4559-b527-fbec656300ea). Para ver el contenido de JSON Web Token (JWT), use <https://jwt.io/> o <https://jwt.ms/>.

Token de invitado de Azure AD

```
Authorization: Bearer  
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ilk0dWVLm9hSU5RaVFiNVlFQ1NZVn1EY3BBVSIsImtpZCI6Ilk0dWVLm9hSU5RaVFiNVlFQ1NZVn1EY3BBVSIsImtpZCI6Ilk0dWVLm9hSU5RaVFiNVlFQ1NZVn1EY3BBVSJ9.eyJhdWQiOiJodHRwczovL2dyYXB0LndpbmRvd3MubmV0LyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzA0ZGNjNmFiLTM40GEtNDU1OS1iNTI3LWZiZWM2NTyZMDB1YS8iLCJpYXQiOjE0ODQ4MDM5MTgsIm5iZiI6MTQ4NDgwMzkxOCwiZXhwIjoxNDg0ODA3ODE4LCJhY3Ii0iIxIiwiYwlvIjoiQVFQkFBURFBURST11sUTNkaFJTcm0tNEstYWRwQ0pJNWNNcGtYQ0VOTHdnN1Z1emhFQURIajNOONWNMzhRWGFBAkhrYUtPRFhneWJpcnVRVhpa3RZZ3I2M0xMQTVVD1EeXV2dEtQSud1XzJpVFRhdjNqSkxuT1RSZ2JWRFpwckhSaEtzbW15RWdBQSIsImFsdHN1Y21kIjoiNt06MTAwMzAwMDA4MDFCQUZDNyIsImFtcii6WjJwd2QiLCJyc2EiXswiYXBwaWQiOijjNDRiNDA4My0zYmIwLTQ5YzEtYjQ3ZC05NzR1NTnjYmRmM2MiLCJhcHBpZGFJciI6IjIiLCJ1X2V4cCI6MTA4MDAsImVtYwlsIjoiCmFqZXNiQG1pY3Jvc29mdC5jb20iLCJpZHAIoIjodHRwczovL3N0cy53aw5kb3dzLm51dC83MmY50DhiZi04NmYxLTQxYWYtOTFhYi0yZDdjZDAXMWRIrNDcvIiwiaw5fY29ycCI6InRydWUiLCJpcGFkZHIoiIxNcuMjIwLjEuMTk1IiwiBmFtZSI6InJhamVzaCIsIm9pZCI6IjA10DAtY2M1LTgxMWUtdNDziZC1iMWi2LTU5NDz1NjY40DIyZiIsInBsYXRmIjoiMyIsInB1aWQiOiiXMDAzM0ZGRj1EOEY50TUzIiwiC2NwIjoidXNlc19pbXBlcNvbmf0aw9uIiwiC3ViIjoiS1d3QnVCNk5R0U5UYmpoSUI10HewM2FlQv16cEk2TwixMkpncGk1aV9ITSIsInRpZCI6IjA0ZGNjNmFiLTM40GEtNDU1OS1iNTI3LWZiZWM2NTyZMDB1YSIsInVuaXF1ZV9uYw11IjoiCmFqZXNiQG1pY3Jvc29mdC5jb20iLCJ2ZXi0iIxLjAifQ.V1lr1hGXpB1pXDBKRHHybMr_1_DwKNY3eCobBoFexJirwqujcZodPrAkIOj1FYyhkILyHZQui_D1w7XoPsd6U4GQlg0OfFzbye-P_NdRFabHmlv32gCgHz1xo11aPP453EiwwG50HnWaHYLBpuqi3sNeKx06xbTFj07HmADDaR4aM0jwy031d6GkD0Ldu-Xkazi-h8parvRLokkLZA0oxMFoxl_-VHr1h0zxCkbWgRoug4t97161i5tGi199CcpJ6NK8uQld7TveC40sjsj735ksn-Uq_NzcJuXCEVsH0xK5evaefBFSEqACXjkTtvYkJwtAx8Kr8yWZAcEg0YMQ
```

Token de cuenta Microsoft para invitados

```
Authorization: Bearer  
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ilk0dWVLm9hSU5RaVFiNVlFQ1NZVn1EY3BBVSIsImtpZCI6Ilk0dWVLm9hSU5RaVFiNVlFQ1NZVn1EY3BBVSJ9.eyJhdWQiOiJodHRwczovL2dyYXB0LndpbmRvd3MubmV0LzA0ZGNjNmFiLTM40GEtNDU1OS1iNTI3LWZiZWM2NTyZMDB1YS8iLCJpYXQiOjE0ODQ4MDMwNjEsIm5iZiI6MTQ4NDgwMza2MSwiZXhwIjoxNDg0ODA20TYxLCJhY3Ii0iIxIiwiYwlvIjoiQVFQkFBURFBURST11sUTNkaFJTcm0tNEstYWRwQ0pEeEd4a3lUdmJ2d1RoSHJnTEDPaGZEbtA1aXJndC11R1d3YT15QUZQQTJQc19nZHF2bhQ1X1AtaDhrT2Iwdudza3dyYk1BbUhvMetRM005N2ZCV1RtdzRKY0NfaFvkW1PZ25QYV1OY1BRQXB1YmFMcUlaZGhaRXhtQVZjeXFmaElBQSIsImFsdHN1Y21kIjoiMTpsaXZ1LmNvbTowMDAzMDAwMEEwNzBCOTYyIiwiYw1IjpbInB3ZCJdLCJhcHBpZCI6ImM0NG10MDgZLTNiyJatNDljMS1iNDdkLTk3NGU1M2NizGYZyYiIsImFwcG1kYwNyIjoiMiIsImVfZXhwIjoxMDgwMCwiZW1haWWi0iJiYXNhcmFqZXNoQGxpdmUuY29tIiwiZmFtaWx5X25hbWuioiJiYXNhIiwiZ21Zw5fbmftZSI6InJhamVzaCIsImlkci6ImxpdmuUy29tIiwiiaXbhZGRyIjoiMTY3LjIyMC4xLjE5NSiIsIm5hbWUiOjjiYXNhcmFqZXNoIiwiB21kIjoiMju0NmU3NDEtNmZjn100ZDI0LTg2NTQtZjkyNdC5MzI0zjM3IiwiCgXhdGyioiIzIiwiChvPZCI6IjEwMDMzRkZGOURBqjk2NDYiLCJzY3Ai0iJ1c2Vyx2ltcGVyc29uYXRpb24iLCJzdWIoiI4Y2N50Eh4cmE5UT12aGdY0XhBODFBewJEV3dsVmwxjXzRBZVJYZ21zamM4IiwiidG1kIjoiMDRky2M2YwItMzg4YS00NTU5LWI1MjctZmJ1YzY1NjMwMGVhIiwidW5pcXv1X25hbWuoijsaXZ1LmNvbSNiYXNhcmFqZXNoQGxpdmUuY29tIiwidmVyIjoiMS4wIn0.LSB1JpElXpsGX0GaFINW-j0BHsI0Dxe3oX-YIEsccegDCsp16UnRjpws0nBL09B4N0oqlD7ZwZAQRpgaaFnWvR0xkIGpNTE_ppSKU1suud8keG5VnTeEu82em95G1_c_eW1n0emPvbADC8h08p2wxNm8QyEhmYqauN6qYbeqOnioRERX03zOPg8nSXFcGPvhvumJ_BW8XKnW4zLdhK78c3PgynPnwtIm08SksMRDzGMgUc9RK1bpPQtgX8iFQByEljf5cuE_h_e1Nr5Y4strhs3JciQLTYZ727YY-1Sm5DERiQrt7MkP5BhprEmSByofSvAcj5TmVdqBFUjobuA
```

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Propiedades de usuario de la colaboración B2B](#)

- Asignación de notificaciones de usuario de colaboración B2B

Acceso condicional para usuarios de colaboración B2B

18/02/2021 • 13 minutes to read • [Edit Online](#)

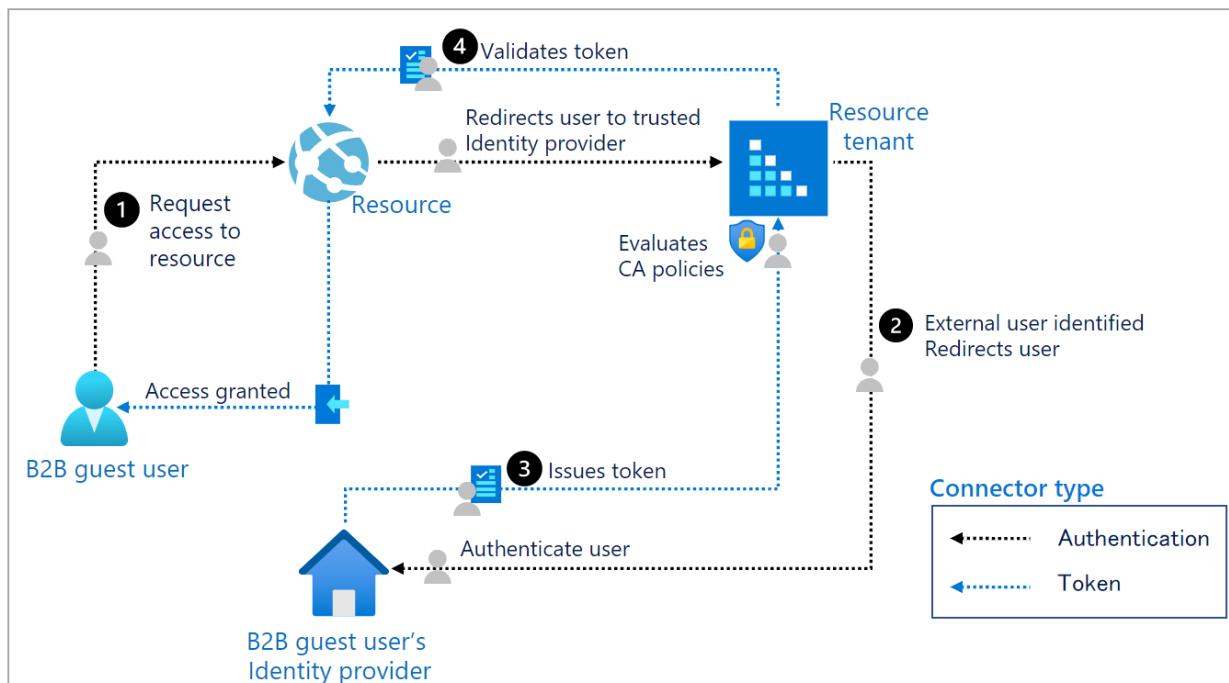
En este artículo se describe cómo las organizaciones pueden examinar las directivas de acceso condicional (CA) para que los usuarios invitados de B2B tengan acceso a sus recursos.

NOTE

Este flujo de autenticación o autorización es un poco diferente para los usuarios invitados que para los usuarios existentes de ese proveedor de identidades (IdP).

Flujo de autenticación para usuarios invitados de B2B desde un directorio externo

En el diagrama siguiente se ilustra el flujo:

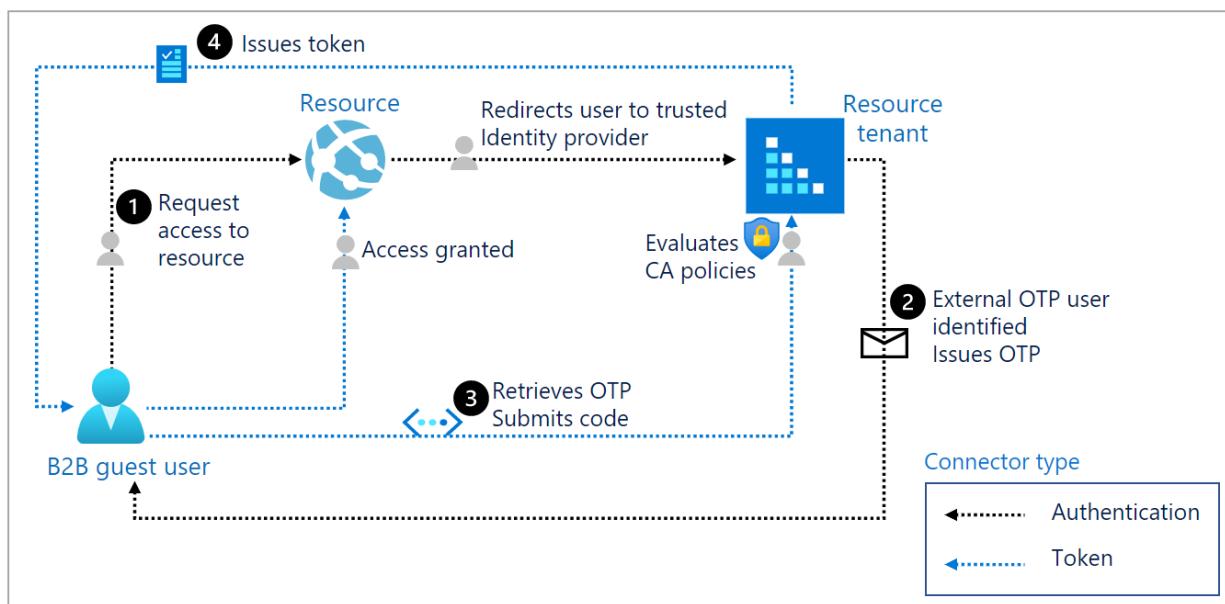


PASO	DESCRIPCIÓN
1.	El usuario invitado de B2B solicita acceso a un recurso. El recurso redirige al usuario a su inquilino de recursos, un IdP de confianza.
2.	El inquilino de recursos identifica al usuario como externo y redirige al usuario al IdP del usuario invitado de B2B. El usuario realiza la autenticación principal en el IdP.

PASO	DESCRIPCIÓN
3.	El IdP del usuario invitado de B2B emite un token para el usuario. El usuario se redirige de nuevo al inquilino de recursos con el token. El inquilino de recursos valida el token y luego evalúa el usuario con sus directivas de CA. Por ejemplo, el inquilino de recursos puede requerir que el usuario realice una autenticación multifactor de Azure Active Directory (AD).
4.	Una vez que se cumplen todas las directivas de CA de inquilino de recursos, el inquilino de recursos emite su propio token y redirige al usuario a su recurso.

Flujo de autenticación para usuarios invitados de B2B con código de acceso de un solo uso

En el diagrama siguiente se ilustra el flujo:



PASO	DESCRIPCIÓN
1.	El usuario solicita acceso a un recurso de otro inquilino. El recurso redirige al usuario a su inquilino de recursos, un IdP de confianza.
2.	El inquilino de recursos identifica al usuario como un usuario de código de acceso de un solo uso (OTP) de correo electrónico externo y envía al usuario un correo electrónico con el OTP.
3.	El usuario recupera el OTP y envía el código. El inquilino de recursos evalúa el usuario con sus directivas de CA.
4.	Una vez que se cumplen todas las directivas de CA, el inquilino de recursos emite un token y redirige al usuario a su recurso.

NOTE

Si el usuario es de un inquilino de recursos externos, no es posible evaluar también las directivas de CA de IdP del usuario invitado de B2B. A partir de hoy, solo las directivas de CA del inquilino de recursos se aplican a sus invitados.

Azure AD Multi-Factor Authentication para usuarios de B2B

Las organizaciones pueden exigir varias directivas de Azure AD Multi-Factor Authentication para los usuarios invitados de B2B. Estas directivas se pueden exigir en el nivel de inquilino, aplicación o usuario individual, del mismo modo que pueden habilitarse para empleados a tiempo completo y miembros de la organización. El inquilino de recursos siempre es responsable de la ejecución de Azure AD Multi-Factor Authentication para los usuarios, aunque la organización del usuario invitado tenga funciones de Multi-Factor Authentication. Este es un ejemplo:

1. Un administrador o un trabajador de la información de una empresa denominada Fabrikam invita a un usuario de otra compañía llamada Contoso a usar su aplicación Woodgrove.
2. La aplicación Woodgrove en Fabrikam está configurada para requerir Azure AD Multi-Factor Authentication en el acceso.
3. Cuando el usuario invitado de B2B de Contoso intenta acceder a Woodgrove en el inquilino de Fabrikam, se le pide que complete la comprobación de Azure AD Multi-Factor Authentication.
4. A continuación, el usuario invitado puede configurar su instancia de Azure AD Multi-Factor Authentication con Fabrikam y seleccionar las opciones.
5. Este escenario funciona con cualquier identidad: Azure AD o una cuenta de Microsoft personal (MSA). Por ejemplo, si el usuario de Contoso se autentica con el id. social.
6. Fabrikam debe tener suficientes licencias Prémium de Azure AD que admitan Azure AD Multi-Factor Authentication. El usuario de Contoso consume esta licencia de Fabrikam. Consulte el [modelo de facturación para Azure AD External Identities](#) para información sobre las licencias de B2B.

NOTE

La comprobación de Azure AD Multi-Factor Authentication se realiza en el inquilino de recursos para garantizar la previsibilidad.

Configuración de Azure AD Multi-Factor Authentication para usuarios de B2B

Para configurar Azure AD Multi-Factor Authentication para los usuarios de colaboración B2B, vea este vídeo:

Azure AD Multi-Factor Authentication de usuarios de B2B para el canje de ofertas

Para obtener más información sobre la experiencia de canje de Azure AD Multi-Factor Authentication, vea este vídeo:

Restablecimiento de Azure AD Multi-Factor Authentication para usuarios de B2B

Ahora, los siguientes cmdlets de PowerShell están disponibles para la prueba de los usuarios invitados de B2B:

1. Conectarse a Azure

```
$cred = Get-Credential  
Connect-MsolService -Credential $cred
```

2. Obtenga todos los usuarios con los métodos de prueba.

```
Get-MsolUser | where { $_.StrongAuthenticationMethods } | select UserPrincipalName, @{n="Methods";e=($_.StrongAuthenticationMethods).MethodType}
```

Este es un ejemplo:

```
Get-MsolUser | where { $_.StrongAuthenticationMethods } | select UserPrincipalName, @{n="Methods";e=($_.StrongAuthenticationMethods).MethodType}
```

3. Restablezca el método de Azure AD Multi-Factor Authentication de un usuario específico para exigir que el usuario de colaboración B2B establezca de nuevo los métodos de prueba. Este es un ejemplo:

```
Reset-MsolStrongAuthenticationMethodByUpn -UserPrincipalName gsamooglegmail.com#EXT#@  
WoodGroveAzureAD.onmicrosoft.com
```

Acceso condicional para usuarios de B2B

Hay varios factores que influyen en las directivas de CA para los usuarios invitados de B2B.

Acceso condicional basado en dispositivos

En CA, hay una opción para requerir que el [dispositivo de un usuario sea compatible o con conexión a Azure AD híbrido](#). Los usuarios invitados de B2B solo pueden satisfacer el requisito de compatibilidad si el inquilino de recursos puede administrar su dispositivo. Los dispositivos no pueden estar administrados por más de una organización a la vez. Los usuarios invitados de B2B no pueden satisfacer el requisito de conexión a Azure AD híbrido porque no tienen una cuenta de AD local. Solo en el caso de que el dispositivo del usuario invitado no esté administrado, pueden registrar o inscribir su dispositivo en el inquilino de recursos y luego hacer que el dispositivo sea compatible. A continuación, el usuario puede cumplir con el control de concesión.

NOTE

No se recomienda requerir un dispositivo administrado para los usuarios externos.

Directivas de administración de aplicaciones móviles

Los controles de concesión de CA, como **Require approved client apps** (Requerir aplicaciones cliente aprobadas) y **Require app protection policies** (Requerir directivas de protección de aplicación), necesitan que el dispositivo esté registrado en el inquilino. Estos controles solo pueden aplicarse a [dispositivos iOS y Android](#). Sin embargo, ninguno de estos controles se puede aplicar a los usuarios invitados de B2B si el dispositivo del usuario ya está administrado por otra organización. Un dispositivo móvil no se puede registrar en más de un inquilino a la vez. Si otra organización administra el dispositivo móvil, se bloqueará al usuario. Solo en el caso de que el dispositivo del usuario invitado no esté administrado, pueden registrar su dispositivo en el inquilino de recursos. A continuación, el usuario puede cumplir con el control de concesión.

NOTE

No se recomienda requerir una directiva de protección de aplicaciones para los usuarios externos.

Acceso condicional basado en la ubicación

La [directiva basada en la ubicación](#) que se fundamenta en intervalos IP se puede aplicar si la organización que invita puede crear un intervalo de direcciones IP de confianza que defina sus organizaciones asociadas.

Las directivas también se pueden aplicar en función de las [ubicaciones geográficas](#).

Acceso condicional basado en riesgos

La [directiva de riesgo de inicio de sesión](#) se aplica si el usuario invitado de B2B cumple el control de concesión. Por ejemplo, una organización puede requerir Azure AD Multi-Factor Authentication para el riesgo medio o alto de inicio de sesión. Sin embargo, si un usuario no se ha registrado previamente en Azure AD Multi-Factor Authentication en el inquilino de recursos, se bloqueará el usuario. Esto se hace para evitar que usuarios malintencionados registren sus propias credenciales de Azure AD Multi-Factor Authentication en el caso de que pongan en peligro la contraseña de un usuario legítimo.

Sin embargo, la [directiva de riesgo de usuario](#) no se puede resolver en el inquilino de recursos. Por ejemplo, si necesita un cambio de contraseña para usuarios invitados de alto riesgo, estos se bloquearán debido a la imposibilidad de restablecer las contraseñas en el directorio de recursos.

Acceso condicional con condición de aplicaciones cliente

Las [condiciones de las aplicaciones cliente](#) se comportan de la misma manera para los usuarios invitados de B2B que para cualquier otro tipo de usuario. Por ejemplo, puede impedir que los usuarios invitados usen protocolos de autenticación heredados.

Controles de sesión de acceso condicional

Los [controles de sesión](#) se comportan de la misma manera para los usuarios invitados de B2B que para cualquier otro tipo de usuario.

Pasos siguientes

Para más información, consulte los siguientes artículos sobre la Colaboración B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Protección de identidades y usuarios de Colaboración B2B](#)
- [Precios de identidades externas](#)
- [Preguntas más frecuentes \(P+F\)](#)

Colaboración B2B de Azure Active Directory para organizaciones híbridas

18/02/2021 • 4 minutes to read • [Edit Online](#)

La colaboración B2B de Azure Active Directory (Azure AD) facilita que pueda proporcionar a los asociados externos acceso a las aplicaciones y recursos de la organización. Esto es cierto incluso en una configuración híbrida en la que hay recursos locales y en la nube. No importa si actualmente administra las cuentas de asociados externos localmente en el sistema de identidades o si administra las cuentas externas en la nube como usuarios de Azure AD B2B. Ya puede conceder a estos usuarios acceso a los recursos en cualquier ubicación mediante las mismas credenciales de inicio de sesión para ambos entornos.

Conceder a los usuarios B2B de Azure AD acceso a las aplicaciones locales

Si la organización usa las funcionalidades de colaboración B2B de Azure AD para invitar a los usuarios invitados de organizaciones asociadas a su instancia de Azure AD, ahora puede proporcionar a estos usuarios B2B acceso a las aplicaciones locales.

Para aquellas aplicaciones que usan la autenticación basada en SAML, puede hacer que esas aplicaciones estén disponibles para los usuarios B2B en Azure Portal usando Azure AD Application Proxy para la autenticación.

Para aquellas aplicaciones que usan la autenticación integrada de Windows (IWA) con la delegación restringida de Kerberos (KCD), también puede usar Azure AD Application Proxy para la autenticación. No obstante, para que la autorización funcione, se requiere que un objeto de usuario esté en la instancia local de Windows Server Active Directory. Hay dos métodos que puede usar para crear objetos de usuario locales que representen a los usuarios B2B invitados.

- Puede usar Microsoft Identity Manager (MIM) 2016 SP1 y el agente de administración de MIM para Microsoft Graph.
- Puede usar un script de PowerShell. (Esta solución no necesita MIM).

Para más información sobre cómo implementar estas soluciones, consulte [Conceder a los usuarios B2B de Azure AD acceso a las aplicaciones locales](#).

Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube

Antes de Azure AD, las organizaciones con sistemas de identidad locales administraban tradicionalmente las cuentas de asociado en sus directorios locales. Si es una organización de este tipo, querrá asegurarse de que los socios seguirán teniendo acceso cuando mueva las aplicaciones y demás recursos a la nube. Idealmente, querrá que estos usuarios utilicen el mismo conjunto de credenciales para acceder a los recursos locales y en la nube.

Ahora se ofrecen métodos en los que puede usar Azure AD Connect para sincronizar estas cuentas locales en la nube como "usuarios invitados", en los que las cuentas se comportan de igual manera que los usuarios B2B de Azure AD.

Para ayudar a proteger los datos de su empresa, puede controlar el acceso solo a los recursos adecuados y configurar directivas de autorización que traten a estos usuarios invitados de manera diferente a los empleados.

Para más información sobre la implementación, consulte [Conceder a las cuentas de asociado administradas](#)

localmente acceso a los recursos en la nube mediante la colaboración B2B de Azure AD.

Pasos siguientes

- Conceder a los usuarios B2B de Azure AD acceso a las aplicaciones locales
- Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube mediante la colaboración B2B de Azure AD

Proveedores de identidades para External Identities

18/02/2021 • 6 minutes to read • [Edit Online](#)

Un *proveedor de identidades* crea, mantiene y administra la información de identidad al tiempo que proporciona servicios de autenticación a las aplicaciones. Al compartir aplicaciones y recursos con usuarios externos, Azure AD es el proveedor de identidades predeterminado para el uso compartido. Esto significa que, al invitar a usuarios externos que ya tienen una cuenta de Azure AD o de Microsoft, estos pueden iniciar sesión automáticamente sin tener que realizar ninguna configuración adicional.

Sin embargo, puede permitir que los usuarios inicien sesión con varios proveedores de identidades.

- **Google:** La federación de Google permite a usuarios externos canjear invitaciones que les haya enviado si inician sesión en sus aplicaciones con sus propias cuentas de Gmail. La federación de Google también se puede usar en los flujos de usuario de registro de autoservicio.

IMPORTANT

A partir del 4 de enero de 2021, Google retira la compatibilidad con el inicio de sesión en WebView. Si usa la federación de Google o el registro de autoservicio con Gmail, debería comprobar la compatibilidad de las aplicaciones nativas de línea de negocio.

NOTE

En la versión preliminar del registro de autoservicio actual, si un flujo de usuario está asociado a una aplicación y le envía a un usuario una invitación a esa aplicación, el usuario no podrá utilizar una cuenta de Gmail para canjear la invitación. Como solución alternativa, el usuario puede pasar por el proceso de registro de autoservicio. O bien, para canjear la invitación, puede acceder a otra aplicación o usar el portal Mis aplicaciones en <https://myapps.microsoft.com>.

- **Facebook:** al compilar una aplicación, puede configurar el registro de autoservicio y habilitar la federación de Facebook para que los usuarios puedan suscribirse a la aplicación con sus propias cuentas de Facebook. Facebook solo se puede usar para flujos de usuario de registro de autoservicio y no está disponible como una opción de inicio de sesión cuando los usuarios canjean las invitaciones que les envíe.
- **Federación directa:** también puede configurar la federación directa con cualquier proveedor de identidades externo que admita los protocolos SAML o WS-Fed. La federación directa permite a los usuarios externos canjear invitaciones que les haya enviado si inician sesión en sus aplicaciones con sus cuentas empresariales o de redes sociales existentes.

NOTE

Los proveedores de identidades de federación directa no se pueden usar en los flujos de usuario de inicio de registro de autoservicio.

Funcionamiento

La característica de registro de autoservicio Identidades externas de Azure AD permite a los usuarios registrarse con su cuenta de Azure AD, Google o Facebook. Para configurar proveedores de identidades sociales en el

inquilino de Azure AD, creará una aplicación en cada proveedor de identidades y configurará las credenciales. Obtendrá un id. de cliente o de aplicación y un secreto de cliente o de aplicación, que puede agregar a su inquilino de Azure AD.

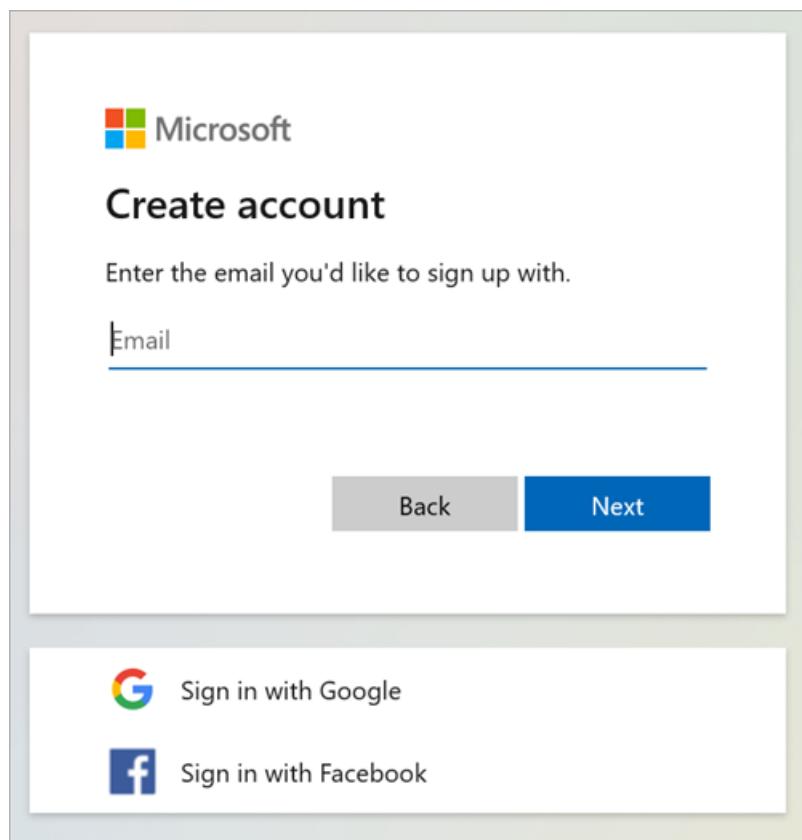
Una vez que haya agregado un proveedor de identidades a su inquilino de Azure AD:

- Cuando invite a un usuario externo a las aplicaciones o recursos de la organización, el usuario externo puede iniciar sesión con la cuenta que tenga con ese proveedor de identidades.
- Al habilitar el [registro de autoservicio](#) para las aplicaciones, los usuarios externos pueden registrarse en las aplicaciones con las cuentas de los proveedores de identidades que haya agregado.

NOTE

Azure AD está habilitado de forma predeterminada para el registro de autoservicio, por lo que los usuarios siempre tienen la opción de registrarse con una cuenta de Azure AD.

Al canjear la invitación o al registrarse en la aplicación, el usuario externo tiene la opción de iniciar sesión y autenticarse con el proveedor de identidades de redes sociales:



Para conseguir una experiencia de inicio de sesión óptima, fedérese con los proveedores de identidades siempre que sea posible para que pueda proporcionar a sus invitados una experiencia de inicio de sesión sin problemas cuando accedan a las aplicaciones.

Pasos siguientes

Para obtener información sobre cómo agregar proveedores de identidades para iniciar sesión en las aplicaciones, consulte los siguientes artículos:

- [Agregar Google](#) a la lista de proveedores de identidades de redes sociales
- [Agregar Facebook](#) a la lista de proveedores de identidades de redes sociales
- [Configuración de federación directa](#) con cualquier organización cuyo proveedor de identidades (IdP) admita el protocolo SAML 2.0 o WS-Fed. Tenga en cuenta que la federación directa no es una opción para los flujos

de usuario de registro de autoservicio.

Registro de autoservicio (versión preliminar)

18/02/2021 • 5 minutes to read • [Edit Online](#)

NOTE

El registro de autoservicio es la característica en versión preliminar pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

Al compartir una aplicación con usuarios externos, es posible que no siempre sepa de antemano quién necesitará tener acceso a la aplicación. Como alternativa al envío de invitaciones directamente a los usuarios, puede permitir que los usuarios externos se registren en aplicaciones específicas habilitando el registro de autoservicio. Puede crear una experiencia de registro personalizada mediante la personalización del flujo de usuario de registro de autoservicio. Por ejemplo, puede proporcionar opciones de registro con Azure AD o proveedores de identidades sociales y recopilar información sobre el usuario durante el proceso de registro.

NOTE

Puede asociar flujos de usuarios a las aplicaciones que compila la organización. Los flujos de usuario no se pueden usar para las aplicaciones de Microsoft, como SharePoint o Teams.

Flujo de usuario para el registro de autoservicio

Un flujo de usuario de registro de autoservicio crea una experiencia de registro para los usuarios externos a través de la aplicación que quiera compartir. El flujo de usuario puede asociarse a una o varias de sus aplicaciones. En primer lugar, habilitará el registro de autoservicio para el inquilino y se federará con los proveedores de identidades que quiera permitir que usen los usuarios externos para iniciar sesión. A continuación, debe crear y personalizar el flujo de usuario de registro y asignarle sus aplicaciones. Puede configurar las opciones de flujo de usuario para controlar el modo en que el usuario se registra en la aplicación:

- Tipos de cuenta utilizados para iniciar sesión, como cuentas de redes sociales (como Facebook) o cuentas de Azure AD.
- Atributos que se recopilan del registro del usuario, como el nombre, el código postal o el país o región de residencia.

Cuando un usuario quiere iniciar sesión en su aplicación, ya sea una aplicación web, móvil, de escritorio o de una sola página (SPA), la aplicación inicia una solicitud de autorización a un punto de conexión proporcionado por el flujo de usuario. El flujo de usuario define y controla la experiencia del usuario. Cuando el usuario completa el flujo de usuario de registro, Azure AD genera un token y, luego, redirige al usuario de vuelta a la aplicación. Una vez completado el registro, se aprovisiona una cuenta de invitado para el usuario en el directorio. Varias aplicaciones pueden usar el mismo flujo de usuario.

Ejemplo de registro de autoservicio

En el ejemplo siguiente, se muestra cómo vamos a traer proveedores de identidades sociales a Azure AD con funcionalidades de registro de autoservicio para usuarios invitados.

Un asociado de Woodgrove abre la aplicación Woodgrove. Decide que quiere registrarse para obtener una cuenta de proveedor, por lo que selecciona Solicitar cuenta de proveedor, que inicia el flujo de registro de autoservicio.



Partners

Manage your local produce in our inventory so we can deliver your fresh groceries to our customers.

[SIGN IN WITH YOUR SUPPLIER ACCOUNT](#)

[REQUEST YOUR SUPPLIER ACCOUNT](#)

Usa el correo electrónico de su elección para registrarse.

 Microsoft

Create account

Enter the email you'd like to sign up with.

[Back](#) [Next](#)

 Sign in with Google

 Sign in with Facebook

Azure AD crea una relación con Woodgrove mediante la cuenta de Facebook del asociado y crea una cuenta de invitado nueva para el usuario después de que se registre.

Woodgrove quiere obtener más información sobre el usuario, como el nombre, el nombre de la empresa, el código de registro del negocio y el número de teléfono.

Carrier 9:41 AM



Add more details

We need more information to set up your account.

Name

Business name

Business registration code

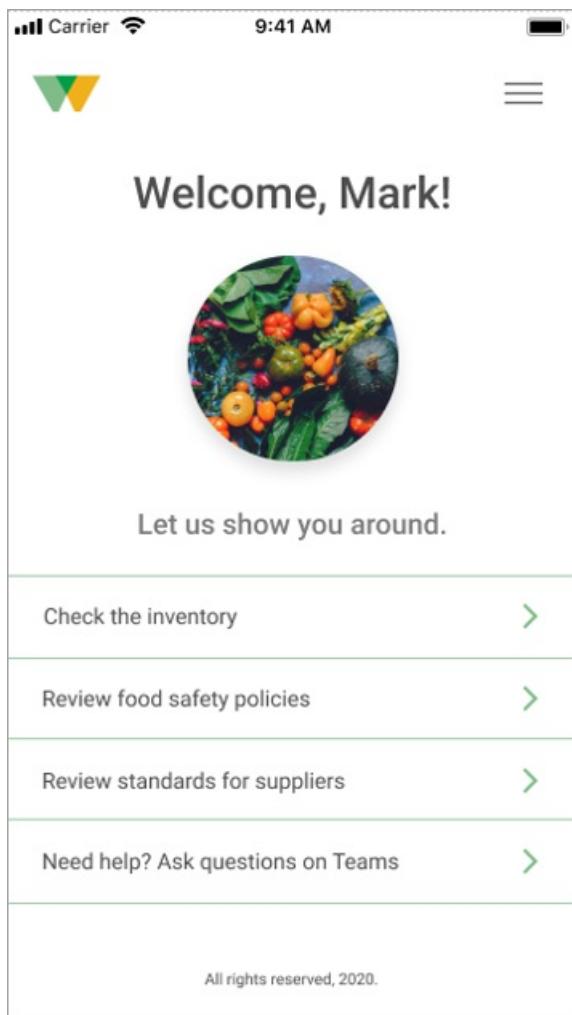
I don't have a code

Phone number

Back

Next

El usuario escribe la información, continúa con el flujo de registro y obtiene acceso a los recursos que necesita.



Pasos siguientes

Para obtener más información, consulte [Incorporación del registro de autoservicio a una aplicación](#).

Uso de conectores de API para personalizar y extender el registro de autoservicio

18/02/2021 • 6 minutes to read • [Edit Online](#)

Información general

Como desarrollador o administrador de TI, puede usar conectores de API para integrar los [flujos de usuario de registro de autoservicio](#) con sistemas externos aprovechando las API web. Por ejemplo, puede usar conectores de API para:

- **Integrarse con un flujo de trabajo de aprobación personalizado.** Conéctese a un sistema de aprobaciones personalizado para administrar la creación de cuentas.
- **Realizar la verificación de identidades.** Use un servicio de verificación de identidad para agregar un nivel de seguridad adicional a las decisiones de creación de cuentas.
- **Validar los datos de entrada del usuario.** Haga una validación de los datos de usuario mal formados o no válidos. Por ejemplo, puede validar los datos proporcionados por el usuario frente a los datos existentes en un almacén de datos externo o una lista de valores permitidos. Si los datos no son válidos, puede pedirle al usuario que proporcione datos válidos o impedir que el usuario continúe con el flujo de registro.
- **Sobrescribir atributos de usuario.** Asigne un valor a un atributo recopilado del usuario o cámbiele el formato. Por ejemplo, si un usuario escribe el nombre con mayúsculas o minúsculas, se le puede dar un formato en el que solo la primera letra esté en mayúscula.
- **Ejecutar una lógica de negocios personalizada.** Puede desencadenar eventos descendentes en los sistemas de la nube para enviar notificaciones push, actualizar las bases de datos corporativas, administrar permisos, auditar bases de datos y realizar otras acciones personalizadas.

Un conector de API proporciona a Azure Active Directory la información necesaria para llamar al punto de conexión de API al definir la dirección URL del punto de conexión HTTP y la autenticación. Una vez que configure un conector de API, puede habilitarlo para un paso específico de un flujo de usuario. Cuando un usuario llega a ese paso del flujo de registro, se invoca el conector de API y se materializa como una solicitud HTTP POST a la API, enviando la información de usuario ("notificaciones") como pares de clave y valor en un cuerpo JSON. La respuesta de la API puede afectar a la ejecución del flujo de usuario. Por ejemplo, la respuesta de la API puede impedir que un usuario se registre, pedir al usuario que vuelva a especificar la información, o sobrescribir y anexar atributos de usuario.

Dónde se puede habilitar un conector de API en un flujo de usuario

El conector de API se puede habilitar en dos lugares del flujo de usuario:

- Despues de iniciar sesión con un proveedor de identidades
- Antes de crear el usuario

IMPORTANT

En ambos casos, los conectores de la API se invocan durante el **registro** del usuario y no en el inicio de sesión.

Después de iniciar sesión con un proveedor de identidades

Inmediatamente después de que el usuario se autentique con un proveedor de identidades (Google, Facebook, Azure AD), se invoca un conector de API en este paso del proceso de registro. Este paso precede a la **página de**

recopilación de atributos, que es el formulario que se muestra al usuario para recopilar los atributos de usuario. A continuación, se muestran ejemplos de escenarios del conector de API que se pueden habilitar en este paso:

- Use el correo electrónico o la identidad federada que el usuario proporcionó para buscar notificaciones en un sistema existente. Devuelva estas notificaciones del sistema existente, rellene previamente la página de recopilación de atributos y haga que estén disponibles para que se devuelvan en el token.
- Compruebe si el usuario está incluido en una lista de permitidos o denegados, y controle si puede continuar con el flujo de registro.

Antes de crear el usuario

Después de la página de recopilación de atributos, se invoca un conector de API en este paso del proceso de registro, si se incluye uno. Este paso siempre se invoca antes de crear una cuenta de usuario en Azure AD. A continuación, se muestran ejemplos de escenarios que se pueden habilitar en este momento del registro:

- Validar datos introducidos por el usuario y pedirle que vuelva a enviarlos.
- Bloquear un registro de usuario en función de los datos especificados por el usuario.
- Realizar la verificación de identidades.
- Consultar en sistemas externos los datos existentes sobre el usuario para devolverlos en el token de aplicación o almacenarlos en Azure AD.

Pasos siguientes

- Obtener información sobre cómo [agregar un conector de API a un flujo de usuario](#)
- Obtener información sobre cómo [agregar un sistema de aprobaciones personalizado al registro de autoservicio](#)

Autoservicio para el registro en la colaboración B2B de Azure AD

18/02/2021 • 2 minutes to read • [Edit Online](#)

Los clientes pueden hacer muchas cosas con las características integradas que se exponen mediante [Azure Portal](#) y el [panel de acceso a las aplicaciones](#) para los usuarios finales. Sin embargo, puede que necesite personalizar el flujo de trabajo de incorporación para los usuarios de B2B para ajustarse a las necesidades de su organización.

Administración de derechos de Azure AD para el registro de usuarios invitados de B2B

Como una organización que invita, puede que no sepa de antemano qué colaboradores externos individuales necesitan acceso a sus recursos. Necesita contar con una forma de que los usuarios de empresas asociadas se registren ellos mismos con unas directivas que usted controle. Si desea permitir que los usuarios de otras organizaciones soliciten acceso y, tras la aprobación, se aprovisionen con cuentas de invitado y se asignen a grupos, aplicaciones y sitios de SharePoint Online, puede usar la [administración de derechos de Azure AD](#) para configurar directivas que [administren el acceso para usuarios externos](#).

API de invitación de Azure Active Directory B2B

Las organizaciones pueden usar la [API del administrador de invitaciones de Microsoft Graph](#) para crear sus propias experiencias de incorporación para los usuarios invitados de B2B. Si desea ofrecer el autoservicio de registro de usuarios invitados de B2B, le recomendamos que use la [administración de derechos de Azure AD](#). Sin embargo, si desea crear su propia experiencia, puede usar la [API de creación de invitaciones](#) para enviar de forma automática el correo electrónico con la invitación personalizada directamente al usuario de B2B, por ejemplo. O bien, la aplicación puede usar el valor de inviteRedeemUrl devuelto en la respuesta de creación para elaborar su propia invitación (a través del mecanismo de comunicación elegido) al usuario invitado.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Precios de identidades externas](#)
- [Preguntas frecuentes sobre la colaboración B2B de Azure Active Directory \(P+F\)](#)

Limitaciones de colaboración B2B de Azure AD

18/02/2021 • 5 minutes to read • [Edit Online](#)

La colaboración B2B de Active Directory (Azure AD) de Azure está sujeta actualmente a las limitaciones descritas en este artículo.

Posibilidad de doble autenticación multifactor

Con B2B de Azure AD, puede aplicar la autenticación multifactor en la organización del recurso (la organización que invita). Los motivos de este enfoque se detallan en [Acceso condicional para usuarios de colaboración B2B](#). Si un asociado ya tiene instalada la autenticación multifactor y la exige, los usuarios del asociado podrían tener que realizar la autenticación una vez en su organización principal y otra vez en la suya.

Activación instantánea

En los flujos de colaboración B2B, hemos agregado usuarios al directorio y los hemos actualizado dinámicamente durante el canje de invitación, la asignación de aplicaciones y así sucesivamente. Las actualizaciones y escrituras se producen normalmente en una instancia de directorio y se deben replicar en todas las instancias. La replicación se completa una vez que se actualicen todas las instancias. En ocasiones, cuando el objeto se escribe o se actualiza en una instancia y la llamada para recuperar este objeto es a otra instancia, pueden producirse latencias en la replicación. Si esto sucede, actualice o vuelva a intentarlo. Si está escribiendo una aplicación mediante la API, los reintentos con algún retroceso es una buena práctica defensiva para mitigar este problema.

Directorios de Azure AD

Azure AD B2B está sujeto a los límites de directorio del servicio Azure AD. Para obtener más información sobre el número de directorios que puede crear un usuario y el número de directorios al que puede pertenecer un usuario o usuario invitado, consulte [Restricciones y límites del servicio Azure AD](#).

Nubes nacionales

Las [nubes nacionales](#) son instancias físicamente aisladas de Azure. La colaboración B2B no se admite más allá de los límites de la nube nacional. Por ejemplo, si el inquilino de Azure está en la nube global pública, no puede invitar a un usuario cuya cuenta está en una nube nacional. Para colaborar con el usuario, pídale otra dirección de correo electrónico o cree una cuenta de usuario miembro para él en el directorio.

Nubes de Azure US Government

Dentro de la nube de Azure US Government, la colaboración B2B solo se admite entre inquilinos que se encuentran dentro de la nube de Azure US Government y que admiten colaboración B2B. Los inquilinos de Azure US Government que admiten la colaboración B2B también pueden colaborar con usuarios sociales mediante cuentas de Microsoft o Google. Si invita a un usuario de fuera de estos grupos (por ejemplo, si el usuario es un inquilino que no forma parte de la nube de Azure US Government o que todavía no admite la colaboración B2B), se produce un error en la invitación o el usuario no puede canjear la invitación. Para obtener más información sobre otras limitaciones, consulte las [variaciones P1 y P2 de Azure Active Directory Premium](#).

¿Cómo puedo saber si la colaboración B2B está disponible en mi inquilino de Azure US Government?

Para averiguar si su inquilino de la nube de Azure US Government admite la colaboración B2B, haga lo siguiente:

1. En un explorador, vaya a la siguiente dirección URL, y sustituya <*tenantname*> por el nombre de su inquilino:

```
https://login.microsoftonline.com/<tenantname>/v2.0/.well-known/openid-configuration
```

2. Busque "tenant_region_scope" en la respuesta JSON:

- Si aparece "tenant_region_scope": "USGOV", se admite B2B.
- Si aparece "tenant_region_scope": "USG", no se admite B2B.

Pasos siguientes

Consulte los siguientes artículos sobre la colaboración de B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Delegación de las invitaciones de colaboración B2B](#)

Habilitación de la colaboración externa B2B y administración de quién puede invitar a otros usuarios

18/02/2021 • 9 minutes to read • [Edit Online](#)

En este artículo se describe cómo habilitar la colaboración B2B de Azure Active Directory (Azure AD), designar quién puede tener invitados y determinar los permisos que tienen los usuarios invitados en Azure AD.

De manera predeterminada, todos los usuarios e invitados del directorio pueden invitar a otros usuarios, incluso si no tienen asignado un rol de administrador. La configuración de colaboración externa le permite activar o desactivar las invitaciones de invitados para los distintos tipos de usuarios de la organización. También puede delegar las invitaciones a usuarios individuales mediante la asignación de roles que les permitan invitar a otros usuarios.

Azure AD le permite restringir qué usuarios invitados externos se pueden ver en el directorio de Azure AD. De forma predeterminada, los usuarios invitados tienen un nivel de permiso limitado que les impide enumerar usuarios, grupos u otros recursos de directorio, pero sí ver la pertenencia de grupos no ocultos. Una nueva opción en versión preliminar le permite restringir aún más el acceso de invitado, de modo que los invitados solo pueden ver su propia información de perfil. Para los detalles, consulte [Restricción de los permisos de acceso de invitado \(versión preliminar\)](#).

Configuración de los valores de colaboración externa B2B

Gracias a la colaboración B2B de Azure AD, el administrador de inquilinos puede establecer las siguientes directivas de invitación:

- Desactivar invitaciones
- Solo los administradores y usuarios del rol Invitador de personas pueden invitar
- Los administradores, el rol Invitador de personas y los miembros pueden invitar
- Todos los usuarios, incluidos los invitados, pueden invitar

De manera predeterminada, todos los usuarios, incluidos los invitados, pueden invitar a usuarios.

Para configurar los valores de colaboración externa B2B:

1. Inicie sesión en [Azure Portal](#) como administrador de inquilinos.
2. Seleccione **Azure Active Directory**.
3. Seleccione **External Identities > Configuración de colaboración externa**.
4. En **Restricciones de acceso de usuarios invitados (versión preliminar)**, elija el nivel de acceso que desea que tengan los usuarios invitados:

Save Discard

Email one-time passcode for guests will be automatically enabled starting March 2021. Learn more. →

Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

Guest users have the same access as members (most inclusive)

Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

- **Guest users have the same access as members (most inclusive)** (Los usuarios invitados tienen el mismo acceso que los miembros [principalmente inclusivo]): esta opción permite a los invitados tener el mismo acceso a los recursos de Azure AD y a los datos del directorio que los usuarios miembros.
- **Guest users have limited access to properties and memberships of directory objects** (Los usuarios invitados tienen acceso limitado a las propiedades y pertenencias de los objetos de directorio): (predeterminada) Esta opción impide que los usuarios realicen determinadas tareas de directorio, como enumerar usuarios, grupos u otros recursos de directorio. Los invitados pueden ver la pertenencia de todos los grupos no ocultos.
- **Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)** (El acceso de los usuarios invitados está restringido a las propiedades y pertenencias de sus propios objetos de directorio [opción más restrictiva]): con esta configuración, los invitados solo pueden tener acceso a sus propios perfiles. No se permite a los invitados ver perfiles, grupos o pertenencias a grupos de otros usuarios.

5. En **Configuración de la invitación de usuarios**, elija la configuración adecuada:

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

- **Los administradores y los usuarios del rol de invitador de usuarios invitados pueden invitar:** Para permitir que los administradores y usuarios del rol "Invitador de usuarios invitados" inviten a otros usuarios, establezca esta directiva en Sí.
- **Los miembros pueden invitar:** Para permitir que los miembros que no son administradores del directorio inviten a otros usuarios, establezca esta directiva en Sí.
- **Los invitados pueden invitar:** Para permitir que los invitados puedan invitar a otros usuarios, establezca esta directiva en Sí.

NOTE

Si Los miembros pueden invitar está establecido en No y Los administradores y los usuarios del rol de invitador de personas pueden invitar está establecido en Sí, los usuarios del rol Invitador de usuarios invitados todavía podrán invitar a usuarios invitados.

6. En **Email one-time passcode for guests** (Código de acceso de un solo uso por correo electrónico para invitados), elija la configuración adecuada. Para más información, consulte [Autenticación con código de acceso de un solo uso por correo electrónico](#):

Email one-time passcode for guests

Email one-time passcode (OTP) supports collaboration and sharing with anyone with an email account, without them having to create a new account. Each time they sign-in to your directory, they receive an OTP via email to authenticate. [Learn more](#)

- Automatically enable email one-time passcode for guests starting March 2021.
- Enable email one-time passcode for guests effective now.
- Disable email one-time passcode for guests.

- **Automatically enable email one-time passcode for guests in March 2021** (Habilitar automáticamente el código de acceso de un solo uso por correo electrónico a partir de marzo de 2021). Valor predeterminado. Si la característica de código de acceso de un solo uso por correo electrónico no está habilitada para el inquilino, se activará automáticamente en marzo de 2021. Si desea que la característica se habilite desde ese momento, no tiene que hacer nada más. Si ya ha habilitado o deshabilitado la característica, esta opción no estará disponible.
- **Enable email one-time passcode for guests effective now** (Habilitar el código de acceso de un solo uso por correo electrónico para invitados desde este momento). Activa la característica de código de acceso de un solo uso por correo electrónico para el inquilino.
- **Disable email one-time passcode for guests** (Deshabilitar el código de acceso de un solo uso por correo electrónico para invitados). Desactiva la característica de código de acceso de un solo uso por correo electrónico para el inquilino y evita que la característica se active en marzo de 2021.

NOTE

En lugar de las opciones anteriores, verá el siguiente botón si ha habilitado o deshabilitado esta característica, o bien si ha participado previamente en la versión preliminar:

Email one-time passcode for guests ⓘ

[Learn more](#)

Yes

No

7. En **Enable guest self-service sign up via user flows (Preview)** (Habilitación del registro de invitados de autoservicio mediante flujos de usuario [versión preliminar]), seleccione **Yes** (Sí) si desea crear flujos de usuario que permitan a los usuarios suscribirse a aplicaciones. para más información sobre esta opción, consulte [Incorporación de un flujo de usuario de registro de autoservicio a una aplicación \(versión preliminar\)](#).

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

Yes

No

8. En **Restricciones de colaboración**, elija si desea permitir o denegar las invitaciones a los dominios que especifique. Para obtener más información, consulte [Allow or block invitations to B2B users from specific organizations](#) (Permitir o bloquear invitaciones a usuarios de B2B procedentes de determinadas organizaciones).

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)

Asignación del rol de invitador de usuarios invitados a un usuario

Con el rol de invitador de usuarios invitados, puede conceder a usuarios individuales la capacidad de invitar a otros usuarios sin asignarles un rol de administrador global u otro rol de administrador. Asigne el rol de invitador de usuarios invitados a diferentes individuos. A continuación, asegúrese de establecer la opción **Los administradores y los usuarios del rol de invitador de usuarios invitados pueden invitar** en Sí.

Este es un ejemplo que muestra cómo usar PowerShell para agregar un usuario al rol Invitador de personas:

```
Add-MsolRoleMember -RoleObjectId 95e79109-95c0-4d8e-aee3-d01accf2d47b -RoleMemberEmailAddress  
<RoleMemberEmailAddress>
```

Pasos siguientes

Consulte los siguientes artículos sobre la colaboración B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Incorporación de usuarios de colaboración B2B sin invitación](#)
- [Incorporación de usuarios de colaboración B2B a un rol](#)

Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal

18/02/2021 • 10 minutes to read • [Edit Online](#)

Como usuario al que se le asignan cualquiera de los roles limitados de directorio de administradores, puede usar Azure Portal para invitar a los usuarios de colaboración B2B. Puede invitar a usuarios invitados al directorio, a un grupo o a una aplicación. Después de invitar a un usuario mediante cualquiera de estos métodos, la cuenta del usuario invitado se agrega a Azure Active Directory (Azure AD), con *invitado* como tipo de usuario. El usuario invitado deberá canjear después su invitación para acceder a los recursos. Una invitación de un usuario no expira.

Después de agregar un usuario invitado al directorio, puede enviarle un vínculo directo a una aplicación compartida o bien, el propio usuario invitado puede hacer clic en la dirección URL de canje del correo electrónico de invitación. Para más información sobre el proceso de canje, consulte [Canje de invitación de colaboración B2B](#).

IMPORTANT

Debe seguir los pasos descritos en [Procedimiento: Agregar información de privacidad con Azure Active Directory](#) para agregar la dirección URL de la declaración de privacidad de su organización. Como parte del proceso de canje de invitación por primera vez, el usuario invitado debe indicar su consentimiento con los términos de privacidad para poder continuar.

Antes de empezar

Asegúrese de que la configuración de colaboración externa de la organización se configure de forma que le permita invitar a otros usuarios. De manera predeterminada, todos los usuarios y administradores pueden invitar a otros usuarios. Sin embargo, las directivas de colaboración externa de la organización pueden estar configuradas para impedir que determinados tipos de usuarios o administradores inviten a otros usuarios. Para obtener información sobre cómo ver y establecer estas directivas, consulte [Enable B2B external collaboration and manage who can invite guests](#) (Habilitación de la colaboración externa B2B y administración de quién puede invitar a otros usuarios).

Adición de usuarios invitados al directorio

Para agregar usuarios de colaboración B2B al directorio, siga estos pasos:

1. Inicie sesión en [Azure Portal](#) como usuario que tiene asignado un rol de directorio administrador limitado o el rol de invitador de usuarios invitados.
2. Busque y seleccione **Azure Active Directory** en cualquier página.
3. En **Administrador**, seleccione **Usuarios**.
4. Seleccione **Nuevo usuario invitado**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Azure logo, a search bar, and a user account section. Below the navigation is a blue header bar with the text 'Microsoft Azure', the current location 'Home > Contoso > Users - All users', and a 'Documentation' link. The main content area has a left sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity', 'Sign-ins', and 'Audit logs'. The main panel displays a table of users with columns: Name, User name, User type, and Source. The 'User type' column shows 'Member' for most users and 'Guest' for Tami Weiss. At the top of the main panel, there are buttons for '+ New user' and '+ New guest user', with '+ New guest user' being the one highlighted by a red box.

- En la página **Nuevo usuario**, seleccione **Invitar usuario** y, después, agregue la información del usuario invitado.

NOTE

No se admiten direcciones de correo electrónico de grupos; escriba la dirección de un usuario individual. Además, algunos proveedores de correo electrónico permiten a los usuarios agregar un signo más (+) y texto adicional a sus direcciones de correo electrónico, ya que ello sirve de ayuda a algunas funciones como el filtrado de la bandeja de entrada. Sin embargo, Azure AD no admite actualmente estos símbolos más (+) en las direcciones de correo electrónico. Para evitar problemas de entrega, omita el signo más y los caracteres siguientes hasta el símbolo @.

- Nombre.** Nombre y apellidos del nuevo usuario.
- Dirección de correo (obligatorio).** La dirección de correo del usuario invitado.
- Mensaje personal (opcional)** Incluye un mensaje de bienvenida personal al usuario invitado.
- Grupos** : Puede agregar al usuario invitado a uno o varios de los grupos existentes, o puede hacerlo después.
- Rol del directorio.** Si necesita permisos administrativos de Azure AD para el usuario, puede agregarlos a un rol de Azure AD.

- Seleccione **Invitar** para enviar automáticamente la invitación al usuario invitado.

Después de enviar la invitación, la cuenta de usuario se agrega automáticamente al directorio como invitado.

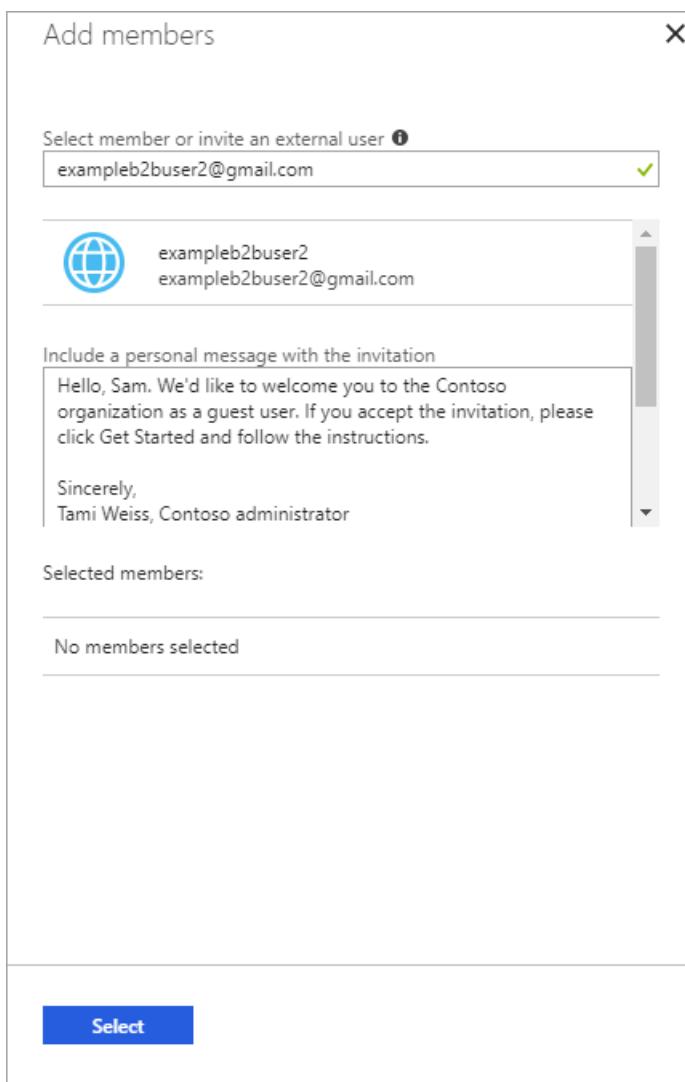
The screenshot shows the Microsoft Azure portal interface, similar to the previous one but for the 'contoso' tenant. The 'New guest user' button is not highlighted. The main panel displays a table of users with columns: NAME, USER NAME, USER TYPE, and SOURCE. The 'USER TYPE' column shows 'Member' for most users and 'Guest' for the user 'exampleb2buser', which is highlighted with a red box.

Adición de usuarios invitados a un grupo

Si necesita agregar manualmente usuarios de colaboración B2B a un grupo, siga estos pasos:

- Inicie sesión en [Azure Portal](#) como administrador de Azure AD.

2. Busque y seleccione Azure Active Directory en cualquier página.
3. En Administrar , seleccione Grupos.
4. Seleccione un grupo (o haga clic en Nuevo grupo para crear uno). Es una buena idea incluir en la descripción del grupo que el grupo contiene los usuarios invitados B2B.
5. Seleccione Miembros.
6. Realice una de las siguientes acciones:
 - Si el usuario invitado ya existe en el directorio, busque el usuario B2B. Seleccione el usuario y haga clic en Seleccionar para agregar el usuario al grupo.
 - Si el usuario invitado no existe ya en el directorio, invítelo al grupo; para ello, escriba su dirección de correo electrónico en el cuadro de búsqueda, escriba un mensaje personal opcional y, a continuación, haga clic en Seleccionar. La invitación se dirige automáticamente al usuario invitado.



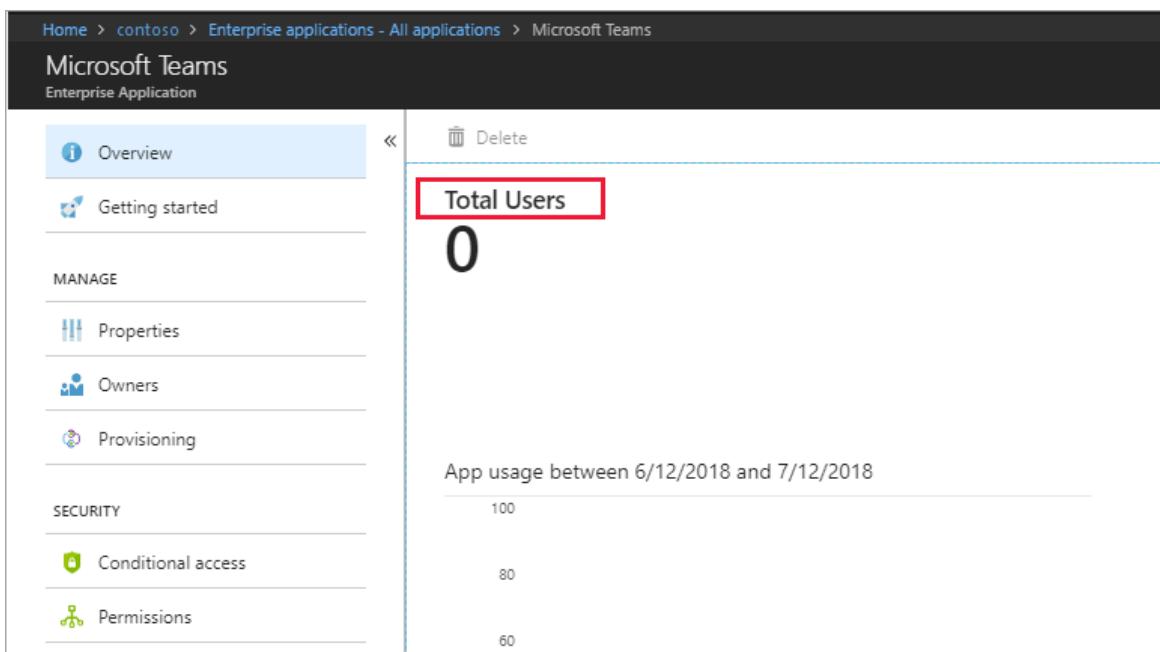
También puede utilizar grupos dinámicos con colaboración B2B de Azure AD. Para más información, consulte [Grupos dinámicos y colaboración B2B de Azure Active Directory](#).

Adición de usuarios invitados a una aplicación

Para agregar usuarios de colaboración B2B a una aplicación, siga estos pasos:

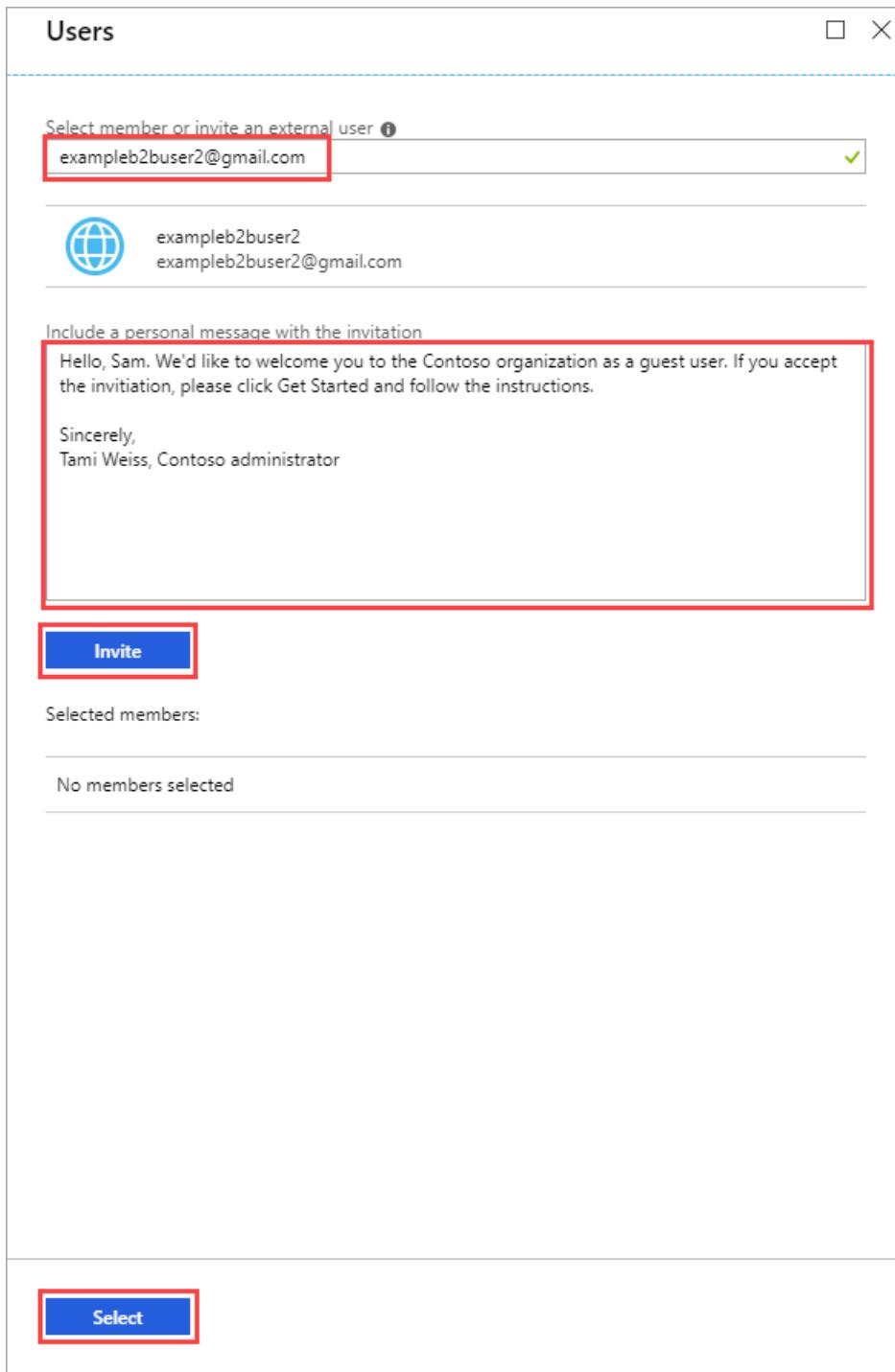
1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. Busque y seleccione Azure Active Directory en cualquier página.
3. En Administrar , seleccione Aplicaciones empresariales > Todas las aplicaciones.

4. Seleccione la aplicación a la que desea agregar usuarios invitados.
5. En el panel de la aplicación, seleccione **Usuarios totales** para abrir el panel **Usuarios y grupos**.



The screenshot shows the Microsoft Teams Enterprise Application Overview page. The top navigation bar includes 'Home > contoso > Enterprise applications - All applications > Microsoft Teams'. The main content area has a sidebar with 'Overview' selected. The right pane displays 'Total Users' with a value of '0'. Below this, there is a chart titled 'App usage between 6/12/2018 and 7/12/2018' showing usage levels at 100, 80, and 60. The 'Overview' tab is highlighted with a blue background and white text. The 'Total Users' section is also highlighted with a red border around the '0' value.

6. Seleccione **Agregar usuario**.
7. En **Agregar asignación**, seleccione **Usuarios y grupos**.
8. Realice una de las siguientes acciones:
 - Si el usuario invitado ya existe en el directorio, busque el usuario B2B. Seleccione el usuario, haga clic en **Seleccionar** y luego haga clic en **Asignar** para agregar el usuario a la aplicación.
 - Si el usuario invitado no existe en el directorio, en **Seleccione un miembro o invite a un usuario externo**, escriba la dirección de correo electrónico del usuario. En el cuadro de mensaje, escriba un mensaje personal opcional. Debajo del cuadro de mensaje, haga clic en **Invitar**.



Haga clic en **Seleccionar** y luego haga clic en **Asignar** para agregar al usuario a la aplicación.
Una invitación se dirige automáticamente al usuario invitado.

9. El usuario invitado aparece en la lista **Usuarios y grupos** de la aplicación con el rol asignado de **Acceso predeterminado**. Si quiere cambiar el rol, haga lo siguiente:

- Seleccione el usuario invitado y, a continuación, seleccione **Editar**.
- En **Editar asignación**, haga clic en **Seleccionar rol** y seleccione el rol que quiere asignar al usuario seleccionado.
- Haga clic en **Seleccionar**.
- Haga clic en **Asignar**.

Reenvío de invitaciones a usuarios invitados

Si un usuario invitado todavía no ha canjeado su invitación, puede volver a enviarle el correo electrónico de invitación.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. Busque y seleccione **Azure Active Directory** en cualquier página.
3. En **Administrar**, seleccione **Usuarios**.
4. Seleccione la cuenta del usuario.
5. En **Administrar**, seleccione **Perfil**.
6. Si el usuario todavía no ha aceptado la invitación, la opción **Volver a enviar la invitación** está disponible. Seleccione este botón para volver a enviarla.

The screenshot shows the Azure portal interface for managing users. The URL in the address bar is `Home > contoso > Users - All users > exampleb2buser - Profile`. The main content area is titled "exampleb2buser - Profile". On the left, there's a sidebar with sections for "MANAGE" (Profile, Directory role, Groups, Applications, Licenses, Devices, Azure resources) and "ACTIVITY" (Sign-ins, Audit logs). Under "TROUBLESHOOTING + SUPPORT", there are links for Troubleshoot and New support request. The "Profile" tab is currently selected. The main right panel displays the user's identity details: Name (exampleb2buser), User name (exampleb2buser@gmail.com), First name, and Last name. It also shows a placeholder photo with a globe icon. Below these fields are Object ID (14b5a731-979f-4f60-8939-540d8fadd7dd), User type (Guest), and Source (Invited user). At the bottom of the form, there is a blue "Resend invitation" button, which is highlighted with a red box.

NOTE

Si vuelve a enviar una invitación que originalmente dirigía al usuario a una aplicación específica, debe entender que el vínculo de la nueva invitación lleva por el contrario al usuario al panel de acceso de nivel superior.

Pasos siguientes

- Para aprender cómo los administradores que no son de Azure AD pueden agregar usuarios invitados B2B, consulte [¿Cómo agregan los trabajadores de la información usuarios de colaboración B2B a Azure Active Directory?](#)
- Para más información sobre el correo electrónico de invitación, consulte [Los elementos del correo electrónico de invitación de colaboración B2B](#).

¿Cómo pueden los usuarios de la organización invitar a usuarios invitados a una aplicación?

18/02/2021 • 10 minutes to read • [Edit Online](#)

Una vez que se haya agregado un usuario invitado al directorio en Azure AD, un propietario de aplicación puede enviar a este un vínculo directo a la aplicación que desea compartir. Los administradores de Azure AD también pueden configurar la administración autoservicio para la galería o las aplicaciones basadas en SAML en su inquilino de Azure AD. De esta forma, los propietarios de aplicaciones puedan administrar sus propios usuarios invitados, incluso aunque los usuarios invitados no se hayan agregado al directorio aún. Si una aplicación está configurada para el autoservicio, el propietario de la aplicación usa su panel de acceso para invitar a un usuario invitado a una aplicación o para agregar un usuario invitado a un grupo que tiene acceso a la aplicación. La administración autoservicio de una galería o aplicación basada en SAML requiere algo de configuración inicial por parte de un administrador. El siguiente es un resumen de los pasos de configuración (para obtener instrucciones detalladas, consulte [Requisitos previos](#) más adelante en esta página):

- Habilite la administración de grupos de autoservicio para el inquilino
- Cree un grupo para asignar a la aplicación y hacer que el usuario sea un propietario
- Configure la aplicación para el autoservicio y asigne el grupo a la aplicación

NOTE

- En este artículo se describe cómo configurar la administración autoservicio para la galería y las aplicaciones basadas en SAML que ha agregado al inquilino de Azure AD. También puede [configurar grupos de autoservicio de Microsoft 365](#) para que los usuarios puedan administrar el acceso a sus propios grupos de Microsoft 365. Para conocer más formas en las que los usuarios pueden compartir sus archivos y aplicaciones, consulte [Agregar invitados a grupos de Microsoft 365 y Uso compartido de archivos o carpetas de SharePoint](#).
- Los usuarios solo pueden realizar invitaciones si tienen el rol **Invitador de usuarios invitados**.

Invitación a un usuario invitado a una aplicación desde el panel de acceso

Después de configurar una aplicación para el autoservicio, los propietarios de la aplicación pueden usar su propio panel de acceso para invitar a un usuario invitado a la aplicación que desean compartir. No es necesario que se agregue el usuario invitado a Azure AD con antelación.

1. Para abrir el panel de acceso, vaya a <https://myapps.microsoft.com>.
2. Apunte a la aplicación, seleccione el ícono de puntos suspensivos (...) y, a continuación, seleccione **Administrar aplicación**.

The screenshot shows the Microsoft Azure Active Directory Access Panel. In the center, there's a grid of application icons. The 'Salesforce' icon is highlighted with a blue box, and a context menu is open over it. The menu has two items: 'Open' and 'Manage app'. The 'Manage app' item is specifically highlighted with a red box.

3. En la parte superior de la lista de usuarios, seleccione + .

This screenshot shows the 'Manage app' interface for the Salesforce application. At the top, there's a back arrow labeled '← Apps' and the app name 'Salesforce'. Below that, there's a thumbnail of the Salesforce logo and its name. Underneath, the URL 'http://www.salesforce.com/' is listed. To the right, there's a table header with columns 'USERS', 'ROLE', and 'ID'. A red box highlights the '+' button in the top right corner of this table area. Below the table, a message says 'No users have been added.'

4. En el cuadro de búsqueda **Agregar miembros**, escriba la dirección de correo electrónico para el usuario invitado. Opcionalmente, puede incluir un mensaje de bienvenida.

This screenshot shows the 'Add members' dialog box. At the top, it says 'Add members'. Below that is an input field containing the email 'sanda@gmail.com'. To the right, there are two buttons: 'sanda@gmail.com' and 'External user'. Below these, there's a message box containing a welcome message: 'Hello Sandra, Welcome to the Salesforce app for Contoso. Sincerely, Sam'. At the bottom, there are two buttons: a blue 'Add' button and a grey 'Cancel' button. A red box highlights the 'Add' button.

5. Seleccione **Agregar** para enviar una invitación al usuario invitado. Después de enviar la invitación, la cuenta de usuario se agrega automáticamente al directorio como invitado.

Invitar a alguien a unirse a un grupo que tiene acceso a la aplicación

Después de configurar una aplicación para el autoservicio, los propietarios de la aplicación pueden invitar a los

usuarios a los grupos que ellos administran y que tienen acceso a las aplicaciones que desean compartir. No es necesario que los usuarios invitados ya existan en el directorio. El propietario de la aplicación debe seguir estos pasos para invitar a un usuario invitado al grupo para que pueda acceder a la aplicación.

1. Asegúrese de que es propietario del grupo de autoservicio que tiene acceso a la aplicación que desea compartir.
2. Para abrir el panel de acceso, vaya a <https://myapps.microsoft.com>.
3. Seleccione la aplicación **Grupos**.

The screenshot shows the Microsoft My Apps portal interface. At the top, there is a header with the company logo 'contoso' and a user profile for 'Sam CONTOSO'. Below the header, there is a search bar labeled 'Search apps'. Under the heading 'Apps', there is a list of applications: 'Salesforce' (with a cloud icon), 'Security & Compli...' (with a blue square icon), 'Store' (with an orange shopping bag icon), 'Azure portal' (with a blue cloud icon), and 'Groups' (with a purple icon showing two people). The 'Groups' application is highlighted with a red rectangular box around its icon and name.

4. En **Grupos de mi propiedad**, seleccione el grupo que tiene acceso a la aplicación que desea compartir.

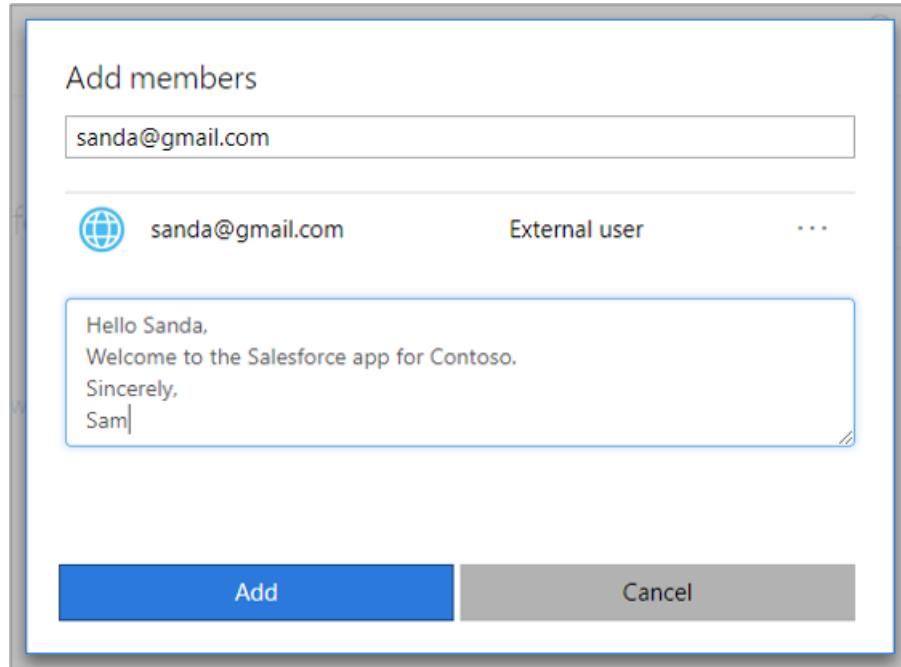
The screenshot shows the 'Groups' page. On the left, under 'Groups I own', there is a '+ Create group' button. Below it are three groups: 'DP Design Partners' (green icon), 'SA Self-Service App Access' (yellow-green icon), and 'SG Self-service group for Office ...' (blue icon). The 'SA' group is highlighted with a red rectangular box. On the right, under 'Groups I'm in', there is a '+ Join group' button and a single group 'DP Design Partners' (green icon).

5. En la parte superior de la lista de miembros de grupos, seleccione + .

The screenshot shows the details page for the 'Self-Service App Access' group. At the top, there is a back arrow and the group name 'Self-Service App Access'. Below the name, there is a table with columns 'MEMBERS', 'ROLE', and 'ID'. A red box highlights the '+' button in the top right corner of this table. On the left, there is information about the group: 'Group type: Security', 'Members: 0', and 'Join policy: This group is open to join for all users'. At the bottom, there are buttons for 'Join group', 'Edit details', and 'Delete group'.

6. En el cuadro de búsqueda **Agregar miembros**, escriba la dirección de correo electrónico para el usuario

invitado. Opcionalmente, puede incluir un mensaje de bienvenida.



7. Seleccione **Agregar** para enviar automáticamente la invitación al usuario invitado. Después de enviar la invitación, la cuenta de usuario se agrega automáticamente al directorio como invitado.

Requisitos previos

La administración de autoservicio de aplicaciones requiere algo de configuración inicial por parte de un administrador global y un administrador de Azure AD. Como parte de esta configuración, deberá configurar la aplicación para el autoservicio y asignar un grupo a la aplicación que pueda administrar el propietario de la misma. También puede configurar el grupo para permitir que cualquier persona solicite la pertenencia, pero requiere la aprobación del propietario del grupo. (Más información acerca de la [administración de grupos de autoservicio](#)).

NOTE

No puede agregar usuarios invitados a un grupo dinámico o a uno que se ha sincronizado con la instancia local de Active Directory.

Habilite la administración de grupos de autoservicio para el inquilino

1. Inicie sesión en [Azure Portal](#) como administrador global.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. Seleccione **Grupos**.
4. En **Configuración**, seleccione **General**.
5. En **Administración de grupos de autoservicio**, junto a **Los propietarios pueden administrar solicitudes de pertenencia a grupos en el Panel de acceso**, seleccione **Sí**.
6. Seleccione **Guardar**.

Cree un grupo para asignar a la aplicación y hacer que el usuario sea un propietario

1. Inicie sesión en [Azure Portal](#) como administrador global o administrador de Azure AD.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. Seleccione **Grupos**.
4. Seleccione **Nuevo grupo**.
5. En **Tipo de grupo**, seleccione **Seguridad**.

6. Escriba un **Nombre de grupo** y una **Descripción del grupo**.
7. En **Tipo de pertenencia**, seleccione **Asignado**.
8. Seleccione **Crear** y cierre la página **Grupo**.
9. En la página **Grupos - Todos los grupos**, abra el grupo.
10. En **Administrar**, seleccione **Propietarios > Agregar propietarios**. Busque el usuario que debe administrar el acceso a la aplicación. Seleccione el usuario y luego haga clic en **Seleccionar**.

Configure la aplicación para el autoservicio y asigne el grupo a la aplicación

1. Inicie sesión en [Azure Portal](#) como administrador global o administrador de Azure AD.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Aplicaciones empresariales > Todas las aplicaciones**.
4. En la lista de aplicaciones, busque y abra la aplicación.
5. En **Administrar**, seleccione **Inicio de sesión único** y configure la aplicación para el inicio de sesión único. (Para más información, consulte [Administración del inicio de sesión único para aplicaciones empresariales](#)).
6. En **Administrar**, seleccione **Autoservicio** y configure el acceso a la aplicación de autoservicio. (Para más información, consulte [Uso del acceso de autoservicio a las aplicaciones](#)).

NOTE

En la opción **¿A qué grupo se deberían agregar los usuarios asignados?** seleccione el grupo que creó en la sección anterior.

7. En **Administrar**, seleccione **Usuarios y grupos** y compruebe que el grupo de autoservicio que creó aparece en la lista.
8. Para agregar la aplicación al panel de acceso del propietario del grupo, seleccione **Agregar usuario > Usuarios y grupos**. Busque al propietario del grupo y seleccione el usuario, haga clic en **Seleccionar** y luego haga clic en **Asignar** para agregar el usuario a la aplicación.

Pasos siguientes

Consulte los siguientes artículos sobre la colaboración de B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [¿Cómo agregan los administradores de Azure Active Directory usuarios de colaboración B2B?](#)
- [Canje de invitación de colaboración B2B](#)
- [Precios de identidades externas](#)

Invitar a usuarios internos a la colaboración B2B

18/02/2021 • 8 minutes to read • [Edit Online](#)

Antes de la disponibilidad de la colaboración B2B de Azure AD, las organizaciones pueden colaborar con distribuidores, proveedores y otros usuarios invitados mediante la configuración de credenciales internas para ellos. Si tiene usuarios de invitado internos como estos, puede invitarlos a usar la colaboración B2B en su lugar. Estos usuarios invitados de B2B podrán usar sus propias identidades y credenciales para iniciar sesión, y no tendrá que mantener contraseñas ni administrar los ciclos de vida de las cuentas.

El envío de una invitación a una cuenta interna existente le permite conservar el identificador de objeto, el UPN, la pertenencia a grupos y las asignaciones de aplicaciones de ese usuario. No es necesario eliminar y volver a invitar al usuario manualmente ni reasignar los recursos. Para invitar al usuario, use la API de invitación para pasar el objeto de usuario interno y la dirección de correo electrónico del usuario invitado junto con la invitación. Cuando el usuario acepta la invitación, el servicio B2B cambia el objeto de usuario interno existente a un usuario de B2B. A partir de ahí, el usuario debe iniciar sesión en los servicios de recursos de nube con sus credenciales de B2B.

Aspectos que se deben tener en cuenta:

- **Acceso a recursos locales:** Una vez que se ha invitado al usuario a la colaboración B2B, todavía puede usar sus credenciales internas para acceder a los recursos locales. Para evitarlo, puede restablecer o cambiar la contraseña en la cuenta interna. La excepción es [Autenticación con código de acceso de un solo uso por correo electrónico](#). Si el método de autenticación del usuario se cambia a código de acceso de un solo uso, ya no podrá usar sus credenciales internas.
- **Facturación:** Esta característica no cambia el UserType del usuario, por lo que no cambia automáticamente el modelo de facturación del usuario a los [precios de usuarios activos mensuales \(MAU\) de External Identities](#). Para activar los precios de MAU para el usuario, cambie UserType para el usuario a `guest`. Además tenga en cuenta que el inquilino de Azure AD debe estar [vinculado a una suscripción de Azure](#) para activar la facturación de MAU.
- **La invitación es unidireccional:** Puede invitar a usuarios internos a usar la colaboración B2B, pero no puede quitar las credenciales de B2B una vez agregadas. Para volver a cambiar el usuario a un usuario solo interno, deberá eliminar el objeto de usuario y crear otro.
- **Teams:** Cuando el usuario accede a Teams con sus credenciales externas, su inquilino no estará disponible inicialmente en el selector de inquilinos de Teams. El usuario puede acceder a Teams mediante una dirección URL que contiene el contexto del inquilino, por ejemplo:
`https://team.microsoft.com/?tenantId=<TenantId>`. Después de esto, el inquilino estará disponible en el selector de inquilinos de Teams.
- **Usuarios sincronizados locales:** para las cuentas de usuario sincronizadas entre el entorno local y la nube, el directorio local sigue siendo el origen de autoridad después de haber invitado a los usuarios a usar la colaboración B2B. Los cambios que realice en la cuenta local se sincronizarán con la cuenta en la nube, incluida la deshabilitación o eliminación de la cuenta. Por lo tanto, solo mediante la eliminación de la cuenta local, no puede evitar que el usuario inicie sesión en su cuenta local mientras conserva su cuenta en la nube. En su lugar, puede establecer la contraseña de la cuenta local en un GUID aleatorio u otro valor desconocido.

Invitación de usuarios internos a la colaboración B2B

Puede usar PowerShell o la API de invitación para enviar una invitación a B2B al usuario interno. Asegúrese de que la dirección de correo electrónico que desea usar para la invitación está establecida como la dirección de correo electrónico externa en el objeto de usuario interno.

- Debe usar la dirección de correo electrónico de la propiedad User.Mail en la invitación.
- El dominio de la propiedad Mail del usuario debe coincidir con la cuenta que usan para iniciar sesión. De lo contrario, algunos servicios, como Teams, no podrán autenticar al usuario.

De forma predeterminada, se enviará un correo electrónico al usuario para notificarle que se le ha invitado, pero puede suprimir el mensaje y escribir uno personalizado.

NOTE

Para enviar su propio correo electrónico u otra comunicación, puede usar `New-AzureADMSInvitation` con `-SendInvitationMessage:$false` para invitar a los usuarios de forma silenciosa y, a continuación, enviar su propio mensaje de correo electrónico al usuario convertido. Vea [Personalización y API de colaboración B2B de Active Directory Azure](#).

Uso de PowerShell para enviar una invitación a B2B

Necesitará el módulo Azure AD PowerShell, versión 2.0.2.130 o posterior. Use el siguiente comando para actualizar al módulo de AzureAD PowerShell más reciente e invitar al usuario interno a la colaboración B2B:

```
Uninstall-Module AzureAD
Install-Module AzureAD
$ADGraphUser = Get-AzureADUser -objectID "UPN of Internal User"
$msgGraphUser = New-Object Microsoft.Open.MSGraph.Model.User -ArgumentList $ADGraphUser.ObjectId
New-AzureADMSInvitation -InvitedUserEmailAddress <>external email<> -SendInvitationMessage $True -
InviteRedirectUrl "http://myapps.microsoft.com" -InvitedUser $msgGraphUser
```

Uso de la API de invitación para enviar una invitación a B2B

En el ejemplo siguiente se muestra cómo llamar a la API de invitación para invitar a un usuario interno como un usuario de B2B.

```
POST https://graph.microsoft.com/v1.0/invitations
Authorization: Bearer eyJ0eX...
ContentType: application/json
{
    "invitedUserEmailAddress": "<>external email><>",
    "sendInvitationMessage": true,
    "invitedUserMessageInfo": {
        "messageLanguage": "en-US",
        "ccRecipients": [
            {
                "emailAddress": {
                    "name": null,
                    "address": "<>optional additional notification email><>"
                }
            }
        ],
        "customizedMessageBody": "<>custom message><>"
    },
    "inviteRedirectUrl": "https://myapps.microsoft.com?tenantId=",
    "invitedUser": {
        "id": "<>ID for the user you want to convert><>"
    }
}
```

La respuesta a la API es la misma respuesta que se obtiene al invitar a un nuevo usuario invitado al directorio.

Pasos siguientes

- [Canje de invitación de colaboración B2B](#)

Permitir o bloquear invitaciones a usuarios B2B procedentes de determinadas organizaciones

18/02/2021 • 11 minutes to read • [Edit Online](#)

Puede usar una lista de permitidos o de denegación para permitir o bloquear las invitaciones a usuarios B2B procedentes de determinadas organizaciones. Por ejemplo, si quiere bloquear dominios de direcciones de correo electrónico personales, puede configurar una lista de denegación que contenga dominios como Gmail.com y Outlook.com. O bien, si su empresa tiene una asociación con otras empresas como Contoso.com, Fabrikam.com y Litware.com, y quiere restringir las invitaciones a solo estas organizaciones, puede agregar Contoso.com, Fabrikam.com y Litware.com a la lista de permitidos.

Consideraciones importantes

- Puede crear una lista de permitidos o una lista de denegación. No se pueden configurar ambos tipos de listas. De forma predeterminada, los dominios que no están en la lista de permitidos están en la de denegación y viceversa.
- Solo puede crear una directiva por organización. Puede actualizar la directiva para incluir más dominios, o puede eliminar la directiva para crear una nueva.
- El número de dominios que puede agregar a una lista de permitidos o de denegación solo se ve limitado por el tamaño de la directiva. Este límite se aplica al número de caracteres, por lo que puede tener dominios más cortos o menos dominios más largos. El tamaño máximo de toda la directiva es de 25 KB (25 000 caracteres), que incluye la lista de permitidos o la lista de denegación y cualquier otro parámetro configurado para otras características.
- Esta lista funciona con independencia de las listas de permitidos o bloqueados de OneDrive para la Empresa y SharePoint Online. Si quiere restringir el uso compartido individual de archivos en SharePoint Online, debe configurar una lista de permitidos o bloqueados para OneDrive para la Empresa y SharePoint Online. Para más información, consulte [Uso compartido de dominios restringidos en SharePoint Online y OneDrive para la Empresa](#).
- Esta lista no se aplica a usuarios externos que ya han canjeado la invitación. La lista se aplicará después de configurarla. Si una invitación de usuario está en estado pendiente y se define una directiva que bloquea su dominio, el intento del usuario para canjear la invitación producirá error.

Definición de la directiva de lista de permitidos o de denegación en el portal

De forma predeterminada, la opción **Allow invitations to be sent to any domain (most inclusive)** (Permitir que se envíen invitaciones a cualquier dominio [más inclusivo]) está habilitada. En este caso, puede invitar a usuarios B2B de cualquier organización.

Adición de una lista de denegación

Este es el escenario más típico, donde su organización quiere trabajar con casi cualquier organización, pero desea impedir que los usuarios de dominios específicos sean invitados como usuarios B2B.

Para agregar una lista de denegación:

1. Inicie sesión en [Azure Portal](#).
2. Seleccione **Azure Active Directory > Usuarios > Configuración de usuario**.

3. En **Usuarios externos**, seleccione **Administrar la configuración de colaboración externa**.
4. En **Restricciones de colaboración**, seleccione **Deny invitations to the specified domains** (Denegar invitaciones a los dominios especificados).
5. En **DOMINIOS DE DESTINO**, escriba el nombre de uno de los dominios que quiere bloquear. Si hay varios dominios, especifique cada dominio en una nueva línea. Por ejemplo:

The screenshot shows the 'Collaboration restrictions' configuration page. At the top, there are three radio button options: 'Allow invitations to be sent to any domain (most inclusive)', 'Deny invitations to the specified domains' (which is selected), and 'Allow invitations only to the specified domains (most restrictive)'. Below this is a 'Delete' button with a trash icon. A section titled 'TARGET DOMAINS' contains three input fields, each with a checkbox: 'gmail.com', 'yahoo.com', and 'example.com or *.example.com or example.*'. The 'example.*' entry is highlighted with a red border.

6. Cuando haya terminado, haga clic en **Guardar**.

Después de establecer la directiva, si intenta invitar a un usuario de un dominio bloqueado, recibirá un mensaje que indica que la directiva actual de invitación bloquea el dominio del usuario.

Adición de una lista de permitidos

Esta es una configuración más restrictiva, donde puede establecer dominios específicos en la lista de permitidos y restringir las invitaciones a las otras organizaciones o dominios que no se mencionan.

Si desea usar una lista de permitidos, asegúrese de dedicar tiempo a evaluar exhaustivamente las necesidades de su empresa. Si hace esta directiva demasiado restrictiva, los usuarios pueden elegir enviar documentos por correo electrónico o buscar otras formas de colaboración no sancionadas por TI.

Para agregar una lista de permitidos:

1. Inicie sesión en [Azure Portal](#).
2. Seleccione **Azure Active Directory > Usuarios > Configuración de usuario**.
3. En **Usuarios externos**, seleccione **Administrar la configuración de colaboración externa**.
4. En **Restricciones de colaboración**, seleccione **Allow invitations only to the specified domains (most restrictive)** (Permitir invitaciones solo a los dominios especificados [más restrictivo]).
5. En **DOMINIOS DE DESTINO**, escriba el nombre de uno de los dominios que quiere permitir. Si hay varios dominios, especifique cada dominio en una nueva línea. Por ejemplo:

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

contoso.com

fabrikam.com

example.com or *.example.com or example.*

6. Cuando haya terminado, haga clic en **Guardar**.

Después de establecer la directiva, si intenta invitar a un usuario de un dominio que no está en la lista de permitidos, recibirá un mensaje que indica que la directiva de invitación actual bloquea el dominio del usuario.

Cambio de la lista de permitidos a la lista de denegación y viceversa

Si cambia de una directiva a la otra, se descarta la configuración de directiva existente. Asegúrese de realizar una copia de seguridad de los detalles de la configuración antes de ejecutar el cambio.

Definición de la directiva de lista de permitidos o lista de denegación con PowerShell

Requisito previo

NOTE

El módulo AzureADPreview no es un módulo totalmente compatible, ya que se encuentra en versión preliminar.

Para establecer la lista de permitidos o de denegación mediante PowerShell, debe instalar la versión preliminar del Módulo Azure Active Directory para Windows PowerShell. En concreto, instale la versión 2.0.0.98 o superior del módulo AzureADPreview.

Para comprobar la versión del módulo (y ver si está instalado):

1. Abra Windows PowerShell como usuario con privilegios elevados (Ejecutar como administrador).
2. Ejecute el siguiente comando para ver si tiene alguna versión del Módulo Azure Active Directory para Windows PowerShell instalada en el equipo:

```
Get-Module -ListAvailable AzureAD*
```

Si el módulo no está instalado o no tiene la versión adecuada, realice lo siguiente:

- Si no se devuelve ningún resultado, ejecute el siguiente comando para instalar la versión más reciente del módulo AzureADPreview:

```
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureAD en los resultados, ejecute los comandos siguientes para instalar el módulo AzureADPreview:

```
Uninstall-Module AzureAD  
Install-Module AzureADPreview
```

- Si solo se muestra el módulo AzureADPreview en los resultados, pero la versión es inferior a 2.0.0.98, ejecute los siguientes comandos para actualizarla:

```
Uninstall-Module AzureADPreview  
Install-Module AzureADPreview
```

- Si ambos módulos, AzureAD y AzureADPreview, se muestran en los resultados, pero la versión del módulo AzureADPreview es inferior a la 2.0.0.98, ejecute los siguientes comandos para actualizarla:

```
Uninstall-Module AzureAD  
Uninstall-Module AzureADPreview  
Install-Module AzureADPreview
```

Uso de los cmdlets de AzureADPolicy para configurar la directiva

Para crear una lista de permitidos o de denegación, use el cmdlet [New-AzureADPolicy](#). En el ejemplo siguiente se muestra cómo establecer una lista de denegación que bloquea el dominio "live.com".

```
$policyValue = @(`"B2BManagementPolicy`":{`"InvitationsAllowedAndBlockedDomainsPolicy`":  
`"AllowedDomains`": [],`"BlockedDomains`": [`"live.com`"]}}})  
  
New-AzureADPolicy -Definition $policyValue -DisplayName B2BManagementPolicy -Type B2BManagementPolicy -  
IsOrganizationDefault $true
```

A continuación se muestra el mismo ejemplo, pero con la definición de directiva insertada.

```
New-AzureADPolicy -Definition @(`"B2BManagementPolicy`":{`"InvitationsAllowedAndBlockedDomainsPolicy`":  
`"AllowedDomains`": [],`"BlockedDomains`": [`"live.com`"]}}}) -DisplayName B2BManagementPolicy -Type  
B2BManagementPolicy -IsOrganizationDefault $true
```

Para establecer la directiva de lista de permitidos o de denegación, use el cmdlet [Set-AzureADPolicy](#). Por ejemplo:

```
Set-AzureADPolicy -Definition $policyValue -Id $currentpolicy.Id
```

Para obtener la directiva, use el cmdlet [Get-AzureADPolicy](#). Por ejemplo:

```
$currentpolicy = Get-AzureADPolicy -All $true | ?{$_.Type -eq 'B2BManagementPolicy'} | select -First 1
```

Para quitar la directiva, use el cmdlet [Remove-AzureADPolicy](#). Por ejemplo:

```
Remove-AzureADPolicy -Id $currentpolicy.Id
```

Pasos siguientes

- Para información general sobre B2B de Azure AD, consulte [¿Qué es la colaboración B2B de Azure AD?](#)
- Para información sobre el acceso condicional y la colaboración B2B, consulte [Acceso condicional para](#)

usuarios de colaboración B2B.

Incorporación de usuarios invitados de colaboración B2B sin enlace ni correo electrónico de invitación

18/02/2021 • 3 minutes to read • [Edit Online](#)

Ahora puede invitar a usuarios mediante el envío de un [vínculo directo](#) a una aplicación compartida. Con este método, los usuarios invitados ya no necesitan usar el correo electrónico de invitación, excepto en algunos casos especiales. Un usuario invitado hace clic en el vínculo de la aplicación, revisa y acepta los términos de privacidad y, después, accede sin problemas a la aplicación. Para más información, consulte [Canje de invitación de colaboración B2B](#).

Antes de que este nuevo método estuviera disponible, podía invitar a los usuarios sin necesidad del correo electrónico de invitación al agregar un invitador (de su organización o de una organización asociada) al rol de directorio **Invitador de usuarios** y, después, hacer que el invitador agregara a los usuarios al directorio, los grupos o las aplicaciones a través de la interfaz de usuario o de PowerShell. (Si usa PowerShell, puede suprimir por completo el correo electrónico de invitación). Por ejemplo:

1. Un usuario de la organización anfitriona (por ejemplo, WoodGrove) invita a un usuario de la organización asociada (por ejemplo, Sam@litware.com) como invitado.
2. El administrador de la organización anfitriona [configura directivas](#) que permiten a Sam identificar y agregar otros usuarios de la organización asociada (Litware). (Debe agregarse a Sam al rol **Invitador de usuarios**).
3. Ahora, Sam puede agregar otros usuarios de Litware al directorio, los grupos o las aplicaciones de WoodGrove sin necesidad de canjear invitaciones. Si Sam tiene los privilegios de enumeración adecuados en Litware, se hará automáticamente.

Este método original sigue funcionando, pero hay una pequeña diferencia en el comportamiento. Si usa PowerShell, observará que una cuenta invitada ahora tiene un estado **PendingAcceptance** en lugar de mostrar inmediatamente como **Accepted**. Aunque el estado sea pendiente, el usuario invitado todavía puede iniciar sesión y acceder a la aplicación sin hacer clic en un vínculo de invitación por correo electrónico. El estado pendiente significa que el usuario aún no ha pasado la [experiencia de consentimiento](#), donde se aceptan los términos de privacidad de la organización que invita. El usuario invitado ve esta pantalla de consentimiento cuando inicia sesión por primera vez.

Si invita a un usuario al directorio, el usuario invitado debe acceder directamente a la URL de Azure Portal específica de su inquilino de recursos (como https://portal.azure.com/*inquilinoderecursos*.onmicrosoft.com) para ver y aceptar los términos de privacidad.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Canje de invitación de colaboración B2B](#)
- [Delegación de invitaciones de la colaboración B2B de Azure Active Directory](#)
- [¿Cómo agregan los trabajadores de la información usuarios de colaboración B2B?](#)

Personalización y API de colaboración B2B de Active Directory Azure

18/02/2021 • 5 minutes to read • [Edit Online](#)

Hemos tenido muchos clientes que nos han dicho que querían personalizar el proceso de invitación de una forma que se adapte menor a sus organizaciones. Con nuestra API, pueden hacer justamente eso.

<https://developer.microsoft.com/graph/docs/api-reference/v1.0/resources/invitation>

Funcionalidades de la API de invitación

La API ofrece las siguientes funcionalidades:

1. Invite a un usuario externo con *cualquier* dirección de correo electrónico.

```
"invitedUserDisplayName": "Sam"  
"invitedUserEmailAddress": "gsamoogle@gmail.com"
```

2. Personalice a qué página desea que lleguen los usuarios finales después de aceptar la invitación.

```
"inviteRedirectUrl": "https://myapps.microsoft.com/"
```

3. Seleccione enviar el correo electrónico de invitación estándar por medio de nosotros

```
"sendInvitationMessage": true
```

con un mensaje al destinatario que pueda personalizar.

```
"customizedMessageBody": "Hello Sam, let's collaborate!"
```

4. Luego, ponga en copia a los usuarios a los que informar de que ha invitado a este colaborador.

5. También puede personalizar completamente su invitación y el flujo de trabajo de incorporación decidiendo no enviar notificaciones a través de Azure AD.

```
"sendInvitationMessage": false
```

En este caso, obtendrá una URL de canje a través de la API, que puede incrustar en una plantilla de correo electrónico, mensaje instantáneo u otro método de distribución que prefiera.

6. Finalmente, si es administrador, puede invitar al usuario como miembro.

```
"invitedUserType": "Member"
```

Determinación de si ya se invitó a un usuario a su directorio

Puede usar la API de invitación para determinar si ya existe un usuario en el inquilino de recursos. Esto puede ser útil cuando está desarrollando una aplicación que usa la API de invitación para invitar a un usuario. Si el

usuario ya existe en el directorio de recursos, no recibirá una invitación, por lo que puede ejecutar primero una consulta para determinar si el correo electrónico ya existe como nombre principal de usuario u otra propiedad de inicio de sesión.

1. Asegúrese de que el dominio de correo electrónico del usuario no forma parte del dominio comprobado del inquilino de recursos.
2. En el inquilino de recursos, use la consulta get user siguiente, donde {0} es la dirección de correo electrónico a la que va a invitar:

```
"userPrincipalName eq '{0}' or mail eq '{0}' or proxyAddresses/any(x:x eq 'SMTP:{0}') or signInNames/any(x:x eq '{0}') or otherMails/any(x:x eq '{0}')"
```

Modelo de autorización

La API se puede ejecutar en los siguientes modos de autorización:

Aplicación y modo de usuario

En este modo, el usuario que usa la API debe tener los permisos necesarios para crear invitaciones de B2B.

Modo de solo aplicación

En el contexto de solo aplicación, la aplicación necesita el ámbito User.Invite.All para que la invitación se realice correctamente.

Para más información, consulte: https://developer.microsoft.com/graph/docs/authorization/permission_scopes

PowerShell

Puede usar PowerShell para agregar e invitar a usuarios externos a una organización fácilmente. Cree una nueva invitación mediante el cmdlet:

```
New-AzureADMSInvitation
```

Puede utilizar las siguientes opciones:

- -InvitedUserDisplayName
- -InvitedUserEmailAddress
- -SendInvitationMessage
- -InvitedUserMessageInfo

Estado de la invitación

Después de enviar una invitación a un usuario externo, puede usar el cmdlet Get-AzureADUser para ver si ya la ha aceptado. Cuando se envía una invitación a un usuario externo, se llenan las propiedades siguientes de Get-AzureADUser:

- **UserState** indica si la invitación está en el estado **PendingAcceptance** o **Accepted**.
- **UserStateChangedOn** muestra la marca de tiempo del cambio más reciente de la propiedad **UserState**.

Puede usar la opción **Filter** para filtrar los resultados por **UserState**. En el ejemplo siguiente se muestra cómo filtrar resultados para mostrar solo a los usuarios que tienen una invitación pendiente. En el ejemplo también se muestra la opción **Format-List**, que le permite especificar las propiedades que se van a mostrar.

```
Get-AzureADUser -Filter "UserState eq 'PendingAcceptance'" | Format-List -Property  
DisplayName,UserPrincipalName,UserState,UserStateChangedOn
```

NOTE

Asegúrese de que tiene la versión más reciente del módulo de AzureAD PowerShell o del módulo AzureADPreview PowerShell.

Consulte también

Consulte la referencia de API de invitación en <https://developer.microsoft.com/graph/docs/api-reference/v1.0/resources/invitation>.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Los elementos del correo electrónico de invitación de colaboración B2B](#)
- [Canje de invitación de colaboración B2B](#)
- [Incorporación de usuarios de colaboración B2B sin invitación](#)

Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B

18/02/2021 • 12 minutes to read • [Edit Online](#)

Si configura la federación con Google, puede permitir que los usuarios invitados puedan iniciar sesión en sus aplicaciones y recursos compartidos con sus propias cuentas de Google, sin tener que crear cuentas Microsoft.

NOTE

La federación de Google está diseñada específicamente para los usuarios de Gmail. Para realizar la federación con los dominios de G Suite, use la [federación directa](#).

IMPORTANT

A partir del 4 de enero de 2021, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa la federación de Google o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).

¿Cuál es la experiencia del usuario de Google?

Cuando envíe una invitación a usuarios de Gmail de Google, el usuario invitado debe acceder a sus aplicaciones o recursos compartidos mediante un vínculo que incluya el contexto del inquilino. Su experiencia varía en función de si ya han iniciado sesión en Google:

- Se pedirá a los usuarios invitados que no hayan iniciado sesión en Google que lo hagan.
- Se pedirá a los usuarios invitados que ya hayan iniciado sesión en Google que elijan la cuenta que desean usar. Deben elegir la cuenta donde hayan recibido la invitación.

Los usuarios invitados que ven un error "encabezado demasiado largo" pueden eliminar sus cookies o abrir una ventana privada o de incógnito e intentar iniciar sesión de nuevo.



Sign in

to continue to microsoftonline.com

Email or phone

[Forgot email?](#)

To continue, Google will share your name, email address, and profile picture with microsoftonline.com.

[Create account](#) Next

Desuso de la compatibilidad con el inicio de sesión en WebView

A partir del 4 de enero de 2021, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa la federación de Google o el [registro de autoservicio con Gmail](#), debería comprobar la compatibilidad de las aplicaciones nativas de línea de negocio. Si las aplicaciones incluyen contenido de WebView que requiere autenticación, los usuarios de Gmail de Google no podrán autenticarse. Estos son escenarios conocidos que afectarán a los usuarios de Gmail:

- Aplicaciones de Windows que usan WebView insertado o WebAccountManager (WAM) en versiones anteriores de Windows.
- Otras aplicaciones nativas que haya desarrollado que usen un marco de explorador insertado para la autenticación.

Este cambio no afecta a:

- Aplicaciones de Windows que usan WebView insertado o WebAccountManager (WAM) en las versiones más recientes de Windows
- Aplicaciones de Microsoft iOS
- Identidades de G Suite; por ejemplo, cuando se usa la [federación directa basada en SAML](#) con G Suite

Seguimos probando varias plataformas y escenarios y actualizaremos este artículo en consecuencia.

Para probar la compatibilidad de las aplicaciones:

1. Siga la [guía de Google](#) para determinar si sus aplicaciones se verán afectadas por este cambio.
2. Con Fiddler u otra herramienta de prueba, inserte un encabezado durante el inicio de sesión y use una identidad externa de Google para probar el inicio de sesión:
 - a. Agregue Google-Accounts-Check-OAuth-Login:true a sus encabezados de solicitud HTTP cuando se envíen las solicitudes a accounts.google.com.
 - b. Intente iniciar sesión en la aplicación escribiendo una dirección de Gmail en la página de inicio de sesión de accounts.google.com.
 - c. Si se produce un error de inicio de sesión y ve un error que dice que es posible que el explorador o la

aplicación no sean seguros, se bloqueará el inicio de sesión para las identidades externas de Google.

3. Para resolver este problema, haga lo siguiente:

- Si la aplicación de Windows usa WebView insertado o WebAccountManager (WAM) en una versión anterior de Windows, actualice a la versión más reciente de esta plataforma.
- Modifique sus aplicaciones para que usen el explorador del sistema para el inicio de sesión. Para más información, consulte [Interfaz de usuario web del sistema frente a insertada](#) en la documentación de MSAL.NET.

Puntos de conexión de inicio de sesión

Teams admite totalmente a los usuarios invitados de Google en todos los dispositivos. Los usuarios de Google pueden iniciar sesión en Teams desde un punto de conexión común, como <https://teams.microsoft.com>.

Es posible que los puntos de conexión comunes de otras aplicaciones no admitan a los usuarios de Google. Los usuarios invitados de Google deberán iniciar sesión con un vínculo que incluya la información del inquilino. A continuación, se muestran algunos ejemplos:

- <https://myapps.microsoft.com/?tenantid=<your tenant ID>>
- <https://portal.azure.com/<your tenant ID>>
- <https://myapps.microsoft.com/<your verified domain>.onmicrosoft.com>

Si los usuarios invitados de Google intentan usar un vínculo como <https://myapps.microsoft.com> o <https://portal.azure.com>, recibirán un error.

También puede proporcionar a los usuarios invitados de Google un vínculo directo a una aplicación o recurso, siempre que el vínculo incluya la información del inquilino. Por ejemplo,

<https://myapps.microsoft.com/signin/Twitter/<application ID?tenantId=<your tenant ID>>.

Paso 1: configuración de un proyecto de desarrollador de Google

En primer lugar, cree un proyecto en la consola de desarrolladores de Google para obtener un identificador y un secreto de cliente que pueda agregar después a Azure Active Directory (Azure AD).

1. Vaya a las API de Google de <https://console.developers.google.com> e inicie sesión con su cuenta de Google. Se recomienda utilizar una cuenta de Google compartida con el equipo.
2. Si se le solicita, acepte los términos del servicio.
3. Cree un nuevo proyecto: En el panel, seleccione **Crear proyecto**, asigne un nombre al proyecto (por ejemplo, **Azure AD B2B**), y, después, seleccione **Crear**:

New Project

You have 11 projects remaining in your quota. Request an increase or delete projects.
[Learn more](#)

[MANAGE QUOTAS](#)

Project Name * [?](#)

Project ID: myb2bapp. It cannot be changed later. [EDIT](#)

Location * [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

4. En la página **API y servicios**, seleccione **Ver** en el nuevo proyecto.
5. Seleccione **Go to APIs overview** (Ir a la información general de las API) en la tarjeta de API. Seleccione **OAuth consent screen** (Pantalla de consentimiento de OAuth).
6. Seleccione **Externo** y después **Crear**.
7. En la **Pantalla de consentimiento de OAuth**, especifique un **nombre de aplicación**:

OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status
Not published

Application name [?](#)
The name of the app asking for consent

Application logo [?](#)
An image on the consent screen that will help users recognize your app
 [Browse](#)



8. Desplácese hasta la sección **Dominios autorizados** y escriba **microsoftonline.com**:

The screenshot shows the 'Authorized domains' section of the Google Cloud Platform Credentials page. It includes a 'Add scope' button and a note about protecting users. Two domains are listed: 'microsoftonline.com' (highlighted with a red box) and 'example.com'. A trash can icon is next to each domain entry.

9. Seleccione Guardar.

10. Seleccione Credenciales. En el menú Crear credenciales, seleccione Id. del cliente de OAuth.

The screenshot shows the 'Create credentials' dropdown menu. The 'OAuth client ID' option is selected and highlighted with a blue background. Other options shown include 'API key', 'Service account key', and 'Help me choose'.

11. En Application type (Tipo de aplicación), seleccione Web application (Aplicación web). Asigne un nombre adecuado a la aplicación, como Azure AD B2B. En URI de redirección autorizados, escriba los siguientes URI:

- `https://login.microsoftonline.com`
- `https://login.microsoftonline.com/te/<tenant ID>/oauth2/authresp`
(donde `<tenant ID>` es el id. de inquilino)

NOTE

Para buscar el identificador de inquilino, vaya a [Azure Portal](#). En **Azure Active Directory**, seleccione **Propiedades** y copie el **Id. del inquilino**.

[←](#) Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

Application type

Web application

Android [Learn more](#)

Chrome App [Learn more](#)

iOS [Learn more](#)

Other

Name [?](#)

AAD B2B Web App

Restrictions

Enter JavaScript origins, redirect URIs, or both [Learn More](#)

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (<https://example.com/subdir>). If you're using a nonstandard port, you must include it in the origin URI.

<https://www.example.com>

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

<https://login.microsoftonline.com>

<https://login.microsoftonline.com/te/.../oauth2/authresp>

<https://www.example.com>

[Create](#) [Cancel](#)

12. Seleccione **Crear**. Copie el identificador de cliente y del secreto de cliente. Los usará cuando agregue el proveedor de identidades en Azure Portal.

OAuth client

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth is limited to 100 sensitive scope logins until the [OAuth consent screen](#) is published. This may require a verification process that can take several days.

Here is your client ID

<https://... .apps.googleusercontent.com>

Here is your client secret

<https://...>

[OK](#)

Paso 2: configuración de la federación de Google en Azure AD

Defina ahora el identificador y el secreto de cliente de Google. Para ello, puede usar Azure Portal o PowerShell. No olvide probar la configuración de la federación de Google; para ello, invítese a usted mismo. Use una

dirección de Gmail e intente canjear la invitación con su cuenta de Google invitada.

Para configurar la federación de Google en Azure Portal

1. Vaya a [Azure Portal](#). En el panel izquierdo, seleccione **Azure Active Directory**.
2. Seleccione **External Identities**.
3. Seleccione **Todos los proveedores de identidades** y haga clic en el botón de Google.
4. Escriba el identificador y el secreto de cliente que obtuvo anteriormente. Seleccione **Guardar**:

The screenshot shows a modal dialog titled 'Add Google identity provider'. It contains fields for 'Name' (set to 'Google'), 'Client ID' (set to 'Client ID'), and 'Client secret' (set to 'Client secret'). A note at the top states: 'You must configure credentials at Google APIs first to get the client ID and client secret.' A 'Save' button is at the bottom.

Configuración de la federación de Google con PowerShell

1. Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)).
2. Ejecute este comando: `Connect-AzureAD`
3. En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.
4. Ejecute el siguiente comando:

```
New-AzureADMSIdentityProvider -Type Google -Name Google -ClientId <client ID> -ClientSecret <client secret>
```

NOTE

Use el identificador y secreto de cliente de la aplicación que creó en el "Paso 1: configuración de un proyecto de desarrollador de Google". Para más información, vea [New-AzureADMSIdentityProvider](#).

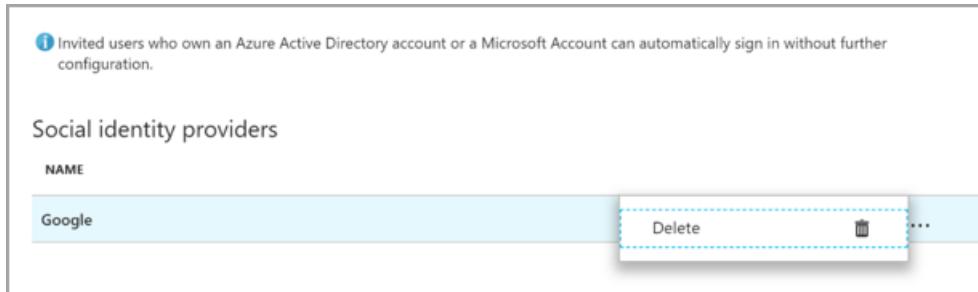
¿Cómo se quita la federación de Google?

La configuración de la federación de Google se puede eliminar. Si lo hace, los usuarios invitados de Google que

ya hayan canjeado su invitación no podrán iniciar sesión. Pero puede darles acceso a los recursos de nuevo si los elimina del directorio y los vuelve a invitar.

Para eliminar la federación de Google desde el portal de Azure AD

1. Vaya a [Azure Portal](#). En el panel izquierdo, seleccione Azure Active Directory.
2. Seleccione External Identities.
3. Seleccione Todos los proveedores de identidades.
4. En la línea de Google, seleccione el botón de puntos suspensivos (...) y, a continuación, seleccione Eliminar.



5. Seleccione Sí para confirmar la eliminación.

Para eliminar la federación de Google mediante PowerShell

1. Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)).
2. Ejecute `Connect-AzureAD`.
3. En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.
4. Escriba el comando siguiente:

```
Remove-AzureADMSIdentityProvider -Id Google-OAUTH
```

NOTE

Para más información, consulte [Remove-AzureADMSIdentityProvider](#).

Incorporación de Facebook como proveedor de identidades para identidades externas

18/02/2021 • 8 minutes to read • [Edit Online](#)

Puede agregar Facebook a los flujos de usuario del registro de autoservicio (versión preliminar) para que los usuarios puedan iniciar sesión en sus aplicaciones con sus propias cuentas de Facebook. Para que los usuarios puedan iniciar sesión con Facebook, primero deberá [habilitar el registro de autoservicio](#) del inquilino. Después de agregar Facebook como proveedor de identidades, configure un flujo de usuario para la aplicación y seleccione Facebook como una de las opciones de inicio de sesión.

NOTE

Los usuarios solo pueden usar sus cuentas de Facebook para suscribirse a través de aplicaciones mediante el registro de autoservicio y los flujos de usuario. No se puede invitar a los usuarios y canjear su invitación mediante una cuenta de Facebook.

Creación de una aplicación en la consola de desarrolladores de Facebook

Para usar una cuenta de Facebook como [proveedor de identidades](#), debe crear una aplicación en la consola de desarrolladores de Facebook. Si aún no tiene una cuenta de Facebook, puede suscribirse en <https://www.facebook.com/>.

NOTE

Use las direcciones URL siguientes en los pasos 9 y 16 que verá a continuación.

- En **URL del sitio**, escriba la dirección de la aplicación, como `https://contoso.com`.
- En **Valid OAuth redirect URIs** (URI de redireccionamiento OAuth válidos), escriba `https://login.microsoftonline.com/te/<tenant-id>/oauth2/authresp`. Puede encontrar el valor `<tenant-ID>` en la hoja de información general de Azure Active Directory.

1. Inicie sesión en [Facebook for developers](#) con las credenciales de su cuenta de Facebook.
2. Si aún no lo ha hecho, debe registrarse como desarrollador de Facebook. Para ello, seleccione **Get Started** (Comenzar) en la esquina superior derecha de la página, acepte las directivas de Facebook y complete los pasos de registro.
3. Seleccione **Mis aplicaciones** y después **Crear una aplicación**.
4. Especifique el valor de **Display Name** (Nombre para mostrar) y un valor de **Contact Email** (Correo electrónico de contacto) válido.
5. Seleccione **Create App ID** (Crear identificador de aplicación). Es posible que deba aceptar las políticas de la plataforma Facebook y realizar una comprobación de seguridad en línea.
6. Seleccione **Settings** (Configuración) > **Basic** (Básica).
7. Elija una **Categoría**, por ejemplo, Negocios y Páginas. Este valor es obligatorio para Facebook, pero no se usa para Azure AD.
8. En la parte inferior de la página, seleccione **Add Platform** (Aregar plataforma) y, después, seleccione **Website** (Sitio web).
9. En la **dirección URL del sitio**, escriba la dirección URL adecuada (indicada anteriormente).

10. En la dirección URL de la directiva de privacidad , escriba la dirección URL de la página donde se mantiene la información de privacidad de la aplicación; por ejemplo, `http://www.contoso.com` .
11. Seleccione **Save changes** (Guardar los cambios).
12. En la parte superior de la página, copie el valor de **App ID** (Id. de la aplicación).
13. Seleccione **Show** (Mostrar) y copie el valor de **App Secret** (Secreto de la aplicación). Use ambos para configurar Facebook como proveedor de identidades de su inquilino. El **secreto de la aplicación** es una credencial de seguridad importante.
14. Seleccione el signo más junto a **PRODUCTS** (Productos) y, después, seleccione **Set up** (Configurar) en **Facebook Login** (Inicio de sesión de Facebook).
15. En **Facebook Login** (Inicio de sesión de Facebook), seleccione **Settings** (Configuración).
16. En **Valid OAuth redirect URIs** (URI de redireccionamiento OAuth válidos), escriba la dirección URL adecuada (indicada anteriormente).
17. Seleccione **Save Changes** (Guardar cambios) en la parte inferior de la página.
18. Para que la aplicación de Facebook esté disponible para Azure AD, seleccione el selector de Estado situado en la parte superior derecha de la página y **actívelo** para hacer que la aplicación sea pública y, después, seleccione **Switch Mode** (Modo de conmutador). En este momento el estado debería cambiar de **Desarrollo a Activo** .

Configuración de una cuenta de Facebook como proveedor de identidades

Ahora podrá establecer el identificador y el secreto de cliente de Facebook, ya sea escribiéndolo en el portal de Azure AD o con PowerShell. Puede probar la configuración de Facebook al suscribirse a través de un flujo de usuario en una aplicación habilitada para el registro de autoservicio.

Para configurar la federación de Facebook en el portal de Azure AD

1. Inicie sesión en [Azure Portal](#) como administrador global del inquilino de Azure AD.
2. En **Servicios de Azure** , seleccione **Azure Active Directory** .
3. En el menú de la izquierda, seleccione **External Identities** .
4. Seleccione **All identity providers** (Todos los proveedores de identidades) y, a continuación, **Facebook** .
5. En el **id. de cliente** , escriba el **id. de aplicación** de Facebook que creó anteriormente.
6. En el **secreto de cliente** , escriba el **secreto de aplicación** que ha anotado.

The screenshot shows the 'Add social identity provider' dialog box. It has a header 'Add social identity provider' and a close button 'X'. Below the header is a note: 'You must configure your Facebook Developer account first to get a client ID and client secret. [Learn more](#)'. There are three input fields: 'Name' (set to 'Facebook'), 'Client ID *' (empty), and 'Client secret *' (empty). Each field has a placeholder text: 'Facebook', 'Client ID', and 'Client secret' respectively.

7. Seleccione **Guardar** .

Para configurar la federación de Facebook con PowerShell

1. Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)).
2. Ejecute el siguiente comando: `Connect-AzureAD`.
3. En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.
4. Ejecute el siguiente comando:

```
New-AzureADMSIdentityProvider -Type Facebook -Name Facebook -ClientId [Client ID] -ClientSecret  
[Client secret]
```

NOTE

Use el identificador y secreto de cliente de la aplicación que creó anteriormente en la consola para desarrolladores de Facebook. Para más información, consulte el artículo sobre [New AzureADMSIdentityProvider](#).

¿Cómo se quita una federación de Facebook?

La configuración de la federación de Facebook se puede eliminar. Si lo hace, los usuarios que se hayan registrado a través de flujos de usuario con sus cuentas de Facebook ya no podrán iniciar sesión.

Para eliminar la federación de Facebook en el portal de Azure AD:

1. Vaya a [Azure Portal](#). En el panel izquierdo, seleccione Azure Active Directory .
2. Seleccione External Identities .
3. Seleccione Todos los proveedores de identidades .
4. En la línea de Facebook , seleccione el menú contextual (...) y, después, seleccione Eliminar .
5. Seleccione Sí para confirmar la eliminación.

Para eliminar la federación de Facebook con PowerShell:

1. Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)).
2. Ejecute `Connect-AzureAD`.
3. En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.
4. Escriba el comando siguiente:

```
Remove-AzureADMSIdentityProvider -Id Facebook-OAUTH
```

NOTE

Para más información, consulte [Remove-AzureADMSIdentityProvider](#).

Pasos siguientes

- [Incorporación del registro de autoservicio a una aplicación](#)

Federación directa con AD FS y proveedores de terceros para usuarios invitados (versión preliminar)

18/02/2021 • 23 minutes to read • [Edit Online](#)

NOTE

La federación directa es una característica en versión preliminar pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

En este artículo se describe cómo establecer una federación directa con otra organización para la colaboración B2B. Puede establecer una federación directa con cualquier organización cuyo proveedor de identidades (IdP) admite el protocolo SAML 2.0 o WS-Fed. Al configurar una federación directa con el proveedor de identidades de un asociado, los nuevos usuarios invitados de ese dominio pueden utilizar su propia cuenta de organización administrada por el proveedor de identidades para iniciar sesión con su inquilino de Azure AD y empezar a colaborar con usted. No es necesario que el usuario invitado cree otra cuenta de Azure AD.

NOTE

Los usuarios invitados de federación directa deben iniciar sesión con un vínculo que incluye el contexto del inquilino (por ejemplo, `https://myapps.microsoft.com/?tenantid=<tenant id>` o `https://portal.azure.com/<tenant id>`, o, en el caso de un dominio comprobado, `https://myapps.microsoft.com/\<verified domain>.onmicrosoft.com`). Los vínculos directos a aplicaciones y los recursos también funcionan siempre que incluyan el contexto del inquilino. Actualmente, los usuarios de federación directa no pueden iniciar sesión con puntos de conexión comunes sin contexto de inquilino. Por ejemplo, si se usa `https://myapps.microsoft.com`, `https://portal.azure.com` o `https://teams.microsoft.com`, se producirá un error.

¿Cuándo se autentica un usuario invitado con la federación directa?

Después de configurar la federación directa con una organización, cualquier nuevo usuario invitado se autenticará mediante la federación directa. Es importante tener en cuenta que la configuración de la federación directa no cambia el método de autenticación para los usuarios invitados que ya han canjeado una invitación. Estos son algunos ejemplos:

- Si los usuarios invitados ya han canjeado sus invitaciones y posteriormente configura la federación directa con su organización, esos usuarios invitados seguirán utilizando el mismo método de autenticación que utilizaron antes de configurar la federación directa.
- Si se configura una federación directa con una organización asociada y se invita a los usuarios y después la organización asociada se traslada a Azure AD, los usuarios invitados que ya han canjeado las invitaciones seguirán utilizando la federación directa, siempre y cuando exista la directiva de federación directa en el inquilino.
- Si se elimina la federación directa con una organización asociada, los usuarios invitados que actualmente utilizan la federación directa no podrán iniciar sesión.

En cualquiera de estos escenarios, puede actualizar el método de autenticación de un usuario invitado eliminando la cuenta de usuario invitado de su directorio y volviéndole a invitar.

La federación directa está asociada a espacios de nombres de dominio, como contoso.com y fabrikam.com. Al establecer una configuración de federación directa con AD FS o un proveedor de identidades de terceros, las organizaciones asocian uno o más espacios de nombres de dominio a estos proveedor de identidades.

Experiencia del usuario final

Con la federación directa, los usuarios invitados inician sesión en el inquilino de Azure AD mediante su propia cuenta de organización. Cuando acceden a los recursos compartidos y se les pide que inicien sesión, los usuarios de la federación directa se redirigen al proveedor de identidades. Después del inicio de sesión correcto, vuelven a Azure AD para acceder a los recursos. Los tokens de actualización de los usuarios de la federación directa son válidos durante 12 horas, [la duración predeterminada del token de actualización de acceso directo en Azure AD](#). Si el proveedor de identidades federado tiene el inicio de sesión único habilitado, el usuario experimentará un inicio de sesión único y no verá ninguna solicitud de inicio de sesión después de la autenticación inicial.

Limitaciones

Dominios comprobados por DNS en Azure AD

El dominio con el que desea federarse ***no** puede estar verificado por DNS en Azure AD. Se puede realizar una federación directa en los inquilinos no administrados (comprobados por correo electrónico o "viral") de Azure AD porque no están comprobados por DNS.

Dirección URL de autenticación

La federación directa solo se permite para las directivas en las que el dominio de la dirección URL de autenticación coincide con el dominio de destino, o en las que la dirección URL de autenticación es uno de estos proveedores de identidades permitidos (esta lista está sujeta a cambios):

- accounts.google.com
- pingidentity.com
- login.pingone.com
- okta.com
- oktapreview.com
- okta-emea.com
- my.salesforce.com
- federation.exostar.com
- federation.exostartest.com

Por ejemplo, al configurar la federación directa para ***fabrikam.com****, la dirección URL de autenticación `https://fabrikam.com/adfs` pasará la validación. Un host en el mismo dominio también pasará, por ejemplo `https://sts.fabrikam.com/adfs`. Sin embargo, la dirección URL de autenticación `https://fabrikamconglomerate.com/adfs` o `https://fabrikam.com.uk/adfs` para el mismo dominio no pasará.

Renovación del certificado de firma

Si especifica la dirección URL de metadatos en la configuración del proveedor de identidades, Azure AD renovará automáticamente el certificado de firma cuando expire. Sin embargo, si el certificado se gira por cualquier razón antes de la hora de expiración, o si no proporciona una dirección URL de metadatos, Azure AD no podrá renovarlo. En este caso, deberá actualizar manualmente el certificado de firma.

Límite de relaciones de federación

Actualmente, se admite un máximo de 1000 relaciones de federación. Este límite incluye tanto las [federaciones internas](#) como las federaciones directas.

Límite de varios dominios

Actualmente no se admite la federación directa con varios dominios del mismo inquilino.

Preguntas más frecuentes

¿Puedo configurar la federación directa con un dominio para el que existe un inquilino no administrado (verificado por correo electrónico)?

Sí. Si el dominio no se ha comprobado y el inquilino no ha experimentado una [adquisición de administración](#),

puede configurar una federación directa con el dominio. Los inquilinos no administrados o comprobados por correo electrónico se crean cuando un usuario canjea una invitación B2B o realiza un registro de autoservicio para Azure AD mediante un dominio que no existe actualmente. Puede configurar la federación directa con estos dominios. Si intenta configurar la federación directa con un dominio comprobado por DNS, ya sea en Azure Portal o con PowerShell, verá un error.

Si la federación directa y la autenticación con código de acceso de un solo uso por correo electrónico están habilitadas, ¿qué método tiene prioridad?

Cuando se establece la federación directa con una organización asociada, tiene prioridad sobre la autenticación con código de acceso de un solo uso por correo electrónico para los nuevos usuarios invitados de esa organización. Si un usuario invitado ha canjeado una invitación mediante la autenticación de código de acceso de un solo uso antes de configurar la federación directa, seguirá utilizando la autenticación de código de acceso de un solo uso.

¿La federación directa se ocupa de los problemas de inicio de sesión debido a un inquilinato parcialmente sincronizado?

No, la característica del [código de acceso de un solo uso por correo electrónico](#) se debe usar en este escenario. Un "inquilinato parcialmente sincronizado" se refiere a un inquilino de Azure AD asociado en el que las identidades de usuario locales no están completamente sincronizadas con la nube. Un invitado cuya identidad aún no existe en la nube pero que intenta canjear su invitación de B2B no podrá iniciar sesión. La característica del código de acceso de un solo uso permitiría a este invitado iniciar sesión. La función de federación directa aborda escenarios en los que el invitado tiene su propia cuenta de organización administrada por el proveedor de identidades, pero la organización no tiene ninguna presencia de Azure AD.

Una vez configurada la federación directa con una organización, ¿es necesario enviar cada invitado y canjear una invitación individual?

La configuración de la federación directa no cambia el método de autenticación para los usuarios invitados que ya han canjeado una invitación. Para actualizar el método de autenticación de un usuario invitado, puede eliminar la cuenta de usuario invitado de su directorio y volverle a invitar.

Paso 1: Configuración del proveedor de identidades de la organización del asociado

En primer lugar, la organización asociada debe configurar el proveedor de identidades con las notificaciones necesarias y las veracidades de los usuarios de confianza.

NOTE

Para ilustrar cómo configurar un proveedor de identidades para la federación directa, usaremos los Servicios de federación de Active Directory (AD FS) como ejemplo. Consulte el artículo [Configuración de la federación directa con AD FS](#), que ofrece ejemplos de cómo configurar AD FS como un proveedor de identidades de SAML 2.0 o WS-Fed en preparación para la federación directa.

Configuración de SAML 2.0

Azure AD B2B se puede configurar para federarse con proveedores de identidades que usan el protocolo SAML con los requisitos específicos que se indican a continuación. Para más información sobre cómo establecer una confianza entre su proveedor de identidades SAML y Azure AD, consulte [Uso de un proveedor de identidades \(IdP\) de SAML 2.0 para el inicio de sesión único](#).

NOTE

El dominio de destino para la federación directa no debe ser comprobado por DNS en Azure AD. El dominio de la URL de autenticación debe coincidir con el dominio de destino o debe ser el dominio de un proveedor de identidades permitido. Consulte la sección [Limitaciones](#) para obtener más información.

En las tablas siguientes se muestran los requisitos de los atributos y las notificaciones específicos que se deben configurar en el proveedor de identidades de terceros. Para establecer una federación directa, se deben recibir los siguientes atributos en la respuesta de SAML 2.0 del proveedor de identidades. Estos atributos se pueden configurar mediante la vinculación con el archivo XML del servicio de token de seguridad en línea o la introducción manual.

Atributos necesarios para la respuesta de SAML 2.0 desde el proveedor de identidades:

ATRIBUTO	VALUE
AssertionConsumerService	https://login.microsoftonline.com/login.srf
Público	urn:federation:MicrosoftOnline
Emisor	El URI del emisor del asociado IdP, por ejemplo http://www.example.com/exk1016w90DHM0yi...

Las notificaciones necesarias para el token de SAML 2.0 emitido por el proveedor de identidades:

ATRIBUTO	VALUE
Formato de NameID	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
emailaddress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddr

Configuración de WS-Fed

Se puede configurar Azure AD B2B para que funcione con proveedores de identidades que usan el protocolo WS-Fed con algunos requisitos específicos, que se indican a continuación. Actualmente, los dos proveedores de WS-Fed se han probado para determinar su compatibilidad con Azure AD e incluyen AD FS y Shibboleth. Para más información sobre cómo establecer la veracidad de un usuario de confianza entre un proveedor compatible con WS-Fed y Azure AD, consulte el documento "STS Integration Paper using WS Protocols" (Documento de integración con STS mediante protocolos WS) en los [documentos de compatibilidad del proveedor de identidades de Azure AD](#).

NOTE

El dominio de destino para la federación directa no debe ser comprobado por DNS en Azure AD. El dominio de la URL de autenticación debe coincidir con el dominio de destino o con el dominio de un proveedor de identidades permitido. Consulte la sección [Limitaciones](#) para obtener más información.

Atributos y notificaciones de WS-Fed necesarios

En las tablas siguientes se muestran los requisitos de los atributos y las notificaciones específicos que se deben configurar en el proveedor de identidades de WS-Fed de terceros. Para configurar una federación directa, se deben recibir los siguientes atributos en el mensaje de WS-Fed del proveedor de identidades. Estos atributos se pueden configurar mediante la vinculación con el archivo XML del servicio de token de seguridad en línea o la introducción manual.

Atributos necesarios en el mensaje de WS-Fed desde el proveedor de identidades:

ATRIBUTO	VALUE
PassiveRequestorEndpoint	https://login.microsoftonline.com/login.srf
Público	urn:federation:MicrosoftOnline

ATTRIBUTO	VALUE
Emisor	El URI del emisor del asociado IdP, por ejemplo <code>http://www.example.com/exk1016w90DHM0yi...</code>

Las notificaciones necesarias para el token de WS-Fed emitido por el proveedor de identidades:

ATTRIBUTO	VALUE
ImmutableID	<code>http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID</code>
emailaddress	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>

Paso 2: Configuración de la federación directa en Azure AD

A continuación, va a configurar la federación con el proveedor de identidades en Azure AD configurado en el paso 1. Puede usar el portal de Azure AD o PowerShell. Pueden pasar de 5 a 10 minutos antes de que la directiva de la federación directa entre en vigor. Durante este tiempo, no intente canjear una invitación por el dominio de la federación directa. Los atributos siguientes son necesarios:

- URI del emisor del proveedor de identidades del asociado
- Punto de conexión de la autenticación pasiva del proveedor de identidades del asociado (solo se admite https)
- Certificado

Para configurar la federación directa en el portal de Azure AD

1. Vaya a [Azure Portal](#). En el panel izquierdo, seleccione **Azure Active Directory**.
2. Seleccione **External Identities > Todos los proveedores de identidades**.
3. Seleccione y, después, **Nuevo proveedor de identidades de SAML/WS-Fed**.

The screenshot shows the 'Organizational relationships - Identity providers' page in the Azure Active Directory portal. On the left, there's a sidebar with options like 'Users from other organizations', 'Identity providers' (which is selected and highlighted in blue), 'Consent options', 'Settings', 'Lifecycle management', 'Terms of use', 'Access reviews', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area has a search bar at the top. Below it, there are two sections: 'Social identity providers' (with a note about invited users) and 'SAML/WS-Fed identity providers'. The 'SAML/WS-Fed identity providers' section includes a search bar and a table with one row: 'fabrikam.com' under 'DOMAIN', 'SAML' under 'PROTOCOL', and a URL under 'ISSUER'. A red box highlights the '+ New SAML/WS-Fed IdP' button.

4. En la página **New SAML/WS-Fed IdP** (Nuevo proveedor de identidades de SAMS/WS-FED), en **Protocolo de proveedor de identidades**, seleccione **SAML** o **WS-FED**.

New SAML/WS-Fed IdP

! You must configure the federating identity provider first. [Learn more](#)

* Identity provider protocol
SAML

* Domain name of federating IdP
fabrikam.com

* Select a method for populating metadata
Parse metadata file

Metadata file
Browse for file

Parse

* Issuer URI
<http://www.example.com/exk10l6w90DHM0yi...>

* Passive authentication endpoint
<https://outlooknk1.example.com/app/outlook...>

* Certificate
MIIDpDCCAoygAwIBAgIGAWLVA3DIM

Metadata URL
https://idp.example.com:9031/pf/federation_...

5. Especifique el nombre de dominio de su organización asociada, que será el nombre de dominio de destino para la federación directa.
6. Puede cargar un archivo de metadatos para llenar los detalles correspondientes. Si decide escribir los metadatos manualmente, introduzca la siguiente información:
 - Nombre de dominio del proveedor de identidades del asociado
 - Identificador de entidad de proveedor de identidades del asociado
 - Punto de conexión de solicitante pasivo del proveedor de identidades del asociado
 - Certificado

NOTE

La dirección URL de metadatos es opcional, pero se recomienda encarecidamente. Si proporciona la dirección URL de metadatos, Azure AD puede renovar automáticamente el certificado de firma cuando expire. Si el certificado se gira por cualquier razón antes de la hora de expiración, o si no proporciona una dirección URL de metadatos, Azure AD no podrá renovarlo. En este caso, deberá actualizar manualmente el certificado de firma.

7. Seleccione **Guardar**.

Para configurar la federación directa en Azure AD con PowerShell

1. Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)). (Si necesita conocer pasos detallados, el inicio rápido para agregar un usuario invitado incluye la sección [Instalación del último módulo de AzureADPreview](#)).
2. Ejecute el siguiente comando:

```
Connect-AzureAD
```

3. En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.

- Ejecute los siguientes comandos, reemplazando los valores del archivo de metadatos de la federación.

Para el servidor de AD FS y Okta, el archivo de federación es federationmetadata.xml, por ejemplo:

```
https://sts.totheclouddemo.com/federationmetadata/2007-06/federationmetadata.xml
```

```
$federationSettings = New-Object Microsoft.Open.AzureAD.Model.DomainFederationSettings
$federationSettings.PassiveLogOnUri ="https://sts.totheclouddemo.com/adfs/ls/"
$federationSettings.LogOffUri = $federationSettings.PassiveLogOnUri
$federationSettings.IssuerUri = "http://sts.totheclouddemo.com/adfs/services/trust"
$federationSettings.MetadataExchangeUri="https://sts.totheclouddemo.com/adfs/services/trust/mex"
$federationSettings.SigningCertificate= <Replace with X509 signing cert's public key>
$federationSettings.PreferredAuthenticationProtocol="WsFed" OR "Samlp"
$domainName = <Replace with domain name>
New-AzureADEExternalDomainFederation -ExternalDomainName $domainName -FederationSettings
$federationSettings
```

Paso 3: Prueba de la federación directa en Azure AD

Ahora pruebe la configuración de la federación directa e invite a un nuevo usuario invitado de B2B. Para más información, consulte [Incorporación de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#).

¿Cómo se puede editar una relación de federación directa?

- Vaya a [Azure Portal](#). En el panel izquierdo, seleccione **Azure Active Directory**.
- Seleccione **External Identities**.
- Seleccione **Todos los proveedores de identidades**.
- En **SAML/WS-Fed identity providers** (Proveedores de identidades SAML/WS-Fed), seleccione el proveedor.
- En el panel de detalles del proveedor de identidades, actualice los valores.
- Seleccione **Guardar**.

¿Cómo se quita una federación directa?

Puede quitar la configuración de la federación directa. Si lo hace, los usuarios invitados de la federación directa que ya hayan canjeado sus invitaciones no podrán iniciar sesión. Pero puede darles acceso a los recursos de nuevo si los elimina del directorio y los vuelve a invitar. Para quitar una federación directa con un proveedor de identidades en el portal de Azure AD:

- Vaya a [Azure Portal](#). En el panel izquierdo, seleccione **Azure Active Directory**.
- Seleccione **External Identities**.
- Seleccione **Todos los proveedores de identidades**.
- Seleccione el proveedor de identidades y, a continuación, seleccione **Eliminar**.
- Seleccione **Sí** para confirmar la eliminación.

Para quitar una federación directa con un proveedor de identidades mediante PowerShell:

- Instale la versión más reciente de Azure AD PowerShell para el módulo Graph ([AzureADPreview](#)).
- Ejecute el siguiente comando:

```
Connect-AzureAD
```

- En el símbolo del sistema, inicie sesión con la cuenta de administrador global administrada.
- Escriba el comando siguiente:

```
Remove-AzureADEExternalDomainFederation -ExternalDomainName $domainName
```

Pasos siguientes

Obtenga más información sobre la [experiencia de canje de invitación](#) cuando los usuarios externos inician sesión con varios proveedores de identidades.

Ejemplo: Federación directa con Servicios de federación de Active Directory (AD FS) (versión preliminar)

18/02/2021 • 13 minutes to read • [Edit Online](#)

NOTE

La federación directa es una característica en versión preliminar pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

En este artículo se describe cómo configurar la [federación directa](#) con los Servicios de federación de Active Directory (AD FS) como proveedor de identidades de SAML 2.0 o WS-Fed. Para admitir la federación directa, deben ser configurados ciertos atributos y notificaciones en el proveedor de identidades. Para ilustrar cómo configurar un proveedor de identidades para la federación directa, usaremos los Servicios de federación de Active Directory (AD FS) como ejemplo. Le mostraremos cómo configurar AD FS como proveedor de identidades de SAML y como un proveedor de identidades de WS-Fed.

NOTE

En este artículo se describe cómo configurar AD FS para SAML y WS-Fed con fines meramente ilustrativos. Para las integraciones de federación directa en las que el proveedor de identidades es AD FS, se recomienda utilizar WS-Fed como protocolo.

Configuración de AD FS para la federación directa de SAML 2.0

Azure AD B2B se puede configurar para federarse con proveedores de identidades que usan el protocolo SAML con los requisitos específicos que se indican a continuación. Para ilustrar los pasos de configuración de SAML, esta sección muestra cómo configurar AD FS para SAML 2.0.

Para establecer una federación directa, se deben recibir los siguientes atributos en la respuesta de SAML 2.0 del proveedor de identidades. Estos atributos se pueden configurar mediante la vinculación con el archivo XML del servicio de token de seguridad en línea o la introducción manual. En el paso 12 de [Create a test AD FS instance](#) (Creación de una instancia de AD FS de prueba) se describe cómo buscar los puntos de conexión de AD FS o generar la dirección URL de metadatos, por ejemplo

`https://fs.iga.azure-test.net/federationmetadata/2007-06/federationmetadata.xml`.

ATRIBUTO	VALUE
AssertionConsumerService	<code>https://login.microsoftonline.com/login.srf</code>
Público	<code>urn:federation:MicrosoftOnline</code>
Emisor	El URI del emisor del asociado IdP, por ejemplo <code>http://www.example.com/exk1016w90DHM0y1...</code>

Las siguientes notificaciones deben configurarse en el token SAML 2.0 emitido por el proveedor de identidades:

ATRIBUTO	VALUE
Formato de NameID	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
emailaddress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddre

En la sección siguiente se muestra cómo configurar los atributos y las notificaciones necesarios mediante AD FS como un ejemplo de un proveedor de identidades de SAML 2.0.

Antes de empezar

Antes de iniciar este procedimiento, se debe configurar y poner en funcionamiento el servidor AD FS. Para obtener ayuda sobre la configuración de un servidor AD FS, consulte [Create a test AD FS 3.0 instance on an Azure virtual machine](#) (Creación de una instancia de prueba de AD FS 3.0 en una máquina virtual de Azure).

Adición de la descripción de notificación

1. En el servidor de AD FS, seleccione **Herramientas > Administración de AD FS**.
2. En el panel de navegación, seleccione **Servicio > Descripciones de notificaciones**.
3. En **Acciones**, seleccione **Agregar descripción de notificación**.
4. En la ventana **Agregar descripción de notificación**, especifique los valores siguientes:
 - **Nombre para mostrar:** Identificador persistente
 - **Identificador de notificación:** urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
 - Active la casilla **Publicar esta descripción de notificación en los metadatos de federación como un tipo de notificación que este Servicio de federación pueda aceptar.**
 - Active la casilla **Publicar esta descripción de notificación en los metadatos de federación como un tipo de notificación que este Servicio de federación pueda enviar.**
5. Haga clic en **Aceptar**.

Adición de las reglas de notificación y de la veracidad de usuarios de confianza

1. En el servidor de AD FS, vaya a **Herramientas > Administración de AD FS**.
2. En el panel de navegación, seleccione **Relaciones de confianza > Veracidades de usuarios de confianza**.
3. En **Acciones**, seleccione **Agregar veracidad del usuario de confianza**.
4. En el Asistente para agregar veracidad del usuario de confianza para **Seleccionar origen de datos**, utilice la opción **Importar los datos sobre el usuario de confianza publicado en línea o en una red local**. Especifique la dirección URL de metadatos de federación <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>. Deje las otras selecciones predeterminadas. Seleccione **Cerrar**.
5. Se abre el asistente **Editar reglas de notificación**.
6. En el asistente **Editar reglas de notificación**, seleccione **Agregar regla**. En **Elegir tipo de regla**, seleccione **Enviar atributos LDAP como notificaciones**. Seleccione **Next (Siguiente)**.
7. En **Configurar regla de notificación**, especifique los siguientes valores:
 - **Nombre de la regla de notificación:** Regla de notificación de correo electrónico
 - **Almacén de atributos:** Active Directory
 - **Atributo LDAP Direcciones de correo electrónico**
 - **Tipo de notificación saliente:** Dirección de correo electrónico
8. Seleccione **Finalizar**.

9. La ventana **Editar reglas de notificación** mostrará la nueva regla. Haga clic en **Aplicar**.

10. Haga clic en **Aceptar**.

Creación de una regla de transformación de correo electrónico

1. Vaya a **Editar reglas de notificación** y haga clic en **Agregar regla**. En **Elegir tipo de regla**, seleccione **Transformar una notificación entrante** y haga clic en **Siguiente**.

2. En **Configurar regla de notificación**, especifique los siguientes valores:

- **Nombre de la regla de notificación**: Regla de transformación de correo electrónico
- **Tipo de notificación entrante**: Dirección de correo electrónico
- **Tipo de notificación saliente**: Identificador de nombre
- **Formato de id. de nombre saliente**: Identificador persistente
- Seleccione **Pasar a través todos los valores de notificaciones**.

3. Haga clic en **Finalizar**

4. La ventana **Editar reglas de notificación** mostrará las nuevas reglas. Haga clic en **Aplicar**.

5. Haga clic en **OK**. El servidor de AD FS ahora está configurado para la federación directa mediante el protocolo SAML 2.0.

Configuración de AD FS para la federación directa de WS-Fed

Azure AD B2B puede configurarse para federar con proveedores de identidades que usan el protocolo WS-Fed con los requisitos específicos que se enumeran a continuación. Actualmente, los dos proveedores de WS-Fed se han probado para determinar su compatibilidad con Azure AD e incluyen AD FS y Shibboleth. En este caso, utilizaremos los Servicios de federación de Active Directory (AD FS) como ejemplo del proveedor de identidades de WS-Fed. Para más información sobre cómo establecer la veracidad de un usuario de confianza entre un proveedor compatible con WS-Fed y Azure AD, descargue los documentos de compatibilidad del proveedor de identidades de Azure AD.

Para configurar una federación directa, se deben recibir los siguientes atributos en el mensaje de WS-Fed del proveedor de identidades. Estos atributos se pueden configurar mediante la vinculación con el archivo XML del servicio de token de seguridad en línea o la introducción manual. En el paso 12 de [Create a test AD FS instance](#) (Creación de una instancia de AD FS de prueba) se describe cómo buscar los puntos de conexión de AD FS o generar la dirección URL de metadatos, por ejemplo

`https://fs.iga.azure-test.net/federationmetadata/2007-06/federationmetadata.xml` .

ATRIBUTO	VALUE
PassiveRequestorEndpoint	<code>https://login.microsoftonline.com/login.srf</code>
Público	<code>urn:federation:MicrosoftOnline</code>
Emisor	El URI del emisor del asociado IdP, por ejemplo <code>http://www.example.com/exk1016w90DHM0y1...</code>

Las notificaciones necesarias para el token de WS-Fed emitido por el proveedor de identidades:

ATRIBUTO	VALUE
ImmutableID	<code>http://schemas.microsoft.com/LiveID/Federation/2008/05/Immutable</code>
emailaddress	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddre</code>

En la sección siguiente se muestra cómo configurar los atributos y las notificaciones necesarios mediante AD FS

como un ejemplo de un proveedor de identidades de WS-Fed.

Antes de empezar

Antes de iniciar este procedimiento, se debe configurar y poner en funcionamiento el servidor AD FS. Para obtener ayuda sobre la configuración de un servidor AD FS, consulte [Create a test AD FS 3.0 instance on an Azure virtual machine](#) (Creación de una instancia de prueba de AD FS 3.0 en una máquina virtual de Azure).

Adición de las reglas de notificación y de la veracidad de usuarios de confianza

1. En el servidor de AD FS, vaya a **Herramientas > Administración de AD FS**.
2. En el panel de navegación, seleccione **Relaciones de confianza > Veracidades de usuarios de confianza**.
3. En **Acciones**, seleccione **Agregar veracidad del usuario de confianza**.
4. En el Asistente para agregar veracidad del usuario de confianza para **Seleccionar origen de datos**, utilice la opción **Importar los datos sobre el usuario de confianza publicado en línea o en una red local**. Especifique la dirección URL de metadatos de federación
`https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml`. Deje las otras selecciones predeterminadas. Seleccione **Cerrar**.
5. Se abre el asistente **Editar reglas de notificación**.
6. En el asistente **Editar reglas de notificación**, seleccione **Agregar regla**. En **Elegir tipo de regla**, seleccione **Enviar notificaciones con una regla personalizada**. Seleccione **Next (Siguiente)**.
7. En **Configurar regla de notificación**, especifique los siguientes valores:
 - **Nombre de la regla de notificación**: Identificador inmutable del problema
 - **Regla personalizada**:
`c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
issue(store = "Active Directory", types =
("http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query = "samAccountName=
{0};objectGUID;{1}", param = regexreplace(c.Value, "(?<domain>[^\\]+)\\((?<user>.+)${user})",
param = c.Value);`
8. Seleccione **Finalizar**.
9. La ventana **Editar reglas de notificación** mostrará la nueva regla. Haga clic en **Aplicar**.
10. En el mismo asistente **Editar reglas de notificación**, seleccione **Agregar regla**. En **Elegir tipo de regla**, seleccione **Enviar atributos LDAP como notificaciones**. Seleccione **Next (Siguiente)**.
11. En **Configurar regla de notificación**, especifique los siguientes valores:
 - **Nombre de la regla de notificación**: Regla de notificación de correo electrónico
 - **Almacén de atributos**: Active Directory
 - **Atributo LDAP**: Direcciones de correo electrónico
 - **Tipo de notificación saliente**: Dirección de correo electrónico
12. Seleccione **Finalizar**.
13. La ventana **Editar reglas de notificación** mostrará la nueva regla. Haga clic en **Aplicar**.
14. Haga clic en **OK**. El servidor de AD FS ahora está configurado para la federación directa mediante WS-Fed.

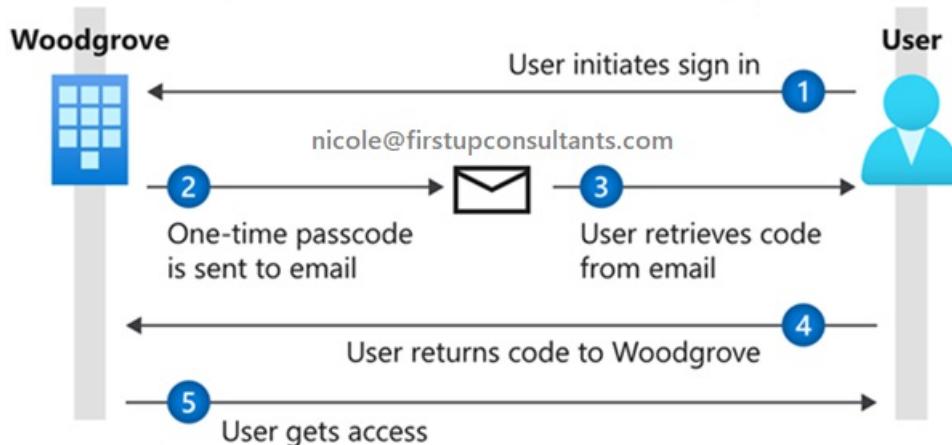
Pasos siguientes

A continuación, va a [configurar la federación directa en Azure AD](#) bien en el portal de Azure AD o con PowerShell.

Autenticación con código de acceso de un solo uso por correo electrónico

18/02/2021 • 12 minutes to read • [Edit Online](#)

En este artículo se describe cómo habilitar la autenticación con código de acceso de un solo uso por correo electrónico para usuarios invitados de B2B. La característica de código de acceso de un solo uso por correo electrónico autentica los usuarios invitados de B2B cuando no pueden autenticarse por otros medios, como Azure AD, una cuenta de Microsoft (MSA) o la federación de Google. Con la autenticación por código de acceso de un solo uso, no hay necesidad de crear una cuenta de Microsoft. Cuando el usuario invitado canjea una invitación o accede a un recurso compartido, puede solicitar un código temporal, que se envía a su dirección de correo electrónico. A continuación, escribe este código para continuar con el inicio de sesión.



IMPORTANT

A partir de marzo de 2021, la característica de código de acceso de un solo uso por correo electrónico se activará para todos los inquilinos existentes, y se habilitará de forma predeterminada para los nuevos. Si no desea permitir que esta característica se active automáticamente, puede deshabilitarla. Consulte [Deshabilitación del código de acceso de un solo uso por correo electrónico](#) más adelante.

NOTE

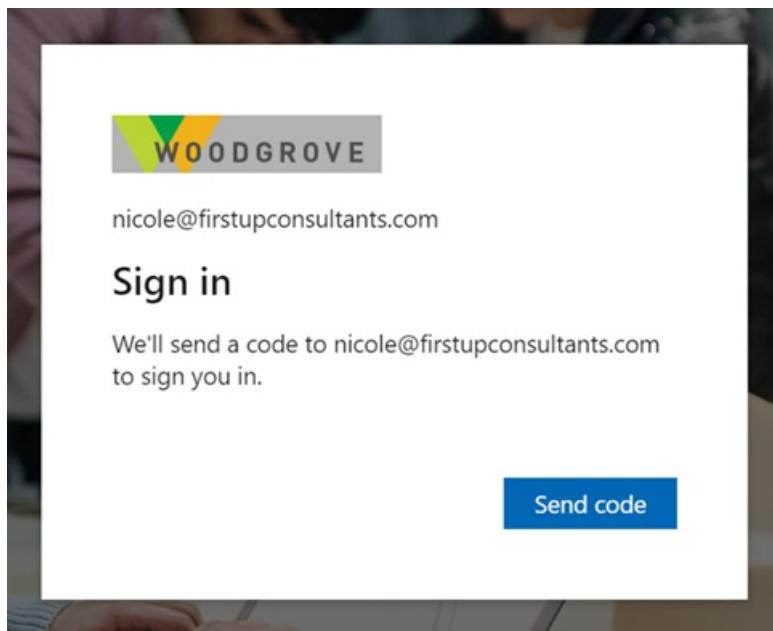
Los usuarios con código de acceso de un solo uso deben iniciar sesión con un vínculo que incluya el contexto del inquilino (por ejemplo, https://myapps.microsoft.com/?tenantid=<tenant_id> o https://portal.azure.com/<tenant_id>, o en el caso de un dominio verificado, <https://myapps.microsoft.com/<verified domain>.onmicrosoft.com>). Los vínculos directos a aplicaciones y los recursos también funcionan siempre que incluyan el contexto del inquilino. Actualmente, los usuarios invitados no pueden iniciar sesión con puntos de conexión sin contexto de inquilino. Por ejemplo, si se usan <https://myapps.microsoft.com>, <https://portal.azure.com>, se producirá un error.

Experiencia de usuario para los usuarios invitados de código de acceso de un solo uso

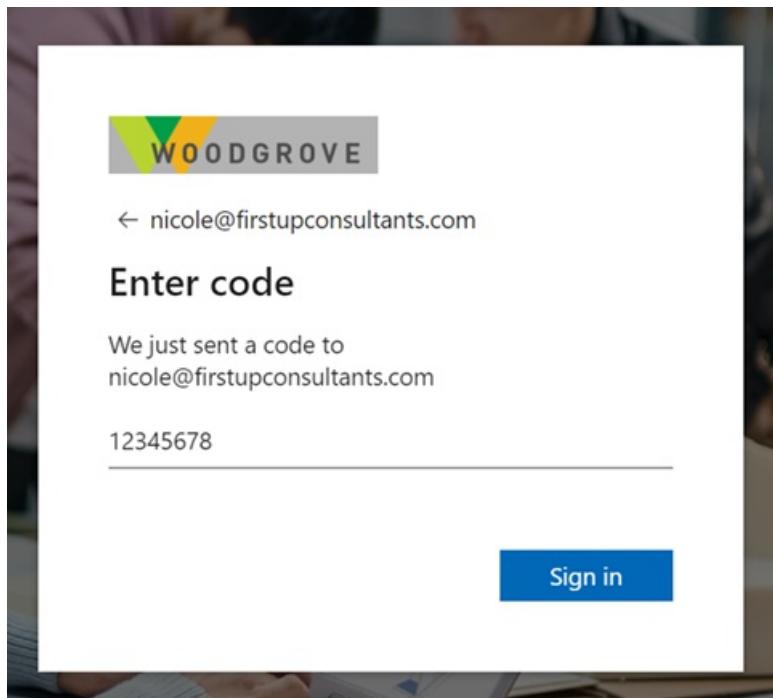
Cuando la característica de código de acceso de un solo uso por correo electrónico está habilitada, los usuarios nuevos invitados [que cumplan ciertas condiciones](#) usarán la autenticación con código de acceso de un solo uso.

Los usuarios invitados que canjearon una invitación antes de la habilitación del código de acceso de un solo uso por correo electrónico seguirán usando su mismo método de autenticación.

Con la autenticación de código de acceso de un solo uso, el usuario invitado puede canjear su invitación haciendo clic en un vínculo directo o mediante el correo electrónico de invitación. En cualquier caso, un mensaje en el explorador indica que se enviará un código a la dirección de correo electrónico del usuario invitado. El usuario invitado selecciona **Enviar código**:



Se envía un código de acceso a la dirección de correo electrónico del usuario. El usuario recupera el código de acceso del correo electrónico y lo escribe en la ventana del explorador:



Ahora el usuario invitado se ha autenticado y puede ver el recurso compartido o continuar con el inicio de sesión.

NOTE

Los códigos de acceso de un solo uso son válidos durante 30 minutos. Después de 30 minutos, ese código de acceso de un solo uso específico ya no será válido y el usuario deberá solicitar uno nuevo. Las sesiones del usuario expiran después de 24 horas. Después de ese tiempo, el usuario invitado recibe un nuevo código de acceso cuando accede al recurso. La expiración de la sesión proporciona mayor seguridad, en especial cuando un usuario invitado deja su empresa o ya no necesita tener acceso.

¿Cuándo un usuario invitado obtiene un código de acceso de un solo uso?

Cuando un usuario invitado canjea una invitación o usa un vínculo a un recurso que se ha compartido con él, recibe un código de acceso de un solo uso si:

- No tiene una cuenta de Azure AD
- No tiene una cuenta de Microsoft
- El inquilino que invita no ha configurado la federación de Google para los usuarios @gmail.com y @googlemail.com

En el momento de la invitación, no hay ninguna indicación de que el usuario al que está invitando usará la autenticación de código de acceso de un solo uso. Pero cuando el usuario invitado inicia sesión, la autenticación de código de acceso de un solo uso será el método de reserva si no se puede usar ningún otro método de autenticación.

Para saber si un usuario invitado se autentica mediante códigos de acceso de un solo uso, compruebe la propiedad **Source** en los detalles del usuario. En el Azure Portal, vaya a **Azure Active Directory > Usuarios** y, a continuación, seleccione el usuario para abrir la página de detalles.

The screenshot shows the Azure Active Directory User Details page for a user named Nicole Wagner. At the top, there is a profile picture placeholder with the letters 'NW'. Below it, the user's name 'Nicole Wagner' and email 'nicole@firstupconsultants.com' are displayed. A summary card shows 'User Sign-ins' (4) and 'Group memberships' (0). A timeline bar indicates activity in November. The 'Identity' section contains the following details:

Name Nicole Wagner	First name Nicole	Last name Wagner
User Principal Name nicole@firstupconsultants...	User type Guest	Invitation accepted Yes
Object ID 000005c2-0009-03...	Source OTP	

NOTE

Cuando un usuario canjea un código de acceso de un solo uso y más adelante obtiene una MSA, una cuenta de Azure AD u otra cuenta federada, seguirá autenticándose con un código de acceso de un solo uso. Si quiere actualizar el método de autenticación, puede eliminar la cuenta de usuario invitado y volver a invitarlo.

Ejemplo

Se invita al usuario invitado teri@gmail.com a Fabrikam, que no tiene configurada la federación de Google. Teri no tiene una cuenta de Microsoft. Recibe un código de acceso de un solo uso para la autenticación.

Deshabilitación del código de acceso de un solo uso por correo electrónico

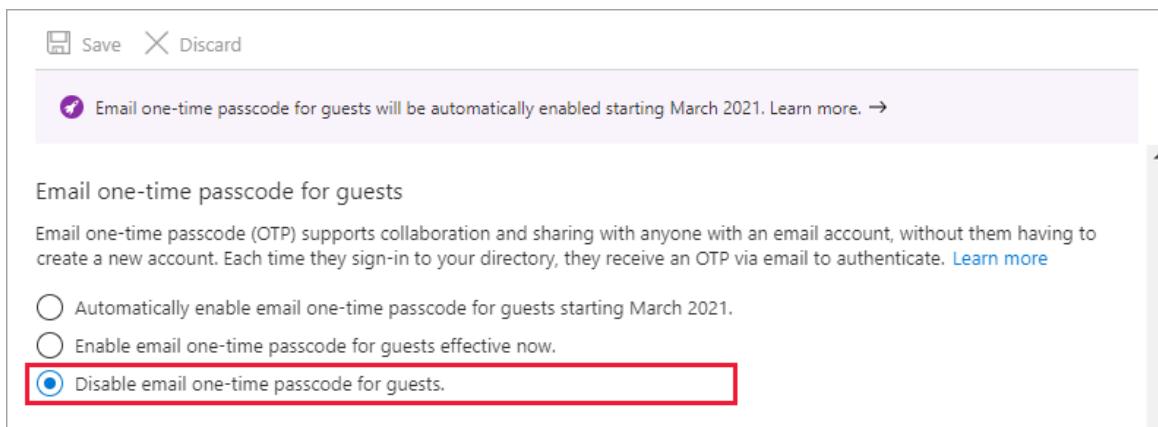
A partir de marzo de 2021, la característica de código de acceso de un solo uso por correo electrónico se activará para todos los inquilinos existentes, y se habilitará de forma predeterminada para los nuevos. En ese momento, Microsoft dejará de admitir el canje de invitaciones mediante la creación de inquilinos y cuentas de Azure AD no administradas ("virales" o "Just-In-Time") para escenarios de colaboración B2B. Vamos a habilitar la característica de código de acceso de un solo uso por correo electrónico, ya que proporciona un método eficaz de autenticación de reserva para usuarios invitados. No obstante, puede deshabilitar esta característica si prefiere no utilizarla.

NOTE

Si la característica de código de acceso de un solo uso por correo electrónico se ha habilitado en el inquilino y la desactiva, los usuarios invitados que hayan canjeado un código de acceso de un solo uso no podrán iniciar sesión. Puede eliminar los usuarios invitados y volver a invitarlos para que puedan volver a iniciar sesión con otro método de autenticación.

Para deshabilitar la característica de código de acceso de un solo uso por correo electrónico

1. Inicie sesión en [Azure Portal](#) como administrador global de Azure AD.
2. En el panel de navegación, seleccione **Azure Active Directory**.
3. Seleccione **External Identities > Configuración de colaboración externa**.
4. En **Email one-time passcode for guests** (Código de acceso de un solo uso por correo electrónico para invitados), seleccione **Disable email one-time passcode for guests** (Deshabilitar el código de acceso de un solo uso por correo electrónico para invitados).



NOTE

Si ve el siguiente botón en lugar de las opciones mostradas anteriormente, significa que ya se le ha habilitado, deshabilitado o ha participado en la versión preliminar de la característica. Seleccione **No** para deshabilitar esta característica.

[Email one-time passcode for guests](#) ⓘ

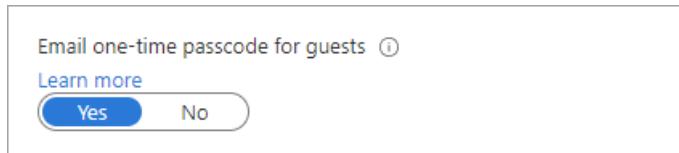
[Learn more](#)

[Yes](#) [No](#)

5. Seleccione Guardar.

Nota para los clientes de la versión preliminar pública

Si previamente ha participado en la versión preliminar pública del código de acceso de un solo uso por correo electrónico, la fecha de habilitación automática de las características en marzo de 2021 no es aplicable a su caso, por lo que sus procesos empresariales relacionados no se verán afectados. Además, en Azure Portal, en las propiedades de **Email one-time passcode for guests** (Código de acceso de un solo uso por correo electrónico para invitados), no verá la opción **Automatically enable email one-time passcode for guests in March 2021** (Habilitar automáticamente el código de acceso de un solo uso por correo electrónico para invitados a partir de marzo de 2021). En su lugar, verá el botón **Yes/No** (Sí/No):



Sin embargo, si prefiere no participar en la característica y permitir que se habilite automáticamente en marzo de 2021, puede revertir a la configuración predeterminada mediante el [tipo de recurso de configuración del método de autenticación por correo electrónico](#) de Microsoft Graph API. Después de revertir a la configuración predeterminada, las siguientes opciones estarán disponibles en **Email one-time passcode for guests** (Código de acceso de un solo uso por correo electrónico para invitados):

- **Automatically enable email one-time passcode for guests in March 2021** (Habilitar automáticamente el código de acceso de un solo uso por correo electrónico a partir de marzo de 2021). Valor predeterminado. Si la característica de código de acceso de un solo uso por correo electrónico no está habilitada para el inquilino, se activará automáticamente en marzo de 2021. Si desea que la característica se habilite desde ese momento, no tiene que hacer nada más. Si ya ha habilitado o deshabilitado la característica, esta opción no estará disponible.
- **Enable email one-time passcode for guests effective now** (Habilitar el código de acceso de un solo uso por correo electrónico para invitados desde este momento). Activa la característica de código de acceso de un solo uso por correo electrónico para el inquilino.
- **Disable email one-time passcode for guests** (Deshabilitar el código de acceso de un solo uso por correo electrónico para invitados). Desactiva la característica de código de acceso de un solo uso por correo electrónico para el inquilino y evita que la característica se active en marzo de 2021.

Incorporación de un flujo de usuario de registro de autoservicio a una aplicación (versión preliminar)

18/02/2021 • 9 minutes to read • [Edit Online](#)

NOTE

El registro de autoservicio es la característica en versión preliminar pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

Puede crear flujos de usuario para aplicaciones compiladas por la organización. La asociación del flujo de usuario con una aplicación le permite habilitar el registro en esa aplicación. Puede optar por asociar más de una aplicación al flujo de usuario. Una vez asociado el flujo de usuario a una o más aplicaciones, los usuarios que visiten esa aplicación podrán registrarse y obtener una cuenta de invitado mediante las opciones configuradas en el flujo de usuario.

NOTE

Puede asociar flujos de usuarios a las aplicaciones compiladas por la organización. Los flujos de usuario no se pueden usar para las aplicaciones de Microsoft, como SharePoint o Teams.

Antes de empezar

Adición de proveedores de identidades sociales (opcional)

Azure AD es el proveedor de identidades predeterminado para el registro de autoservicio. Esto significa que los usuarios pueden registrarse de manera predeterminada con una cuenta de Azure AD. Los proveedores de identidades sociales también pueden incluirse en estos flujos de registro para admitir cuentas de Google y Facebook.

- [Incorporación de Facebook a la lista de proveedores de identidades sociales](#)
- [Incorporación de Google a la lista de proveedores de identidades sociales](#)

NOTE

En la versión preliminar, si un flujo de usuario de registro de autoservicio se asocia a una aplicación y le envía a un usuario una invitación a esa aplicación, el usuario no podrá utilizar una cuenta de Gmail para canjear la invitación. Como solución alternativa, el usuario puede pasar por el proceso de registro de autoservicio. O bien, para canjear la invitación, puede acceder a otra aplicación o usar el portal Mis aplicaciones en <https://myapps.microsoft.com>.

Definición de atributos personalizados (opcional)

Los atributos de usuario son valores recopilados del usuario durante el registro de autoservicio. Azure AD incluye un conjunto de atributos integrado, pero puede crear atributos personalizados para utilizar en el flujo de usuario. También puede leer y escribir estos atributos mediante Microsoft Graph API. Consulte [Definición de atributos personalizados para flujos de usuario](#).

Habilitación del registro de autoservicio para el inquilino

Para poder agregar un flujo de usuario de registro de autoservicio a las aplicaciones, debe habilitar la característica para el inquilino. Cuando se haya habilitado, los controles estarán disponibles en el flujo de usuario, lo que le permite asociar el flujo de usuario con una aplicación.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. Seleccione **Configuración de usuario** y, a continuación, en **Usuarios externos**, seleccione **Administrar la configuración de colaboración externa**.
4. Establezca la alternancia **Habilitación del registro de invitados de autoservicio mediante flujos de usuario (versión preliminar)** en Sí.

The screenshot shows the 'External collaboration settings' page in the Azure portal. It includes sections for guest permissions, invitation roles, and collaboration restrictions. A specific section, 'Enable guest self-service sign up via user flows (Preview)', is highlighted with a red box.

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

Enable Email One-Time Passcode for guests (Preview) ⓘ
[Learn more](#)
Yes No

Enable guest self-service sign up via user flows (Preview) ⓘ
[Learn more](#)
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)

5. Seleccione **Guardar**.

Creación del flujo de usuario para el registro de autoservicio

A continuación, debe crear el flujo de usuario para el registro de autoservicio y agregarlo a una aplicación.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **Flujos de usuario (versión preliminar)** y, a continuación, seleccione **Nuevo flujo de**

usuario.

The screenshot shows the 'External Identities | User flows (Preview)' page in the Azure portal. On the left, there's a sidebar with links like 'Get started', 'All identity providers', 'External collaboration settings', 'Diagnose and solve problems', 'Self-service sign up', 'Custom user attributes (Preview)', and 'User flows (Preview)', which is currently selected and highlighted with a grey background. At the top right, there's a 'New user flow' button with a plus sign, which is also highlighted with a red box. Below it, there's a search bar for 'User flow name' and a section for 'Name' with the placeholder 'Search using user flow name'. A message 'No user flows found' is displayed at the bottom of this section.

5. En la página **Crear**, escriba un **Nombre** para el flujo de usuario. Tenga en cuenta que el nombre incluye automáticamente el prefijo **B2X_1_**.
6. En la lista **Proveedores de identidades**, seleccione uno o varios proveedores de identidades que los usuarios externos puedan usar para iniciar sesión en la aplicación. La opción **Registro en Azure Active Directory** se selecciona de manera predeterminada. (Consulte la sección [Antes de empezar](#) que aparece más arriba en este artículo para obtener información sobre cómo agregar proveedores de identidades).
7. En **Atributos de usuario**, elija los atributos que quiere recopilar del usuario. En el caso de los atributos adicionales, seleccione **Mostrar más**. Por ejemplo, seleccione **Mostrar más** y elija los atributos y las通知iones de **País o región**, **Nombre para mostrar** y **Código postal**. Seleccione **Aceptar**.

Create

Sign up and sign in

[← Select a different type of user flow](#)

Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.

1. Name *

The unique string used to identify this user flow in requests to Azure AD. This cannot be changed after a user flow has been created.

B2X_1_* contoso-sign-up

2. Identity providers *

Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you can add more in the Identity providers section for your directory. [Learn more about identity providers](#).

Please select at least one identity provider

- Azure Active Directory Sign up
- Google
- Facebook

3. User attributes

User attributes are values collected on sign up. You can create custom attributes for use in your directory. [Learn more about user attributes](#).

Collect attribute

- | | |
|----------------|-------------------------------------|
| Given Name | <input checked="" type="checkbox"/> |
| Surname | <input checked="" type="checkbox"/> |
| City | <input checked="" type="checkbox"/> |
| Country/Region | <input checked="" type="checkbox"/> |
| Display Name | <input checked="" type="checkbox"/> |

[Show more...](#)**Create****NOTE**

Solo puede recopilar atributos cuando un usuario se registra por primera vez. Una vez que un usuario se registra, ya no se le pedirá que recopile información de atributos, aunque cambie el flujo de usuario.

8. Seleccione **Crear**.

9. El nuevo flujo de usuario aparece en la lista **Flujos de usuario (versión preliminar)**. Si es necesario, actualice la página.

Selección del diseño del formulario de colección de atributos

Puede elegir el orden en que se muestran los atributos en la página de registro.

1. En [Azure Portal](#), seleccione Azure Active Directory.
2. Seleccione External Identities y, después, Flujos de usuario (versión preliminar) .
3. Seleccione el flujo de usuario de registro de autoservicio de la lista.
4. En Personalizar, seleccione Diseños de página.
5. Aparecen los atributos que eligió recopilar. Para cambiar el orden de visualización, seleccione un atributo y, a continuación, seleccione Subir, Bajar, Mover a la parte superior o Mover a la parte inferior.
6. Seleccione Guardar.

Incorporación de aplicaciones al flujo de usuario de registro de autoservicio

Ya puede asociar aplicaciones al flujo de usuario.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En [Servicios de Azure](#), seleccione Azure Active Directory.
3. En el menú de la izquierda, seleccione External Identities.
4. En Registro de autoservicio, seleccione Flujos de usuario (versión preliminar) .
5. Seleccione el flujo de usuario de registro de autoservicio de la lista.
6. En el menú de la izquierda, en Usar, seleccione Aplicaciones.
7. Seleccione Agregar una aplicación.

The screenshot shows the Azure portal interface for managing user flows. The top navigation bar includes Home, Contoso, External Identities | User flows (Preview), B2X_1_contoso-sign-up, and Applications. The main title is 'B2X_1_contoso-sign-up | Applications'. Below the title, there's a sub-header 'Sign up and sign in'. On the left, a sidebar lists several sections: Overview, Settings, Identity providers, User attributes, Customize, Page layouts, Languages, Use, and Applications. The 'Applications' section is currently selected. At the top right, there's a search bar labeled 'Search (Ctrl+/' followed by a '«' icon. To the right of the search bar is a button with a plus sign and the text 'Add application', which is highlighted with a red box. The main content area contains a message: 'Associating your user flow with an application allows you to enable sign up on that app. You sign up using the options configured in the user flow.' It also includes a 'Display name' field and a note stating 'This user flow is not assigned to any applications'.

8. Seleccione la aplicación de la lista. O bien, use el cuadro de búsqueda para encontrar la aplicación y, a continuación, selecciónela.
9. Haga clic en Seleccionar.

Pasos siguientes

- [Incorporación de Google a la lista de proveedores de identidades sociales](#)
- [Incorporación de Facebook a la lista de proveedores de identidades sociales](#)
- [Uso de conectores de API para personalizar y extender los flujos de usuario a través de las API web](#)

- Incorporación de un flujo de trabajo de aprobación personalizado al flujo del usuario

Definición de atributos personalizados para flujos de usuario (versión preliminar)

18/02/2021 • 4 minutes to read • [Edit Online](#)

NOTE

La característica de atributos de usuario personalizados es una característica en vista previa pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

Para cada aplicación, puede tener requisitos diferentes para la información que quiere recopilar durante el registro. El inquilino de Azure AD incluye un conjunto integrado de información almacenada en atributos, como el nombre propio, los apellidos, la ciudad y el código postal. Con Azure AD, puede extender el conjunto de atributos almacenados en una cuenta de invitado cuando el usuario externo se registre a través de un flujo de usuario.

Puede crear atributos personalizados en Azure Portal y usarlos en los flujos de usuario de registro de autoservicio. También puede leer y escribir estos atributos mediante [Microsoft Graph API](#). Microsoft Graph API admite la creación y actualización de un usuario con atributos de extensión. Los atributos de extensión en Graph API se denominan mediante la convención `extension_<extensions-app-id>_attributename`. Por ejemplo:

```
"extension_831374b3bd5041bfaa54263ec9e050fc_loyaltyNumber": "212342"
```

`<extensions-app-id>` es específico del inquilino. Para hallar este identificador, vaya a Azure Active Directory > Registros de aplicaciones > Ver todas las aplicaciones. Busque la aplicación que comienza por "aad-extensions-app" y selecciónela. En la página Información general de la aplicación, anote el valor que aparece en Id. de aplicación (cliente).

Creación de un atributo personalizado

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **Atributos de usuario personalizados (versión preliminar)**. Se muestran los atributos de usuario disponibles.

External Identities Custom user attributes (Preview)				
Contoso - Azure Active Directory				
<input type="text" value="Search (Ctrl+ /)"/> <>		+ Add		
Get started		Name	Data Type	Description
All identity providers		City	String	The city in which the user is located.
External collaboration settings		Country/Region	String	The country/region in which the user is located.
Diagnose and solve problems		CustomAttribute	String	
Self-service sign up		Customattribute1	String	This is a custom attribute.
Custom user attributes (Preview)		Display Name	String	
User flows (Preview)		enrichedClaim	String	
Lifecycle management		Given Name	String	The user's given name (also known as first name).
Terms of use		Identity Provider	String	
Access reviews		Job Title	String	The user's job title.
Troubleshooting + Support		Postal Code	String	The postal code of the user's address.
		State/Province	String	The state or province in user's address

5. Para agregar un atributo, seleccione **Agregar**.

6. En el panel **Agregar un atributo**, escriba los valores siguientes:

- **Nombre**: proporcione un nombre para el atributo personalizado (por ejemplo, "ShoeSize").
- **Tipo de datos**: elija un tipo de datos (**Cadena** , **Booleano** o **Int**).
- **Descripción**: también puede escribir una descripción del atributo personalizado para uso interno. Esta descripción no es visible para el usuario.

Add an attribute □ X

Name ⓘ	<input type="text" value="ShoeSize"/> ✓
Data Type ⓘ	<input type="text" value="String"/> ▾
Description ⓘ	The user's shoe size
<input type="button" value="Create"/>	

7. Seleccione **Crear**.

El atributo personalizado ya está disponible en la lista de atributos de usuario y puede usarlo en los flujos de usuario. Solo se crea la primera vez que se utiliza en cualquier flujo de usuario y no cuando se agrega a la lista de atributos de usuario.

Después de crear un usuario mediante un flujo de usuario que usa el atributo personalizado recién creado, el objeto se puede consultar en el [Explorador de Microsoft Graph](#). Ahora debe ver **ShoeSize** en la lista de atributos que se recopilan durante el viaje de suscripción en el objeto de usuario. Puede llamar a Graph API desde la aplicación para obtener los datos de este atributo una vez que se agregue al objeto de usuario.

Pasos siguientes

[Incorporación de un flujo de usuario de registro de autoservicio a una aplicación](#)

Personalización de idioma en Azure Active Directory (versión preliminar)

18/02/2021 • 9 minutes to read • [Edit Online](#)

NOTE

El registro de autoservicio es la característica en versión preliminar pública de Azure Active Directory. Para más información sobre las versiones preliminares, consulte [Términos de uso complementarios de las versiones preliminares de Microsoft Azure](#).

La personalización de idioma en Azure Active Directory (Azure AD) permite que el flujo de usuario albergue distintos idiomas a fin de satisfacer las necesidades del usuario. Microsoft proporciona las traducciones de [36 idiomas](#). Incluso si su experiencia se proporciona únicamente para un idioma, puede personalizar los nombres de atributos en la página de la colección de atributos.

¿Cómo funciona la personalización de idioma?

De manera predeterminada, la personalización de idioma está habilitada para que los usuarios se registren a fin de garantizar una experiencia de registro coherente. Puede usar idiomas para modificar las cadenas que se muestran a los usuarios como parte del proceso de la colección de atributos durante el registro.

NOTE

Si va a usar atributos de usuario personalizados, debe proporcionar sus propias traducciones. Para más información, consulte [Personalización de las cadenas](#).

Personalización de las cadenas

La personalización de idioma le permite personalizar cualquier cadena del flujo de usuario.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **Flujos de usuario (versión preliminar)**.
5. Seleccione el flujo de usuario que quiere habilitar para las traducciones.
6. Seleccione **Idiomas**.
7. En la página **Idiomas** del flujo de usuario, seleccione un idioma que desee personalizar.
8. Expanda la página **Colección de atributos**.
9. Seleccione **Descargar valores predeterminados** (o **Descargar invalidaciones** si ha editado anteriormente este idioma).

Estos pasos le proporcionan un archivo JSON que puede usar para comenzar a editar las cadenas.

Cambio de cualquier cadena en la página

1. Abra el archivo JSON descargado según las instrucciones anteriores en un editor JSON.
2. Busque el elemento que desea cambiar. Puede encontrar el valor de `StringId` de la cadena que busca o buscar el atributo `Value` que quiere cambiar.

3. Actualice el atributo `value` con el que quiere que se muestre.
4. Para cada cadena que desea cambiar, cambie `Override` a `true`.
5. Guarde el archivo y cargue los cambios. (Puede encontrar el control de carga en el mismo lugar que donde descargó el archivo JSON).

IMPORTANT

Si necesita reemplazar una cadena, asegúrese de establecer el valor `Override` en `true`. Si no se cambia el valor, se omite la entrada.

Cambio de los atributos de extensión

Si quiere cambiar la cadena de un atributo de usuario personalizado, o quiere agregar una a JSON, debe estar en el siguiente formato:

```
{
  "LocalizedStrings": [
    {
      "ElementType": "ClaimType",
      "ElementId": "extension_<ExtensionAttribute>",
      "StringId": "DisplayName",
      "Override": true,
      "Value": "<ExtensionAttributeValue>"
    }
    [...]
  }
}
```

Reemplace `<ExtensionAttribute>` por el nombre de su atributo de usuario personalizado.

Reemplace `<ExtensionAttributeValue>` por la nueva cadena que se mostrará.

Entrega de una lista de valores mediante LocalizedCollections

Si desea proporcionar una lista establecida de valores para respuestas, debe crear un atributo `LocalizedCollections`. `LocalizedCollections` es una matriz de pares de `Name` y `Value`. El orden de los elementos será el orden en el que se muestran. Para agregar `LocalizedCollections`, utilice el siguiente formato:

```
{
  "LocalizedStrings": [...],
  "LocalizedCollections": [
    {
      "ElementType": "ClaimType",
      "ElementId": "<UserAttribute>",
      "TargetCollection": "Restriction",
      "Override": true,
      "Items": [
        {
          "Name": "<Response1>",
          "Value": "<Value1>"
        },
        {
          "Name": "<Response2>",
          "Value": "<Value2>"
        }
      ]
    }
  ]
}
```

- `ElementId` es el atributo de usuario para el que este atributo `LocalizedCollections` es una respuesta.
- `Name` es el valor que se muestra al usuario.

- `value` es lo que se devuelve en la notificación cuando se selecciona esta opción.

Carga de los cambios

1. Una vez completados los cambios en el archivo JSON, vuelva al inquilino.
2. Seleccione **Flujos de usuario** y haga clic en el flujo de usuario que desea habilitar para las traducciones.
3. Seleccione **Idiomas**.
4. Seleccione el idioma al que quiere traducir.
5. Seleccione la página **Colección de atributos**.
6. Seleccione el ícono de carpeta y el archivo JSON para cargar.

Este cambio se guarda en el flujo de usuario automáticamente.

Información adicional

Etiquetas de personalización de la interfaz de usuario de página como invalidaciones

Cuando se habilita la personalización de idioma, las ediciones anteriores de etiquetas que usan la personalización de la interfaz de usuario de página se almacenan en un archivo JSON para inglés (en). Para seguir cambiando las etiquetas y otras cadenas, cargue los recursos de idioma en Personalización de idioma.

Actualización de traducciones

Microsoft se compromete a proporcionar las traducciones más actualizadas para que haga uso de ellas. Microsoft mejora continuamente las traducciones y garantiza su cumplimiento. Microsoft identificará errores y cambios en la terminología global y creará actualizaciones que funcionen perfectamente en su flujo de usuario.

Compatibilidad con idiomas que se leen de derecha a izquierda

Microsoft no proporciona actualmente compatibilidad con idiomas que se leen de derecha a izquierda. Para ello, puede usar configuraciones regionales personalizadas y CSS para cambiar la manera en la que se muestran las cadenas. Si necesita esta característica, vote por ella en [Comentarios de Azure](#).

Traducciones de proveedores de identidades sociales

Microsoft proporciona el parámetro OIDC `ui_locales` a los inicios de sesión de redes sociales. Pero algunos proveedores de identidades de redes sociales, incluidas Facebook y Google, no los respetan.

Comportamiento del explorador

Tanto Chrome como Firefox solicitan su idioma establecido. Si es un idioma admitido, se muestra antes el valor predeterminado. Microsoft Edge no solicita actualmente un idioma y va directamente al predeterminado.

Idiomas compatibles

Azure AD incluye compatibilidad con los idiomas siguientes. Azure AD proporciona los idiomas de flujo de usuario. [Azure AD MFA](#) proporciona los idiomas de notificación de autenticación multifactor (MFA).

IDIOMA	CÓDIGO DE LENGUAJE	FLUJOS DE USUARIO	NOTIFICACIONES DE MFA
Árabe	ar	✗	✓
Búlgaro	bg	✗	✓
Bengalí	bn	✓	✗
Catalán	ca	✗	✓

IDIOMA	CÓDIGO DE LENGUAJE	FLUJOS DE USUARIO	NOTIFICACIONES DE MFA
Checo	cs	✓	✓
Danés	da	✓	✓
Alemán	de	✓	✓
Griego	el	✓	✓
Inglés	en	✓	✓
Español	es	✓	✓
Estonio	et	✗	✓
Vasco	eu	✗	✓
Finés	fi	✓	✓
Francés	fr	✓	✓
Gallego	gl	✗	✓
Gujarati	gu	✓	✗
Hebreo	he	✗	✓
Hindi	hi	✓	✓
Croata	hr	✓	✓
Húngaro	hu	✓	✓
Indonesio	id	✗	✓
Italiano	it	✓	✓
Japonés	ja	✓	✓
Kazajo	kk	✗	✓
Canarés	kn	✓	✗
Coreano	ko	✓	✓
Lituano	lt	✗	✓
Letón	lv	✗	✓

IDIOMA	CÓDIGO DE LENGUAJE	FLUJOS DE USUARIO	NOTIFICACIONES DE MFA
Malayalam	ml	✓	✗
Maratí	mr	✓	✗
Malayo	ms	✓	✓
Noruego Bokmal	nb	✓	✗
Neerlandés	nl	✓	✓
Noruego	no	✗	✓
Punjabi	pa	✓	✗
Polaco	pl	✓	✓
Portugués (Brasil)	pt-br	✓	✓
Portugués (Portugal)	pt-pt	✓	✓
Rumano	ro	✓	✓
Ruso	ru	✓	✓
Eslavo	sk	✓	✓
Eslovenio	sl	✗	✓
Serbio (cirílico)	sr-cryl-cs	✗	✓
Serbio (latino)	sr-latn-cs	✗	✓
Sueco	sv	✓	✓
Tamil	ta	✓	✗
Telugu	te	✓	✗
Tailandés	th	✓	✓
Turco	tr	✓	✓
Ucraniano	uk	✗	✓
Vietnamita	vi	✗	✓
Chino (simplificado)	zh-hans	✓	✓

IDIOMA	CÓDIGO DE LENGUAJE	FLUJOS DE USUARIO	NOTIFICACIONES DE MFA
Chino (tradicional)	zh-hant	✓	✓

Adición de un conector de API a un flujo de usuario

18/02/2021 • 17 minutes to read • [Edit Online](#)

Para usar un [conector de API](#), primero debe crear el conector de API y, después, habilitarlo en un flujo de usuario.

IMPORTANT

A partir del **4 de enero de 2021**, Google deja [en desuso el soporte de inicio de sesión de WebView](#). Si usa Google Federation o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).

Creación de un conector de API

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **All API connectors (Preview)** (Todos los conectores de API [versión preliminar]) y, después, seleccione **New API connector** (Nuevo conector de API).

The screenshot shows the 'External Identities' section of the Azure Active Directory portal. On the left, there's a sidebar with links like 'Get started', 'All identity providers', 'External collaboration settings', and 'Diagnose and solve problems'. Below that is a 'Self-service sign up' section with 'Custom user attributes (Preview)' and 'All API connectors (Preview)' (which is highlighted with a grey background). The main area has a heading 'External Identities | All API connectors (Preview)' and a sub-section 'Contoso - Azure Active Directory'. It includes a search bar, a 'New API connector' button (which is highlighted with a red box), and a table with columns 'Display name' and 'URL'. A message at the bottom says 'No API connectors found'.

5. Escriba el nombre para mostrar de la llamada. Por ejemplo, **Comprobar el estado de aprobación**.
6. Proporcione el valor de **Dirección URL del punto de conexión** de la llamada API.
7. Indique la información de autenticación de la API.
 - Actualmente solo se admite la autenticación básica. Si desea usar una API sin autenticación básica con fines de desarrollo, solo tiene que escribir un **Nombre de usuario** y una **Contraseña** ficticios que la API pueda omitir. Si se usa con una instancia de Azure Functions y una clave de API, puede incluir el código como un parámetro de consulta en **Dirección URL del punto de conexión** (por ejemplo, <https://contoso.azurewebsites.net/api/endpoint?code=0123456789>).

Configure an API connector

X

 Save  Discard  Remove

Configure an API connector. You can use API connectors within a user flow to send a request to an HTTP endpoint. [Learn more](#)

Display name * ⓘ

API connector 1 

Endpoint URL * ⓘ

<https://userflows.contoso.com/api/endpoint> 

Username * ⓘ

contosouser1 

Password * ⓘ

***** 

8. Seleccione Guardar.

IMPORTANT

Anteriormente, tenía que configurar los atributos de usuario que se enviaban a la API ("Claims to send") y los atributos de usuario que se aceptaban de la API ("Claims to receive"). Ahora, todos los atributos de usuario se envían de forma predeterminada si tienen un valor y la API puede devolver cualquier atributo de usuario en una respuesta de "continuación".

Solicitud enviada a la API

Un conector de API se materializa como una solicitud HTTP POST y envía los atributos de usuario ("claims") como pares de clave y valor en un cuerpo JSON. Los atributos se serializan de forma similar a las propiedades de usuario de [Microsoft Graph](#).

Solicitud de ejemplo

```

POST <API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "identities": [ //Sent for Google and Facebook identity providers
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "givenName": "John",
  "surname": "Smith",
  "jobTitle": "Supplier",
  "streetAddress": "1000 Microsoft Way",
  "city": "Seattle",
  "postalCode": "12345",
  "state": "Washington",
  "country": "United States",
  "extension_<extensions-app-id>_CustomAttribute1": "custom attribute value",
  "extension_<extensions-app-id>_CustomAttribute2": "custom attribute value",
  "ui_locales": "en-US"
}

```

Solo se pueden enviar en la solicitud las propiedades de usuario y los atributos personalizados que se enumeran en la experiencia **Azure Active Directory > Identidades externas > Atributos de usuario personalizados**.

Los atributos personalizados existen en el formato **extension_<extensions-app-id>_AttributeName** en el directorio. La API esperará recibir las notificaciones con este mismo formato serializado. Para más información acerca de los atributos personalizados, consulte cómo [definir atributos personalizados para flujos de autoservicio de registro](#).

Además, en todas las solicitudes se envía de forma predeterminada la notificación de **configuración regional de UI ("ui_locales")**. Proporciona la configuración o configuraciones regionales de un usuario, tal como están definidas en su dispositivo que la API puede utilizar para devolver respuestas internacionalizadas.

IMPORTANT

Si una notificación para enviar no tiene un valor en el momento en que se llama al punto de conexión de la API, la notificación no se enviará a la API. La API debe estar diseñada para comprobar explícitamente el valor que espera.

TIP

La API puede utilizar notificaciones de **identidades ("identities")** y de dirección de correo electrónico ("email") para identificar a un usuario antes de que tenga una cuenta en el inquilino. La notificación "identities" se envía cuando un usuario se autentica con un proveedor de identidades como Google o Facebook. Siempre se envía "email".

Habilitación del conector de API en un flujo de usuario

Siga estos pasos para agregar el conector de API a un flujo de usuario de autoservicio de registro.

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.

3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **Flujos de usuario (versión preliminar)** y, después, seleccione el flujo de usuario para el que desea habilitar el conector de API.
5. Seleccione **Conectores de API** y, después, seleccione los puntos de conexión de API que desea invocar en los pasos siguientes del flujo de usuario:
 - Después de iniciar sesión con un proveedor de identidades
 - Antes de crear el usuario

Choose which, if any, API connector to invoke at a specific step in the user flow. [Learn more](#)

After signing in with an identity provider: API connector 1

Before creating the user: API connector 2

6. Seleccione **Guardar**.

Después de iniciar sesión con un proveedor de identidades

Inmediatamente después de que el usuario se autentique con un proveedor de identidades (Google, Facebook, Azure AD), se invoca un conector de API en este paso del proceso de registro. Este paso precede a la **página de recopilación de atributos**, que es el formulario que se muestra al usuario para recopilar los atributos de usuario.

Solicitud de ejemplo enviada a la API en este paso

```
POST <API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "identities": [ //Sent for Google and Facebook identity providers
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "givenName": "John",
  "lastName": "Smith",
  "ui_locales": "en-US"
}
```

Las notificaciones exactas enviadas a la API dependen de la información proporcionada por el proveedor de identidades. Siempre se envía "email".

Tipos de respuesta esperados de la API web en este paso

Cuando la API web recibe una solicitud HTTP de Azure AD durante un flujo de usuario, puede devolver estas respuestas:

- Respuesta de continuación
- Respuesta de bloqueo

Respuesta de continuación

Una respuesta de continuación indica que el flujo de usuario debe continuar en el paso siguiente: la página de colección de atributos.

En una respuesta de continuación, la API puede devolver notificaciones. Si la API devuelve una notificación, esta realiza lo siguiente:

- Rellena previamente el campo de entrada en la página de colección de atributos.

Vea un ejemplo de una [respuesta de continuación](#).

Respuesta de bloqueo

Una respuesta de bloqueo termina el flujo de usuario. La API puede emitirla intencionadamente para detener el flujo de usuario y mostrar una página de bloqueo al usuario. La página de bloqueo muestra el mensaje

`userMessage` proporcionado por la API.

Vea un ejemplo de una [respuesta de bloqueo](#).

Antes de crear el usuario

Después de la página de recopilación de atributos, se invoca un conector de API en este paso del proceso de registro, si se incluye uno. Este paso siempre se invoca antes de crear una cuenta de usuario en Azure AD.

Solicitud de ejemplo enviada a la API en este paso

```
POST <API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "identities": [ //Sent for Google and Facebook identity providers
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "givenName": "John",
  "surname": "Smith",
  "jobTitle": "Supplier",
  "streetAddress": "1000 Microsoft Way",
  "city": "Seattle",
  "postalCode": "12345",
  "state": "Washington",
  "country": "United States",
  "extension_<extensions-app-id>_CustomAttribute1": "custom attribute value",
  "extension_<extensions-app-id>_CustomAttribute2": "custom attribute value",
  "ui_locales": "en-US"
}
```

Las notificaciones exactas enviadas a la API dependen de la información recopilada por el usuario o proporcionada por el proveedor de identidades.

Tipos de respuesta esperados de la API web en este paso

Cuando la API web recibe una solicitud HTTP de Azure AD durante un flujo de usuario, puede devolver estas respuestas:

- Respuesta de continuación
- Respuesta de bloqueo
- Respuesta de validación

Respuesta de continuación

Una respuesta de continuación indica que el flujo de usuario debe continuar en el paso siguiente: creación del usuario en el directorio.

En una respuesta de continuación, la API puede devolver notificaciones. Si la API devuelve una notificación, esta realiza lo siguiente:

- Invalida cualquier valor que ya se haya asignado a la notificación de la página de colección de atributos.

Vea un ejemplo de una [respuesta de continuación](#).

Respuesta de bloqueo

Una respuesta de bloqueo termina el flujo de usuario. La API puede emitirla intencionadamente para detener el flujo de usuario y mostrar una página de bloqueo al usuario. La página de bloqueo muestra el mensaje `userMessage` proporcionado por la API.

Vea un ejemplo de una [respuesta de bloqueo](#).

Respuesta de error de validación

Cuando la API responde con una respuesta de error de validación, el flujo de usuario permanece en la página de colección de atributos y se muestra `userMessage` al usuario. El usuario puede editar el formulario y volver a enviarlo. Este tipo de respuesta se puede usar para la validación de datos de entrada.

Vea un ejemplo de una [respuesta de error de validación](#).

Respuestas de ejemplo

Ejemplo de una respuesta de continuación

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "Continue",
    "postalCode": "12349", // return claim
    "extension_<extensions-app-id>_CustomAttribute": "value" // return claim
}
```

PARÁMETRO	TIPO	REQUERIDO	DESCRIPCIÓN
version	String	Sí	La versión de la API.
action	String	Sí	El valor debe ser <code>Continue</code> .

PARÁMETRO	TIPO	REQUERIDO	DESCRIPCIÓN
<builtInUserAttribute>	<attribute-type>	No	Los valores se pueden almacenar en el directorio si están seleccionados como Claim to receive (Notificación para recibir) en la configuración del conector de API y User attribute (Atributo de usuario) de un flujo de usuario. Los valores se pueden devolver en el token si están seleccionados como Application claim (Notificación de aplicación).
<extension_{extensions-app-id}_CustomAttribute>	<attribute-type>	No	No es necesario que la notificación devuelta contenga <code>_<extensions-app-id>_</code> . Los valores se almacenan en el directorio si están seleccionados como Claim to receive (Notificación para recibir) en la configuración del conector de API y User attribute (Atributo de usuario) de un flujo de usuario. Los atributos personalizados no se pueden devolver en el token.

Ejemplo de una respuesta de bloqueo

```

HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "ShowBlockPage",
    "userMessage": "There was a problem with your request. You are not able to sign up at this time.",
    "code": "CONTOSO-BLOCK-00"
}

```

PARÁMETRO	TIPO	REQUERIDO	DESCRIPCIÓN
version	String	Sí	La versión de la API.
action	String	Sí	El valor debe ser <code>ShowBlockPage</code> .
userMessage	String	Sí	Mensaje que se va a mostrar al usuario.

PARÁMETRO	TIPO	REQUERIDO	DESCRIPCIÓN
código	String	No	Código de error. Se puede usar con fines de depuración. No se muestra al usuario.

Experiencia del usuario final con una respuesta de bloqueo



There was an error with your request. Please try again or contact support.

Done

Ejemplo de una respuesta de error de validación

```
HTTP/1.1 400 Bad Request
Content-type: application/json

{
    "version": "1.0.0",
    "status": 400,
    "action": "Validation Error",
    "userMessage": "Please enter a valid Postal Code.",
    "code": "CONTOSO-VALIDATION-00"
}
```

PARÁMETRO	TIPO	REQUERIDO	DESCRIPCIÓN
version	String	Sí	La versión de la API.
action	String	Sí	El valor debe ser ValidationError.
status	Entero	Sí	Debe ser un valor 400 para una respuesta ValidationError.
userMessage	String	Sí	Mensaje que se va a mostrar al usuario.
código	String	No	Código de error. Se puede usar con fines de depuración. No se muestra al usuario.

Experiencia del usuario final con una respuesta de error de validación



Please provide the following details.

Please enter a valid Postal Code.

Johnathan Schramm

12345

Continue

Cancel

Procedimientos recomendados y solución de problemas

Uso de funciones de nube sin servidor

Las funciones sin servidor, como los desencadenadores HTTP en Azure Functions, proporcionan una manera sencilla de crear puntos de conexión de API para usarlos con el conector de API. Puede usar la función de nube sin servidor para, [por ejemplo](#), crear la lógica de validación y limitar los registros a dominios específicos. La función de nube sin servidor también puede llamar e invocar otras API web, almacenes de usuarios y otros servicios en la nube para escenarios más complejos.

Procedimientos recomendados

Asegúrese de que:

- La API sigue los contratos de solicitud y respuesta de la API, tal y como se describe anteriormente.
- La **URL del punto de conexión** del conector de API apunta al punto de conexión de API correcto.
- La API comprueba explícitamente si hay valores NULL de las notificaciones recibidas.
- La API responde lo más rápido posible para garantizar una experiencia de usuario fluida.
 - Si usa una función sin servidor o un servicio web escalable, use un plan de hospedaje que mantenga la API "activa" o "cliente". Para Azure Functions, se recomienda usar el [plan Premium](#).

Uso del registro

En general, resulta útil usar las herramientas de registro que habilita el servicio de API web, como [Application Insights](#), para supervisar la API en busca de códigos de error inesperados, excepciones y rendimiento deficiente.

- Supervise los códigos de estado HTTP que no sean HTTP 200 ni 400.
- Un código de estado HTTP 401 o 403 suele indicar que hay un problema con la autenticación. Compruebe la capa de autenticación de la API y la configuración correspondiente en el conector de API.
- Use niveles más agresivos de registro (por ejemplo, "trace" o "debug") en el desarrollo, si es necesario.
- Supervise la API en busca de tiempos de respuesta prolongados.

Pasos siguientes

- Obtenga información sobre cómo [agregar un flujo de trabajo personalizado de aprobación al autoservicio de registro](#).
- Vea una introducción a los [ejemplos de inicio rápido de Azure Functions](#).

Adición de un flujo de trabajo de aprobaciones personalizado al registro de autoservicio

18/02/2021 • 15 minutes to read • [Edit Online](#)

Con [conectores de API](#), puede realizar la integración con sus propios flujos de trabajo de aprobaciones personalizados con el registro de autoservicio, para que pueda administrar qué cuentas de usuario invitado se crean en el inquilino.

En este artículo se proporciona un ejemplo de cómo realizar la integración con un sistema de aprobación. En este ejemplo, el flujo de usuario de registro de autoservicio recopila datos de usuario durante el proceso de registro y los pasa al sistema de aprobación. Después, el sistema de aprobación puede:

- Aprobar automáticamente el usuario y permitir que Azure AD cree la cuenta de usuario.
- Desencadenar una revisión manual. Si se aprueba la solicitud, el sistema de aprobación utiliza Microsoft Graph para aprovisionar la cuenta de usuario. El sistema de aprobación también puede notificar al usuario que se ha creado su cuenta.

IMPORTANT

A partir del 4 de enero de 2021, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa la federación de Google o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).

Registro de una aplicación para el sistema de aprobación

Debe registrar el sistema de aprobación como una aplicación en el inquilino de Azure AD para que pueda autenticarse en Azure AD y tener permiso para crear usuarios. Obtenga más información en [Aspectos básicos de autorización y autenticación de Microsoft Graph](#).

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **Registros de aplicaciones** y luego **Nuevo registro**.
4. Escriba un **Nombre** para la aplicación; por ejemplo, *Sign-up Approvals*.
5. Seleccione **Registrar**. Puede dejar todos los demás campos con sus valores predeterminados.

Register an application

X

* Name

The user-facing display name for this application (this can be changed later).



Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Microsoft only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

6. En **Administrar**, en el menú de la izquierda, seleccione **Permisos de API** y, después, **Agregar un permiso**.
7. En la página **Solicitud de permisos de API**, seleccione **Microsoft Graph** y, después, **Permisos de la aplicación**.
8. En **Seleccionar permisos**, expanda **Usuario** y, después, seleccione la casilla **User.ReadWrite.All**. Este permiso permite al sistema de aprobación crear el usuario tras su aprobación. Seleccione **Agregar permisos**.

Request API permissions

X

< All APIs

> TrustFrameworkKeySet

> UserAuthenticationMethod

> UserNotification

> UserShiftPreferences

▼ **User (1)**

<input type="checkbox"/> User.Export.All Export user's data ⓘ	Yes
<input type="checkbox"/> User.Invite.All Invite guest users to the organization ⓘ	Yes
<input type="checkbox"/> User.ManageIdentities.All Manage all users' identities ⓘ	Yes
<input type="checkbox"/> User.Read.All Read all users' full profiles ⓘ	Yes
<input checked="" type="checkbox"/> User.ReadWrite.All Read and write all users' full profiles ⓘ	Yes

9. En la página **Permisos de API**, seleccione **Conceder consentimiento de administrador para (nombre del inquilino)** y, después, seleccione **Sí**.
10. En **Administrar**, en el menú de la izquierda, seleccione **Certificados y secretos** y luego **Nuevo**

secreto de cliente.

11. Escriba una **Descripción** para el secreto, por ejemplo, *Secreto de cliente de aprobaciones* y seleccione la duración para la **Expiración** del secreto de cliente. A continuación, seleccione **Agregar**.
 12. Copie el valor del secreto de cliente.

13. Configure el sistema de aprobación para usar el **Id. de la aplicación** como el identificador de cliente y el **secreto de cliente** generado para autenticarse en Azure AD.

Creación de los conectores de API

A continuación, [creará los conectores de API](#) para el flujo de usuario de registro de autoservicio. La API del sistema de aprobación necesita dos conectores y los puntos de conexión correspondientes, como los ejemplos que se muestran a continuación. Estos conectores de API hacen lo siguiente:

- **Comprobar el estado de aprobación.** Enviar una llamada al sistema de aprobación inmediatamente después de que un usuario inicie sesión con un proveedor de identidades, para comprobar si el usuario tiene una solicitud de aprobación existente o si ya se ha denegado. Si el sistema de aprobación solo toma decisiones de aprobación automáticas, es posible que este conector de API no sea necesario. Ejemplo de un conector de API "Check approval status".

Configure an API connector

Save Discard Remove

Configure an API connector. You can use API connectors within a user flow to send a request to an HTTP endpoint. [Learn more](#)

Display name * ⓘ
Check approval status ✓

Endpoint URL * ⓘ
https://approvals.contoso.com/checkApprovalStatus ✓

Username * ⓘ
<api_username> ✓

Password * ⓘ
<api_password> ✓

- **Solicitar aprobación.** Enviar una llamada al sistema de aprobación después de que un usuario complete la página de la colección de atributos, pero antes de que se cree la cuenta de usuario, para solicitar la aprobación. La solicitud de aprobación se puede conceder automáticamente o revisar de forma manual. Ejemplo de un conector de API "Request approval".

Configure an API connector

X

 Save  Discard  Remove

Configure an API connector. You can use API connectors within a user flow to send a request to an HTTP endpoint. [Learn more](#)

Display name * ⓘ

Request approval



Endpoint URL * ⓘ

https://approvals.contoso.com/api/requestApproval



Username * ⓘ

<api_username>



Password * ⓘ

<api_password>



Para crear estos conectores, siga los pasos descritos en [Creación de un conector de API](#).

Habilitación de los conectores de API en un flujo de usuario

Ahora, agregará los conectores de API a un flujo de usuario de registro de autoservicio con estos pasos:

1. Inicie sesión en [Azure Portal](#) como administrador de Azure AD.
2. En **Servicios de Azure**, seleccione **Azure Active Directory**.
3. En el menú de la izquierda, seleccione **External Identities**.
4. Seleccione **Flujos de usuario (versión preliminar)** y, después, seleccione el flujo de usuario para el que desea habilitar el conector de API.
5. Seleccione **Conectores de API** y, después, seleccione los puntos de conexión de API que desea invocar en los pasos siguientes del flujo de usuario:
 - **Después de iniciar sesión con un proveedor de identidades:** seleccione el conector de API del estado de aprobación; por ejemplo, *Check approval status*.
 - **Antes de crear el usuario:** seleccione el conector de API de solicitud de aprobación; por ejemplo, *Request approval*.

The screenshot shows the 'B2X_1_SignUp | API connectors' configuration page. The left sidebar includes 'Overview', 'Settings', 'Identity providers', 'User attributes', and 'API connectors' (which is selected). The main area has sections for 'Choose which, if any, API connector to invoke at a specific step in the user flow' and 'Learn more'. It lists two steps: 'After signing in with an identity provider' (set to 'Check approval status') and 'Before creating the user' (set to 'Request approval'). Both of these settings are highlighted with red boxes.

6. Seleccione Guardar.

Control del flujo de registro con respuestas de API

El sistema de aprobación puede usar sus respuestas cuando se llama para controlar el flujo de registro.

Solicitud y respuestas del conector de API "Check approval status"

Ejemplo de la solicitud recibida por la API desde el conector de API "Check approval status":

```
POST <API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "identities": [ //Sent for Google and Facebook identity providers
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "givenName": "John",
  "lastName": "Smith",
  "ui_locales": "en-US"
}
```

Las notificaciones exactas enviadas a la API dependen de la información proporcionada por el proveedor de identidades. Siempre se envía "email".

Respuesta de continuación para "Check approval status"

El punto de conexión de la API **Check approval status** debe devolver una respuesta de continuación si:

- El usuario no ha solicitado previamente una aprobación.

Ejemplo de la respuesta de continuación:

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "Continue"
}
```

Respuesta de bloqueo para "Check approval status"

El punto de conexión de la API **Check approval status** debe devolver una respuesta de bloqueo si:

- La aprobación del usuario está pendiente.
- Se denegó el usuario y no se le debería permitir volver a solicitar la aprobación.

Estos son ejemplos de respuestas de bloqueo:

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "ShowBlockPage",
    "userMessage": "Your access request is already processing. You'll be notified when your request has been approved.",
    "code": "CONTOSO-APPROVAL-PENDING"
}
```

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "ShowBlockPage",
    "userMessage": "Your sign up request has been denied. Please contact an administrator if you believe this is an error",
    "code": "CONTOSO-APPROVAL-DENIED"
}
```

Solicitud y respuestas del conector de API "Request approval"

Ejemplo de una solicitud HTTP recibida por la API desde el conector de API "Request approval":

```

POST <API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "identities": [ //Sent for Google and Facebook identity providers
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "givenName": "John",
  "surname": "Smith",
  "jobTitle": "Supplier",
  "streetAddress": "1000 Microsoft Way",
  "city": "Seattle",
  "postalCode": "12345",
  "state": "Washington",
  "country": "United States",
  "extension_<extensions-app-id>_CustomAttribute1": "custom attribute value",
  "extension_<extensions-app-id>_CustomAttribute2": "custom attribute value",
  "ui_locales": "en-US"
}

```

Las notificaciones exactas enviadas a la API dependen de la información recopilada por el usuario o proporcionada por el proveedor de identidades.

Respuesta de continuación para "Request approval"

El punto de conexión de la API **Request approval** debe devolver una respuesta de continuación si:

- El usuario se puede *aprobar automáticamente*.

Ejemplo de la respuesta de continuación:

```

HTTP/1.1 200 OK
Content-type: application/json

{
  "version": "1.0.0",
  "action": "Continue"
}

```

IMPORTANT

Si se recibe una respuesta de continuación, Azure AD crea una cuenta de usuario y dirige al usuario a la aplicación.

Respuesta de bloqueo para "Request approval"

El punto de conexión de la API **Request approval** debe devolver una respuesta de bloqueo si:

- Se ha creado una solicitud de aprobación de usuario y está pendiente.
- Se denegó automáticamente una solicitud de aprobación de usuario.

Estos son ejemplos de respuestas de bloqueo:

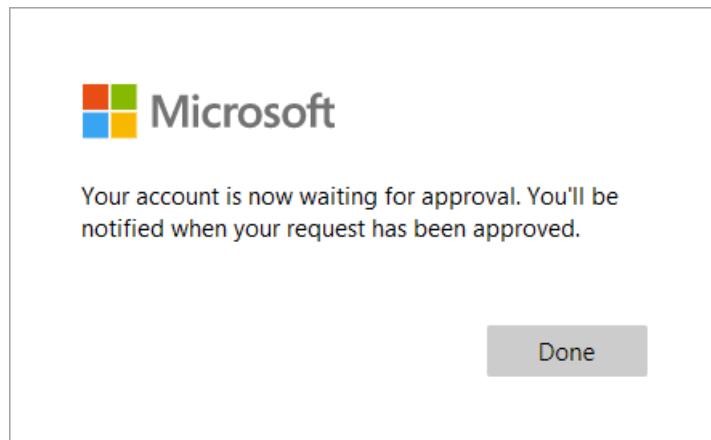
```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "ShowBlockPage",
    "userMessage": "Your account is now waiting for approval. You'll be notified when your request has been approved.",
    "code": "CONTOSO-APPROVAL-REQUESTED"
}
```

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "version": "1.0.0",
    "action": "ShowBlockPage",
    "userMessage": "Your sign up request has been denied. Please contact an administrator if you believe this is an error",
    "code": "CONTOSO-APPROVAL-AUTO-DENIED"
}
```

El valor `userMessage` se muestra al usuario en la respuesta; por ejemplo:



Creación de cuentas de usuario después de la aprobación manual

Después de obtener la aprobación manual, el sistema de aprobación personalizado crea una cuenta de [usuario](#) mediante [Microsoft Graph](#). La forma en que el sistema de aprobación aprovisiona la cuenta de usuario depende del proveedor de identidades que el usuario utiliza.

Para un usuario federado de Google o Facebook

IMPORTANT

El sistema de aprobación debe comprobar explícitamente que `identities`, `identities[0]` y `identities[0].issuer` están presentes y que `identities[0].issuer` es igual a "facebook" o "google" para usar este método.

Si el usuario ha iniciado sesión con una cuenta de Google o Facebook, puede usar la [API de creación de usuarios](#).

1. El sistema de aprobación recibe la solicitud HTTP del flujo de usuario.

```

POST <Approvals-API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@outlook.com",
  "identities": [
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "city": "Redmond",
  "extension_<extensions-app-id>_CustomAttribute": "custom attribute value",
  "ui_locales": "en-US"
}

```

2. El sistema de aprobación utiliza Microsoft Graph para crear una cuenta de usuario.

```

POST https://graph.microsoft.com/v1.0/users
Content-type: application/json

{
  "userPrincipalName": "johnsmith_outlook.com#EXT@contoso.onmicrosoft.com",
  "accountEnabled": true,
  "mail": "johnsmith@outlook.com",
  "userType": "Guest",
  "identities": [
    {
      "signInType": "federated",
      "issuer": "facebook.com",
      "issuerAssignedId": "0123456789"
    }
  ],
  "displayName": "John Smith",
  "city": "Redmond",
  "extension_<extensions-app-id>_CustomAttribute": "custom attribute value"
}

```

PARÁMETRO	OBLIGATORIO	DESCRIPCIÓN
userPrincipalName	Sí	Se puede generar con la utilización de la notificación <code>email</code> enviada a la API, la sustitución del carácter <code>@</code> por <code>_</code> y anteponiéndolo a <code>#EXT@<tenant-name>.onmicrosoft.com</code> .
accountEnabled	Sí	Se debe establecer en <code>true</code> .
mail	Sí	Equivalente a la notificación <code>email</code> enviada a la API.
userType	Sí	Debe ser <code>Guest</code> . Designa a este usuario como un usuario invitado.
Identidades	Sí	Información de la identidad federada.

PARÁMETRO	OBLIGATORIO	DESCRIPCIÓN
<otherBuiltInAttribute>	No	Otros atributos integrados, como <code>displayName</code> , <code>city</code> y otros. Los nombres de los parámetros son los mismos que los que envía el conector de API.
<extension_{extensions-app-id}_CustomAttribute>	No	Atributos personalizados sobre el usuario. Los nombres de los parámetros son los mismos que los que envía el conector de API.

Para un usuario de Azure Active Directory federado

Si un usuario inicia sesión con una cuenta de Azure Active Directory federada, debe usar la [API de invitación](#) para crear el usuario y, opcionalmente, la [API de actualización de usuario](#) para asignar más atributos al usuario.

- El sistema de aprobación recibe la solicitud HTTP del flujo de usuario.

```
POST <Approvals-API-endpoint>
Content-type: application/json

{
  "email": "johnsmith@fabrikam.onmicrosoft.com",
  "displayName": "John Smith",
  "city": "Redmond",
  "extension_{extensions-app-id}_CustomAttribute": "custom attribute value",
  "ui_locales": "en-US"
}
```

- El sistema de aprobación crea la invitación mediante el atributo `email` proporcionado por el conector de API.

```
POST https://graph.microsoft.com/v1.0/invitations
Content-type: application/json

{
  "invitedUserEmailAddress": "johnsmith@fabrikam.onmicrosoft.com",
  "inviteRedirectUrl": "https://myapp.com"
}
```

Ejemplo de la respuesta:

```
HTTP/1.1 201 OK
Content-type: application/json

{
  ...
  "invitedUser": {
    "id": "<generated-user-guid>"
  }
}
```

- El sistema de aprobación usa el identificador del usuario invitado para actualizar la cuenta del usuario con los atributos de usuario recopilados (opcional).

```
PATCHhttps://graph.microsoft.com/v1.0/users/<generated-user-guid>
Content-type: application/json

{
    "displayName": "John Smith",
    "city": "Redmond",
    "extension_<extensions-app-id>_AttributeName": "custom attribute value"
}
```

Pasos siguientes

- Introducción a los [ejemplos de inicio rápido de Azure Functions](#).
- Compruebe el [registro de autoservicio para usuarios invitados con el ejemplo de aprobación manual](#).

Conceda permisos a los usuarios de organizaciones asociadas en el inquilino de Azure Active Directory

18/02/2021 • 2 minutes to read • [Edit Online](#)

Los usuarios de colaboración B2B de Azure Active Directory (Azure AD) se agregan como usuarios invitados al directorio y los permisos de invitado del directorio están restringidos de forma predeterminada. Asimismo, su empresa puede necesitar algunos usuarios invitados para cubrir más roles con privilegios en su organización. Para respaldar la definición de roles de privilegios más elevados, se pueden agregar usuarios invitados a los roles que desee, según las necesidades de su organización.

Rol predeterminado

The screenshot shows the Azure portal interface for managing a user's directory role. The title bar reads "Sam Oogle - Directory role" and "User - PREVIEW". The top navigation bar includes "Save" and "Discard" buttons. On the left, a sidebar menu lists "Overview", "Profile", "Directory role" (which is selected and highlighted in blue), "Groups", "Licenses", "Devices", and "Azure resources". Below this, under "ACTIVITY", are "Sign-ins" and "Audit logs". The main content area is titled "Directory role" and contains three radio button options: "User" (selected), "Global administrator", and "Limited administrator". A descriptive text block states: "Users can access assigned resources but cannot manage most directory resources." followed by a "Learn More" link.

Rol de administrador global

Sam Oogle - Directory role

User - PREVIEW



Save Discard

Search (Ctrl+ /)

Overview

MANAGE

Profile

Directory role

Groups

Licenses

Devices

Azure resources

ACTIVITY

Sign-ins

Audit logs

Directory role

User

Global administrator

Limited administrator

Global administrators have full control over all directory resources.

[Learn More](#)

Rol de administrador limitado

Sam Oogle - Directory role

User - PREVIEW

Save Discard

Search (Ctrl+ /)

Overview

MANAGE

Profile

Directory role

Groups

Licenses

Devices

Azure resources

ACTIVITY

Sign-ins

Audit logs

Directory role ●

User

Global administrator

Limited administrator

Select the administrative role or roles for this user.

[Learn More](#)

Password administrator ●

Service administrator ●

Billing administrator ●

Exchange administrator ●

Skype for Business administrator ●

User administrator ●

SharePoint administrator ●

Compliance administrator ●

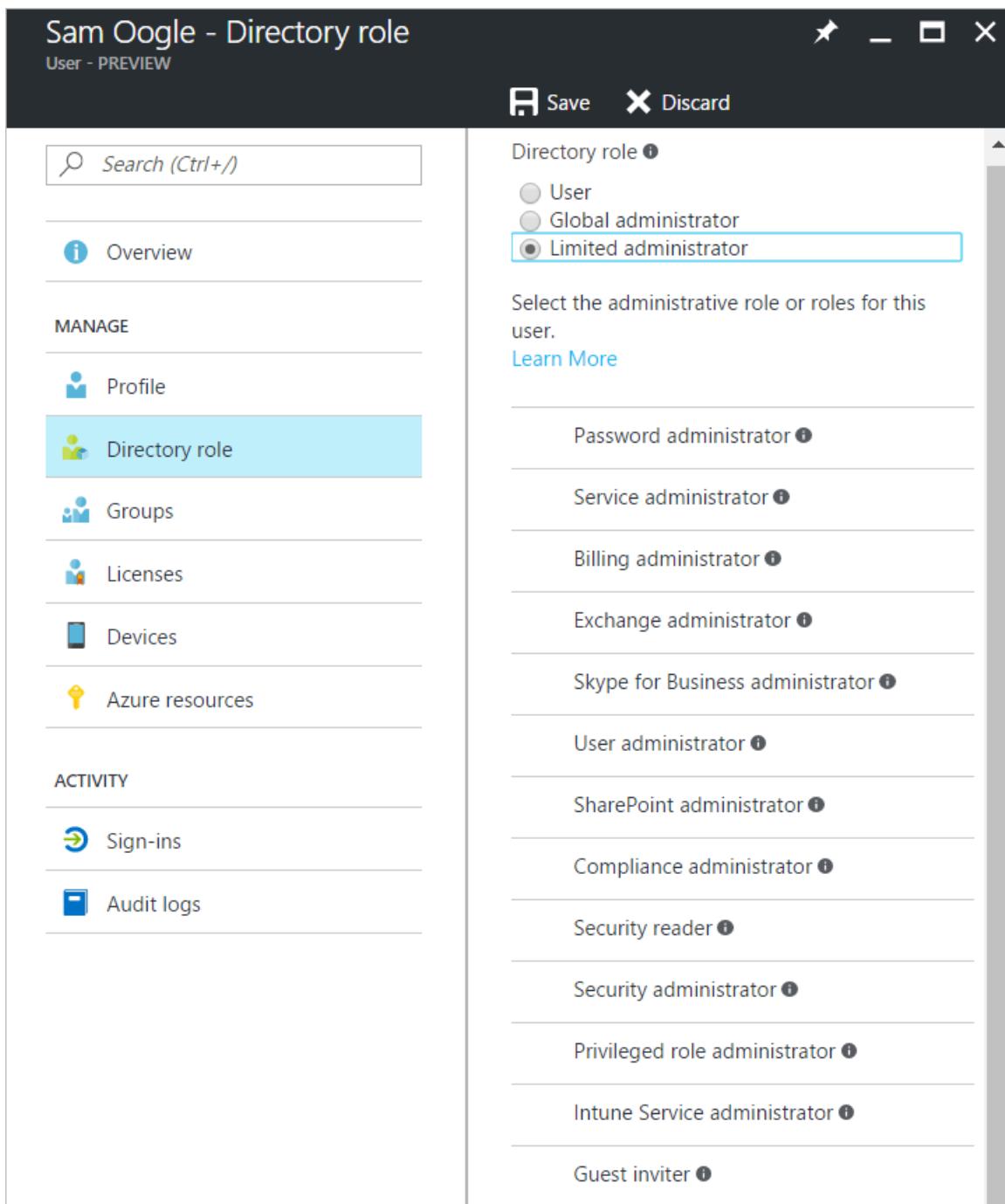
Security reader ●

Security administrator ●

Privileged role administrator ●

Intune Service administrator ●

Guest inviter ●



Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Propiedades de usuario de la colaboración B2B](#)

Grupos dinámicos y colaboración B2B de Azure Active Directory

18/02/2021 • 4 minutes to read • [Edit Online](#)

¿Qué son los grupos dinámicos?

La configuración dinámica de pertenencia a grupos de seguridad de Azure Active Directory (Azure AD) está disponible en [Azure Portal](#). Los administradores pueden establecer reglas para llenar los grupos que se crean en Azure AD en función de los atributos de usuario (por ejemplo, userType, department o country/region). Los miembros se agregan automáticamente a un grupo de seguridad, o se quitan de este, según sus atributos. Estos grupos pueden proporcionar acceso a aplicaciones o recursos en la nube (documentos y sitios de SharePoint) y para asignar licencias a miembros. Obtenga más información sobre los grupos dinámicos en [Grupos dedicados en Azure Active Directory](#).

La [licencia Azure AD Premium P1 o P2](#) apropiada se necesita para crear y usar grupos dinámicos. Obtenga más información en el artículo [Creación de reglas de pertenencia dinámica a grupos basadas en atributos en Azure Active Directory](#).

Creación del grupo dinámico «Todos los usuarios»

Puede crear un grupo que contenga todos los usuarios de un inquilino mediante una regla de pertenencia. Cuando se agreguen o eliminen usuarios del inquilino en el futuro, la pertenencia al grupo se ajustará automáticamente.

1. Inicie la sesión en [Azure Portal](#) con una cuenta a la que se haya asignado el rol de administrador global o administrador de usuarios en la organización.
2. Seleccione **Azure Active Directory**.
3. Seleccione **Administrar**, **Grupos** y, a continuación, **Nuevo grupo**.
4. En la página **Nuevo grupo**, en **Tipo de grupo**, seleccione **Seguridad**. Escriba un **Nombre de grupo** y una **Descripción del grupo** para el nuevo grupo.
5. En **Tipo de pertenencia**, seleccione **Usuario dinámico** y, a continuación, **Agregar una consulta dinámica**.
6. Encima del cuadro de texto **Sintaxis de regla**, seleccione **Editar**. En la página **Editar sintaxis de la regla**, escriba la siguiente expresión en el cuadro de texto:

```
user.ObjectId -ne null
```

7. Seleccione **Aceptar**. La regla aparece en el cuadro Sintaxis de regla:

Dynamic membership rules

Save Discard Got feedback? 

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.  [Learn more](#)

And/Or	Property	Operator	Value	
And	<Choose a Property>	<Choose an Operat...	Add a value	

+ Add expression + Get custom extension properties 

 Some items could not be displayed in the rule builder. [Learn more](#)

Rule syntax 

```
user.ObjectId -ne null
```

8. Seleccione **Guardar**. En el nuevo grupo dinámico se incluirán ahora los usuarios invitados de B2B y los usuarios miembros.
9. Seleccione **Crear** en la página **Nuevo grupo** para crear el grupo.

Creación de un grupo de miembros solamente

Si desea que el grupo excluya los usuarios invitados e incluya solo los miembros de su inquilino, cree un grupo dinámico tal como se describió anteriormente, pero en el cuadro **Sintaxis de regla**, escriba la siguiente expresión:

```
(user.ObjectId -ne null) and (user.userType -eq "Member")
```

En la siguiente imagen se muestra la sintaxis de la regla para un grupo dinámico modificado, para que incluya solo miembros y excluya invitados.

Dynamic membership rules

Save Discard Got feedback?

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	objectId	Not Equals	null
And	userType	Equals	Member

+ Add expression + Get custom extension properties [\(i\)](#)

Rule syntax [\(i\)](#)

(user.ObjectId -ne null) and (user.userType -eq "Member")

[Edit](#)

Creación de un grupo de invitados solamente

Puede que también encuentre esto útil para crear un grupo dinámico que contenga solo usuarios invitados, de manera que pueda aplicar directivas (como directivas de acceso condicional de Azure AD) para ellos. Cree un grupo dinámico tal como se describió anteriormente, pero en el cuadro **Sintaxis de regla**, escriba la siguiente expresión:

```
(user.ObjectId -ne null) and (user.userType -eq "Guest")
```

En la siguiente imagen se muestra la sintaxis de la regla de un grupo dinámico modificado, para que incluya solo invitados y excluya miembros.

Dynamic membership rules

Save Discard Got feedback?

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	objectId	Not Equals	null
And	userType	Equals	Guest

+ Add expression + Get custom extension properties [\(i\)](#)

Rule syntax [\(i\)](#)

(user.ObjectId -ne null) and (user.userType -eq "Guest")

[Edit](#)

Pasos siguientes

- [Propiedades de usuario de la colaboración B2B](#)
- [Incorporación de usuarios de colaboración B2B a un rol](#)
- [Acceso condicional para usuarios de colaboración B2B](#)

Propiedades de un usuario de colaboración B2B de Azure Active Directory

18/02/2021 • 13 minutes to read • [Edit Online](#)

En este artículo se describen las propiedades y los estados del objeto de usuario invitado B2B en Azure Active Directory (Azure AD) antes y después del canje de invitación. Un usuario de colaboración de negocio a negocio (B2B) de Azure AD es un usuario con UserType = Guest. Dicho usuario suele ser de una organización asociada y tiene, de forma predeterminada, privilegios limitados en el directorio de la invitación.

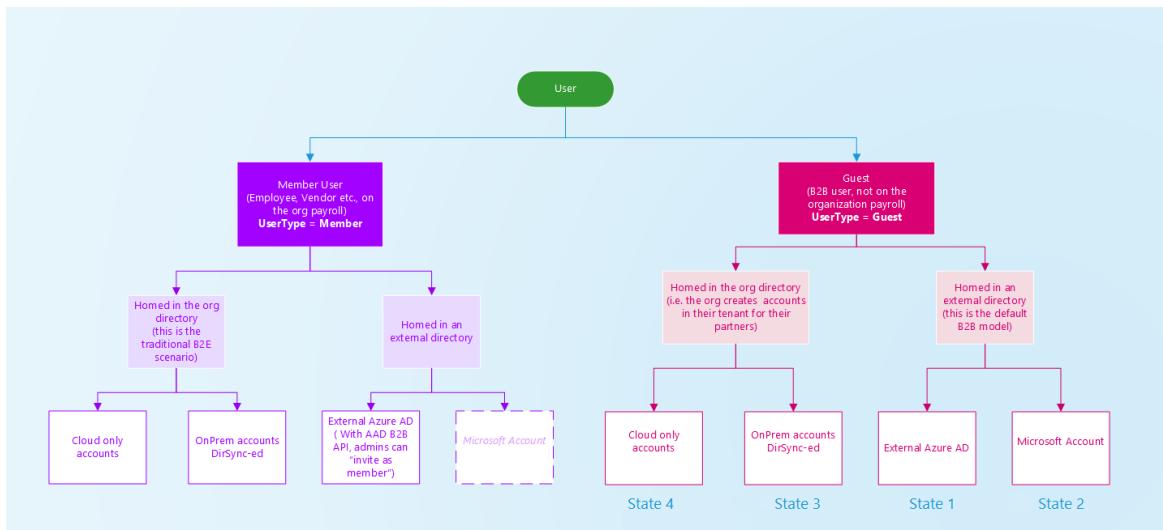
En función de las necesidades de la organización invitadora, un usuario de colaboración de B2B de Azure AD puede tener cualquiera de los siguientes estados de cuenta:

- Estado 1: alojado en una instancia externa de Azure AD y representado como un usuario invitado en la organización que invita. En este caso, el usuario de B2B inicia sesión con una cuenta de Azure AD que pertenece al inquilino invitado. Aunque la organización asociada no use Azure AD, se crea el usuario invitado en Azure AD. Los requisitos son que el usuario canjea su invitación y Azure AD comprueba su dirección de correo electrónico. Esta solución también se denomina inquilino Just-In-Time (JIT) o inquilino "viral".

IMPORTANT

A partir del 31 de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

- Estado 2: alojado en una cuenta Microsoft u otra cuenta y representado como usuario invitado en la organización host. En este caso, el usuario invitado inicia sesión con una cuenta de Microsoft o una cuenta social (google.com o similar). La identidad del usuario invitado se crea como una cuenta de Microsoft en el directorio de la organización que invita durante el canje de la oferta.
- Estado 3: alojado en la instancia de Active Directory local de la organización host y sincronizado con la instancia de Azure AD de la organización host. Puede usar Azure AD Connect para sincronizar las cuentas de asociado con la nube como usuarios B2B de Azure AD con UserType = Invitado. Vea [Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube](#).
- Estado 4: alojado en la instancia de Azure AD de la organización host con UserType = Invitado y credenciales que administra dicha organización.



Ahora, veamos cómo es un usuario de colaboración de B2B de Azure AD en Azure AD.

Antes del canje de la invitación

Las cuentas de estado 1 y estado 2 resultan de los usuarios invitados que invitan a colaborar con el uso de las propias credenciales de los usuarios invitados. Cuando se envía inicialmente la invitación al usuario invitado, se crea una cuenta en el directorio. Esta cuenta no tiene ninguna credencial asociada, ya que la autenticación la realiza el proveedor de identidades del usuario invitado. La propiedad **Origen** de la cuenta de usuario invitado del directorio se establece en **Usuario invitado**.

Identity		
Name	First name	Last name
gsamoogleg	-- --	-- --
User name	User type	Group memberships
gsamoogleg@gmail.com	Guest	0
Object ID	Source	
8ea9cea8-1594-41bf...	Invited user	Resend invitation

Después del canje de la invitación

Una vez que el usuario invitado acepta la invitación, la propiedad **Origen** se actualiza según determine el proveedor de identidades del usuario invitado.

Para los usuarios invitados en estado 1, el **origen** es **Azure Active Directory externo**.

Home > Users - All users > Guest User1 - Profile

Guest User1 - Profile

User

Manage

- Profile**
- Directory role
- Groups
- Applications
- Licenses
- Devices
- Azure resources

Activity

- Sign-ins
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Edit **Reset password** **Delete**

Guest User1

guestuser1@fabrikam.com



User Sign-ins



Group memberships

0

Identity [edit](#)

Name	First name	Last name
Guest User1	---	---
User name	User type	Invitation accepted
guestuser1@fabrikam.com	Guest	Yes
Object ID	Source	
462cd2ac-018a-4194...	External Azure Active Directory	

Job info [edit](#)

Job title	Department	Manager
-----------	------------	---------

Para los usuarios invitados en estado 2, el origen es Cuenta Microsoft.

Home > Users - All users > gsamoogle - Profile

gsamoogle - Profile

User

Manage

- Profile**
- Directory role
- Groups
- Applications
- Licenses
- Devices
- Azure resources

Activity

- Sign-ins
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Edit **Reset password** **Delete**

gsamoogle

gsamoogle@gmail.com



User Sign-ins



Group memberships

0

Identity [edit](#)

Name	First name	Last name
gsamoogle	---	---
User name	User type	Invitation accepted
gsamoogle@gmail.com	Guest	Yes
Object ID	Source	
8ea9cea8-1594-4...	Microsoft Account	

Job info [edit](#)

Job title	Department	Manager
-----------	------------	---------

Para los usuarios invitados en estado 3 y estado 4, la propiedad Origen se establece en Azure Active Directory o Windows Server Active Directory, como se describe en la siguiente sección.

Propiedades clave del usuario de colaboración de B2B de Azure AD

UserType

Esta propiedad indica la relación del usuario con el espacio host. Esta propiedad puede tener dos valores:

- Miembro: este valor indica un empleado de la organización host y un usuario en la plantilla de dicha organización. Por ejemplo, este usuario espera tener acceso solo a sitios internos. Este usuario no se considera como un colaborador externo.
- Invitado: Este valor indica un usuario que no se considera interno de la empresa, como un colaborador externo, un asociado o un cliente. No se espera que dicho usuario reciba una comunicación interna del CEO o que reciba beneficios de la empresa, por ejemplo.

NOTE

UserType no tiene relación alguna con la forma en que el usuario inicia sesión, el rol de directorio del usuario, etc. Esta propiedad simplemente indica la relación del usuario con la organización host y permite a la organización exigir directivas que dependan de esta propiedad.

Para obtener detalles relacionados con los precios, consulte [Precios de Azure Active Directory](#).

Source

Esta propiedad indica la forma en que el usuario inicia sesión.

- Usuario invitado: este usuario ha recibido la invitación, pero aún no la ha canjeado.
- Azure Active Directory externo: este usuario está alojado en una organización externa y se autentica mediante una cuenta de Azure AD que pertenece a la otra organización. Este tipo de inicio de sesión corresponde al estado 1.
- Cuenta de Microsoft: el usuario está alojado en una cuenta de Microsoft y se autentica mediante una cuenta de Microsoft. Este tipo de inicio de sesión corresponde al estado 2.
- Windows Server Active Directory: este usuario inicia sesión desde una instancia de Active Directory local que pertenece a esta organización. Este tipo de inicio de sesión corresponde al estado 3.
- Azure Active Directory: este usuario se autentica mediante una cuenta de Azure AD que pertenece a esta organización. Este tipo de inicio de sesión corresponde al estado 4.

NOTE

Source y UserType son propiedades independientes. Un valor de Source no implica un valor concreto de UserType.

¿Se pueden agregar usuarios de B2B de Azure AD como miembros, en lugar de como invitados?

Normalmente, un usuario invitado y uno de B2B de Azure AD son sinónimos. Por tanto, de manera predeterminada los usuarios de colaboración de B2B de Azure AD se agregan como usuario con UserType = Guest. Sin embargo, en algunos casos, la organización asociada forma parte de una organización mayor a la que también pertenece la organización host. En ese caso, la organización host puede tratar a los usuarios de la organización asociada como miembros, en lugar de como invitados. Use las API del Administrador de invitaciones de B2B de Azure AD para agregar un usuario de la organización asociada a la organización host como miembro, o para invitarlo.

Filtro de usuarios invitados en el directorio

The screenshot shows the 'Users - All users' page in Microsoft Azure Active Directory. On the left, there's a sidebar with navigation links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Activity', 'Sign-ins', 'Audit logs', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area has a search bar for 'Name' and a dropdown for 'Show' set to 'Guest users only'. A table lists six guest users with columns for 'NAME', 'USER NAME', 'USER TYPE', and 'SOURCE'. The users are:

NAME	USER NAME	USER TYPE	SOURCE
stdealer	stdealer@comcast.net	Guest	Microsoft Account
bryce	bryce@litwarecorp.com	Guest	Invited user
basarajesh	basarajesh@yahoo.com	Guest	Microsoft Account
Sanda	sanda@contoso.com	Guest	Azure Active Directory
Sarat Subramaniam	sarat@fabrikam.com	Guest	External Azure Active Directory
tjb2b	tjb2b@live.com	Guest	Invited user

Conversión de UserType

Es posible convertir UserType de miembro a invitado, y viceversa, mediante PowerShell. Sin embargo, la propiedad UserType representa la relación del usuario con la organización. Por tanto, debe cambiar esta propiedad solo si cambia la relación del usuario con la organización. Si cambia la relación del usuario, ¿se debe cambiar el nombre principal de usuario (UPN)? ¿Debe el usuario seguir teniendo acceso a los mismos recursos? ¿Debe asignarse un buzón de correo? No se recomienda cambiar el valor de UserType mediante el uso de PowerShell como una actividad atómica. Además, en caso de que esta propiedad se vuelva inmutable mediante PowerShell, no se recomienda depender de este valor.

Eliminación de limitaciones de usuarios invitados

Puede haber casos en los que desee ofrecer a los usuarios invitados privilegios más altos. Puede agregar un usuario invitado a cualquier rol e, incluso, eliminar las restricciones de usuario invitado predeterminadas en el directorio para concederle los mismos privilegios que a los miembros.

Se pueden desactivar las limitaciones predeterminadas para que un usuario invitado del directorio de la empresa tenga los mismos permisos que un usuario que sea miembro.

The screenshot shows the 'Microsoft - User settings' page in the Azure Active Directory portal. The left sidebar has a search bar and a list of options: App registrations, App registrations (Preview), Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings (selected), Properties, and Notifications settings. Below these are sections for Security: Identity Secure Score (Preview) and Conditional Access. The main pane shows 'Enterprise applications' with a link to 'Manage how end users launch and view their applications'. Under 'App registrations', it says 'Users can register applications' with 'Yes' and 'No' buttons ('Yes' is selected). The 'Administration portal' section has 'Restrict access to Azure AD administration portal' with 'Yes' and 'No' buttons ('No' is selected). The 'External users' section has a link to 'Manage external collaboration settings'. The 'Access panel' section has a link to 'Manage settings for access panel preview features'.

¿Puedo hacer visibles a los usuarios invitados en la lista global de direcciones de Exchange?

Sí. De forma predeterminada, los objetos de invitado no aparecen en la lista global de direcciones de la organización, pero puede usar Azure Active Directory PowerShell para que figuren. Para más información, consulte [¿Puedo hacer visibles los objetos de invitado de la lista global de direcciones?](#) en [Administración del acceso de invitados en grupos de Microsoft 365](#).

¿Puedo actualizar la dirección de correo electrónico de un usuario invitado?

Si un usuario invitado acepta su invitación y cambia posteriormente su dirección de correo electrónico, el nuevo correo electrónico no se sincroniza automáticamente con el objeto de usuario invitado en el directorio. La propiedad mail se crea a través de [Microsoft Graph API](#). Puede actualizar la propiedad de correo electrónico mediante Microsoft Graph API, el centro de administración de Exchange o [PowerShell de Exchange Online](#). El cambio se reflejará en el objeto de usuario invitado de Azure AD.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Tokens de usuario de colaboración B2B](#)
- [Asignación de notificaciones de usuario de colaboración B2B](#)

Restablecimiento del estado de canje para un usuario invitado

18/02/2021 • 3 minutes to read • [Edit Online](#)

Una vez que un usuario invitado ha canjeado su invitación para la colaboración B2B, puede haber ocasiones en las que tenga que actualizar la información de inicio de sesión, por ejemplo, cuando:

- El usuario quiera iniciar sesión con otro correo electrónico y proveedor de identidades.
- Se haya eliminado y vuelto crear la cuenta del usuario en su inquilino principal.
- El usuario esté trabajando en otra empresa, pero todavía necesite el mismo acceso a los recursos.
- Las responsabilidades del usuario se hayan pasado a otro usuario.

Para administrar estos escenarios, anteriormente tenía que eliminar manualmente la cuenta del usuario invitado de su directorio y volver a invitar al usuario. Ahora puede usar PowerShell o la API de invitación de Microsoft Graph para restablecer el estado de canje del usuario y volver a invitarlo, a la vez que conserva el identificador de objeto del usuario, las pertenencias a grupos y las asignaciones de aplicaciones. Cuando el usuario canjea la nueva invitación, la nueva dirección de correo electrónico se convierte en el UPN del usuario. Posteriormente, el usuario puede iniciar sesión con el nuevo correo electrónico o con un correo electrónico que se haya agregado a la propiedad `otherMails` del objeto de usuario.

Uso de PowerShell para restablecer el estado de canje

Instale el módulo AzureADPreview de PowerShell más reciente y cree una nueva invitación con `invitedUserEmailAddress` establecido en la nueva dirección de correo electrónico, y `ResetRedemption` establecido en `true`.

```
Uninstall-Module AzureADPreview
Install-Module AzureADPreview
Connect-AzureAD
$ADGraphUser = Get-AzureADUser -objectID "UPN of User to Reset"
$msGraphUser = New-Object Microsoft.Open.MSGraph.Model.User -ArgumentList $ADGraphUser.ObjectId
New-AzureADMSInvitation -invitedUserEmailAddress <>external email></> -SendInvitationMessage $True -
InviteRedirectUrl "http://myapps.microsoft.com" -invitedUser $msGraphUser -ResetRedemption $True
```

Uso de Microsoft Graph API para restablecer el estado de canje

Con la [API de invitación de Microsoft Graph](#), establezca la propiedad `resetRedemption` en `true` y especifique la nueva dirección de correo electrónico en la propiedad `invitedUserEmailAddress`.

```
POST https://graph.microsoft.com/beta/invitations
Authorization: Bearer eyJ0eX...
ContentType: application/json
{
  "invitedUserEmailAddress": "<<external email>>",
  "sendInvitationMessage": true,
  "invitedUserMessageInfo": {
    "messageLanguage": "en-US",
    "ccRecipients": [
      {
        "emailAddress": {
          "name": null,
          "address": "<<optional additional notification email>>"
        }
      }
    ],
    "customizedMessageBody": "<<custom message>>"
  },
  "inviteRedirectUrl": "https://myapps.microsoft.com?tenantId=",
  "invitedUser": {
    "id": "<<ID for the user you want to reset>>"
  },
  "resetRedemption": true
}
```

Pasos siguientes

- [Incorporación de usuarios de colaboración B2B de Azure Active Directory con PowerShell](#)
- [Propiedades de un usuario invitado de Azure AD B2B](#)

Configuración de aplicaciones de SaaS para la colaboración B2B

18/02/2021 • 6 minutes to read • [Edit Online](#)

La colaboración de B2B de Azure Active Directory (Azure AD) funciona con la mayoría de las aplicaciones que se integran con Azure AD. En esta sección, se proporcionan las instrucciones necesarias para configurar varias aplicaciones populares de SAS para usarlas con B2B de Azure AD.

Antes de examinar las instrucciones específicas de la aplicación, estas son algunas reglas generales:

- En la mayoría de las aplicaciones, la instalación del usuario se debe realizar de forma manual. Es decir, los usuarios deben crearse de forma manual también en la aplicación.
- En el caso de las aplicaciones que admiten la instalación automática, como Dropbox, se crean invitaciones independientes desde las aplicaciones. Los usuarios debe asegurarse de aceptar cada invitación.
- En los atributos del usuario, para mitigar cualquier problema de alteración del disco de perfil de usuario (UPD) en usuarios invitados, en **Identificador de usuario**, seleccione siempre **user.mail**.

Dropbox Business

Para permitir que los usuarios inicien sesión con su cuenta de organización, es preciso configurar manualmente Dropbox Business para que use Azure AD como proveedor de identidades del lenguaje de marcado de aserción de seguridad (SAML). Si Dropbox Business no se ha configurado para ello, no puede solicitar o, en caso contrario, permitir a los usuarios que inicien sesión con Azure AD.

1. Para agregar la aplicación Dropbox Business a Azure AD, seleccione **Aplicaciones empresariales** en el panel izquierdo y, después, haga clic en **Agregar**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various icons. The main area is titled 'Enterprise applications'. At the top right, there's a large green circle highlighting the '+ Add' button. Below it, the text 'Total Apps' and the number '5' are displayed. To the right, there's a chart showing 'Top 3 Applications' and 'App usage between 12/24/2016 and Dec 25'. At the bottom, it says 'AZURE CLASSIC PORTAL' and '0 SIGN-INS'.

2. En la ventana Agregar una aplicación, escriba **dropbox** en el cuadro de búsqueda y seleccione **Dropbox for Business** en la lista de resultados.

The screenshot shows the 'Add an application' dialog. The search bar at the top contains 'dropbox'. Below it, a message says 'Search thousands of pre-configured applications, or add your own.' A list of results is shown, with '1 applications matched "dropbox". Choose one below or [add your own application.](#)' Below the list, there's a table with columns 'NAME' and 'CATEGORY'. One result is listed: 'Dropbox for Business' under 'Collaboration'.

3. En la página Inicio de sesión único, seleccione Inicio de sesión único en el panel izquierdo y, después, escriba **user.mail** en el cuadro Identificador de usuario (de manera predeterminada se establece como UPN).

DropBox1 - Single sign-on

Enterprise Application - PREVIEW

Save Discard

Search (Ctrl+ /)

Mode SAML-based Sign-on

Federated single sign-on enables rich and secure authentication to applications using the SAML protocol. Follow the steps below to connect Salesforce to Azure AD using SAML.

DropBox1 Domain and URLs
Input the URLs and other details about your DropBox1 tenant into Azure AD.

* Sign on URL: https://www.dropbox.com/sso/3438145437

* Identifier:

Show advanced URL settings

User Attributes
Edit the user information sent in the SAML token when user sign in to DropBox1.

User Identifier: user.mail

View and edit all other user attributes

SAML Signing Certificate
Manage the certificate used by Azure AD to sign SAML tokens issued to DropBox1.

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	1/19/2019	D714B3DCC4CF64AB6E68705C41E1CEA1813FE...	Certificate (Base64)
Create new certificate			

4. Para descargar el certificado que se va a usar para la configuración de Dropbox, seleccione **Configurar DropBoxy**, después, seleccione **SAML Single Sign On Service URL** (URL del servicio de inicio de sesión único de SAML) en la lista.

User Attributes
Edit the user information sent in the SAML token when user sign in to DropBox1.

User Identifier: user.mail

View and edit all other user attributes

SAML Signing Certificate
Manage the certificate used by Azure AD to sign SAML tokens issued to DropBox1.

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	1/19/2019	D714B3DCC4CF64AB6E68705C41E1CEA1813FE...	Certificate (Base64)
Create new certificate			

* Notification Email: ravikiran.netty@live.com

DropBox1 Configuration
DropBox1 must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

[Configure DropBox1](#)

1. Review the process for configuring SAML identity providers in Dropbox for Business. To determine the correct process, view the documentation for Dropbox for Business or contact your Dropbox for Business representative for more information.

2. Note: Some guidance on how to configure Dropbox for Business can be found on Azure.com, and we are in the process of migrating the application-specific steps to this guide. The older article on how to configure Dropbox for Business can be found here, where only the steps related to uploading the Azure AD files and URLs to Dropbox for Business need to be followed.

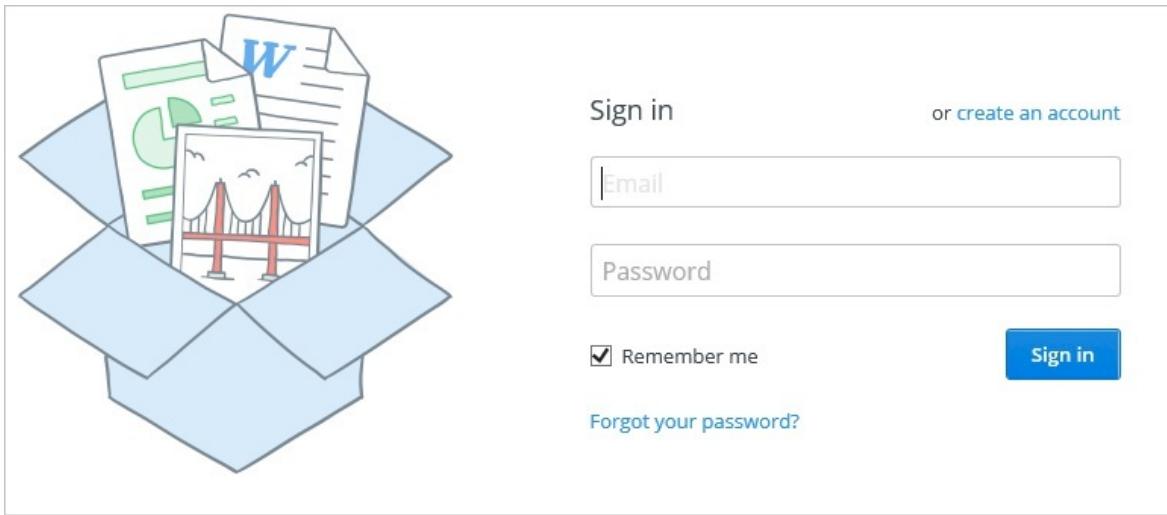
3. During this process, you will be prompted to provide files and URLs that correspond to Azure Active Directory. When prompted, use the files and URLs shown below:

- SAML Single Sign-On Service URL: https://login.microsoftonline.com/e64ac786-965b-4ebf-8e75-1addbf9543e7/saml2
- SAML Entity ID: https://sts.windows.net/e64ac786-965b-4ebf-8e75-1addbf9543e7/
- Sign-Out URL: https://login.microsoftonline.com/common/wsfedederation?wa=wsignout1.0
- SAML Signing Certificate - Base64 encoded
- SAML Signing Certificate - Raw
- SAML XML Metadata

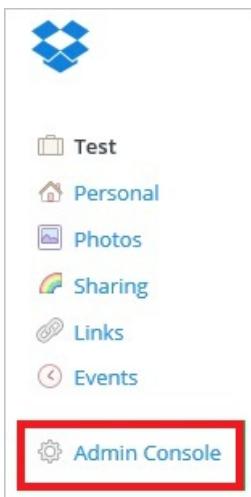
4. Once this information has been provided and configured in Dropbox for Business, Dropbox for Business will begin to require or otherwise allow users to sign in using your instance of Azure Active Directory.

Next steps
To ensure users can sign-in to Dropbox for Business after it has been configured to use Azure Active Directory, review the following tasks and topics:

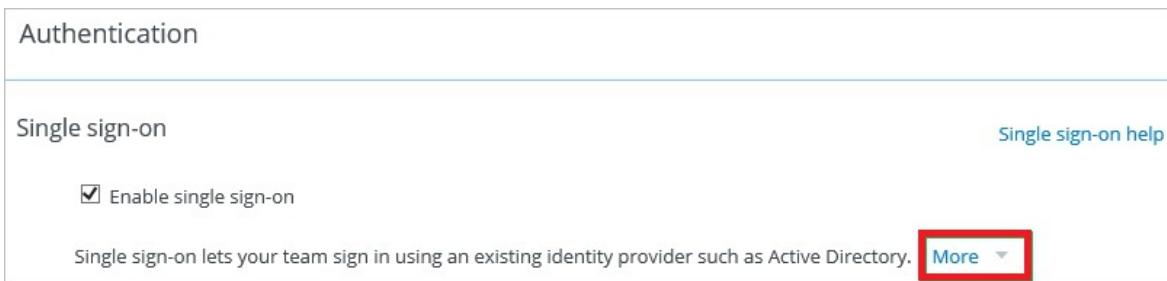
5. Inicie sesión en Dropbox con la URL de inicio de sesión desde la página **Inicio de sesión único**.



6. En el menú, seleccione Admin Console (Consola de administración).



7. En el cuadro de diálogo Authentication (Autenticación), seleccione More (Más), cargue el certificado y, después, en el cuadro Sign in URL (URL de inicio de sesión), escriba la URL de inicio de sesión único de SAML.



Authentication

Single sign-on

[Single sign-on help](#)

Enable single sign-on

Single sign-on lets your team sign in using an existing identity provider such as Active Directory. [Less](#) ▾

- Users can sign in by entering just their email address or they can go directly to <https://www.dropbox.com/sso/264030810>.
- Users' existing desktop and mobile clients will remain linked to their accounts.
- Dropbox two-step verification will be disabled when using single sign-on to avoid overlapping settings.
- Your identity provider may have a [pre-configured Dropbox application](#). If not, you may need to [configure it](#).
- When you first enable required mode, we'll send [this email](#) to notify users. In optional mode, you can use [this template](#) to manually tell users.

<input type="radio"/> Optional Ideal for testing your implementation. Users will be able to sign in with either their Dropbox or single sign-on credentials.	<input checked="" type="radio"/> Required Users will be required to sign in with their single sign-on credentials. Only admins can sign in with a Dropbox password.
--	---

Sign in URL [i](#)

X.509 certificate [i](#)

8. Para configurar la instalación automática del usuario en Azure Portal, seleccione **Aprovisionamiento** en el panel izquierdo, después **Automático** en el cuadro **Modo de aprovisionamiento** y, finalmente, seleccione **Autorizar**.

DropBox1 - Provisioning
Enterprise Application - PREVIEW

Save Discard

Search (Ctrl+ /)

Overview Quick start

MANAGE

Properties Users and groups Single sign-on Provisioning (highlighted)

Self-service Conditional access Permissions

ACTIVITY

Sign-ins Audit logs

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in DropBox1 based on user and group assignment.

Admin Credentials

Azure AD needs authorization to connect to DropBox1's API and synchronize user data.

Authorize (highlighted)

Test Connection

Notification Email: ravikiran.nety@live.com

Send an email notification when a failure occurs

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and Dropbox.

NAME	ENABLED
Synchronize Azure Active Directory Users to Dropbox	Yes

Restore default mappings

Settings

Start and stop provisioning to DropBox1, and view provisioning status.

Provisioning Status: On (highlighted)

Clear current state and restart synchronization

Synchronization Details

Summary

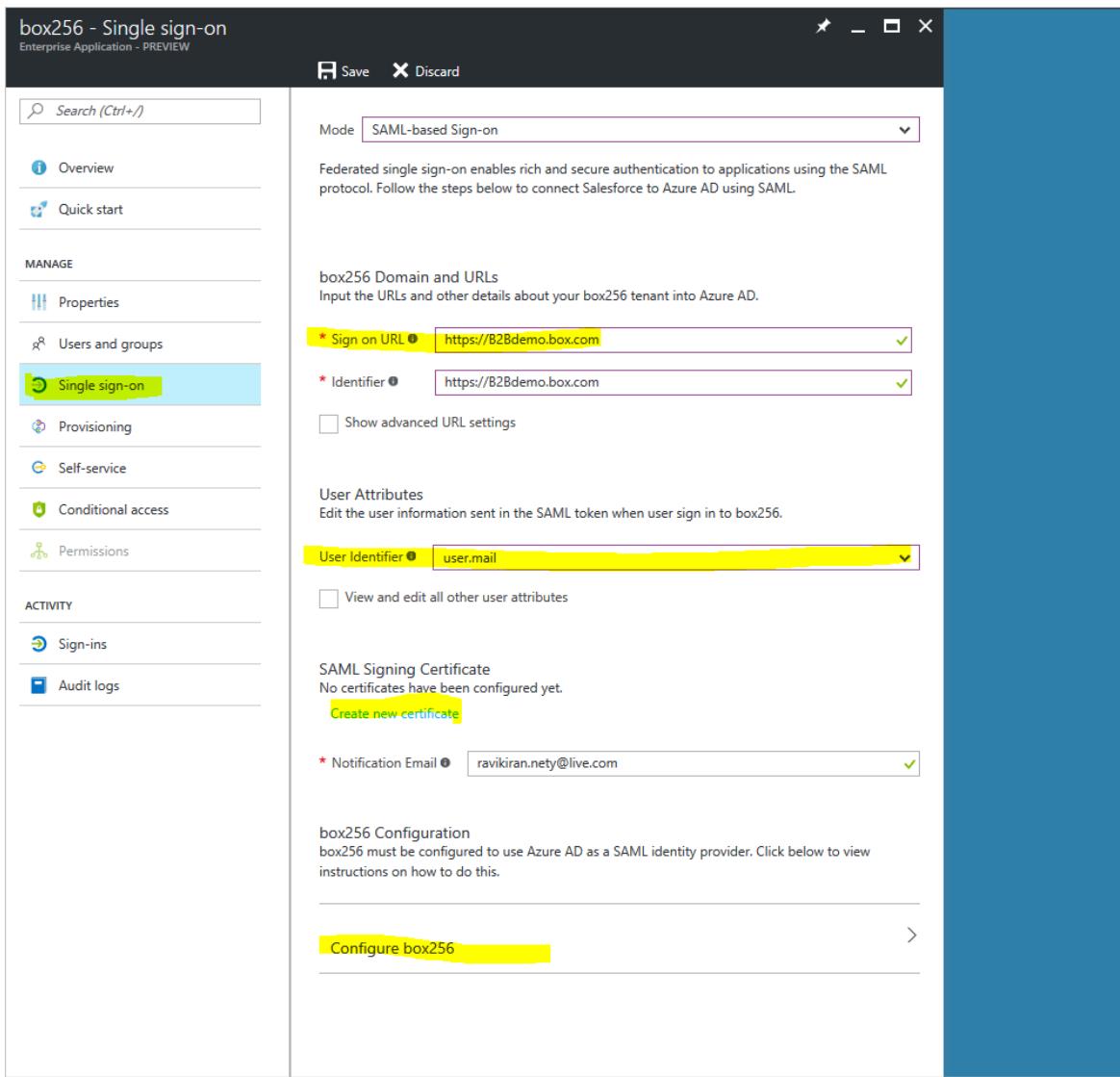
We have synchronized 7 object(s) of type User to User.
Synchronization was last run on Mon Jan 23 2017 09:23:37 GMT-0800 (Pacific Standard Time)
Most recent full synchronization was completed Mon Jan 23 2017 09:23:37 GMT-0800 (Pacific Standard Time)
We completed the first full synchronization on Tue Jan 17 2017 20:00:05 GMT-0800 (Pacific Standard Time)

Una vez que los usuarios miembros o invitados se hayan configurado en la aplicación de Dropbox, reciben una invitación independiente de Dropbox. Para usar el inicio de sesión único de Dropbox, los invitados deben aceptar dicha invitación haciendo clic en un vínculo de ella.

Box

Puede permitir que los usuarios autentiquen usuarios invitados de Box con su cuenta de Azure AD mediante el uso de una federación basada en el protocolo SAML. En este procedimiento, se cargan metadatos en Box.com.

1. Agregue la aplicación Box desde las aplicaciones empresariales.
2. Configure el inicio de sesión único en el orden siguiente:



- a. En el cuadro **URL de inicio de sesión**, asegúrese de que la dirección URL de inicio de sesión se ha establecido correctamente para Box en Azure Portal. Esta es la dirección URL de su inquilino de Box.com. Debe seguir la convención de nomenclatura <https://box.com>.
Identificador no se aplica a esta aplicación, pero sigue apareciendo como campo obligatorio.
 - b. En el cuadro **Identificador de usuario**, escriba **user.mail** (para el SSO de las cuentas de invitado).
 - c. En **Certificado de firma de SAML**, haga clic en **Crear nuevo certificado**.
 - d. Para empezar a configurar el inquilino de Box.com para que use Azure AD como proveedor de identidades, descargue el archivo de metadatos y guárdelo en una unidad local.
 - e. Reenvíe el archivo de metadatos al equipo de soporte técnico de Box para que configuren el inicio de sesión único.
3. Para la instalación automática de usuarios de Azure AD, en el panel izquierdo, seleccione **Aprovisionamiento** y, después, **Autorizar**.

The screenshot shows the Azure AD Enterprise Application - PREVIEW interface. On the left, there's a navigation menu with options like Overview, Quick start, Properties, Users and groups, Single sign-on, Provisioning (which is selected and highlighted in blue), Self-service, Conditional access, Permissions, and Sign-ins. The main area has a heading 'Admin Credentials' and a note: 'Azure AD needs authorization to connect to box256's API and synchronize user data.' It contains fields for 'Admin Username', 'Admin Password', and 'appkey', along with a 'Test Connection' button and a checkbox for 'Send an email notification when a failure occurs'. A large yellow circle highlights the 'Authorize' button. Below this, another yellow circle highlights the 'Log in to grant access to Box' button on a separate screenshot of the Box login page.

Los invitados de Box deben canjear su invitación desde la aplicación de Box tal como lo hacen los de Dropbox.

Pasos siguientes

Consulte los siguientes artículos sobre la colaboración de B2B de Azure AD:

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Grupos dinámicos y colaboración B2B](#)
- [Asignación de notificaciones de usuario de colaboración B2B](#)
- [Uso compartido externo de Microsoft 365](#)

Conceder a las cuentas de asociado administradas localmente acceso a los recursos en la nube mediante la colaboración B2B de Azure AD

18/02/2021 • 5 minutes to read • [Edit Online](#)

Antes de Azure Active Directory (Azure AD), las organizaciones con sistemas de identidad locales han administrado tradicionalmente las cuentas de asociado en sus directorios locales. En este tipo de organización, cuando comienzan a moverse las aplicaciones a Azure AD, quiere tener la seguridad de que los asociados pueden acceder a los recursos que necesitan. No importa si los recursos se encuentran en el entorno local o en la nube. Además, quiere que los usuarios asociados puedan usar las mismas credenciales de inicio de sesión tanto para los recursos locales como para los de Azure AD.

Si crea cuentas para los asociados externos en el directorio local (por ejemplo, crea una cuenta con un nombre de inicio de sesión de "wmoran" para un usuario externo llamado Wendy Moran en el dominio partners.contoso.com), ahora puede sincronizarlas con la nube. En concreto, puede usar Azure AD Connect para sincronizar las cuentas de asociados con la nube, lo que crea una cuenta de usuario con UserType = Guest. De esta manera, los usuarios asociados pueden acceder a los recursos en la nube con las mismas credenciales que las de sus cuentas locales, sin concederles más acceso del que necesitan.

NOTE

Consulte también [Invitación de usuarios internos a la colaboración B2B](#). Con esta característica, puede proponer a los usuarios internos invitados que usen la colaboración B2B, independientemente de si se han sincronizado sus cuentas del directorio local con la nube. Una vez que los usuarios aceptan la invitación para usar la colaboración B2B, pueden usar su propia identidad y credenciales para iniciar sesión en los recursos a los que se les da acceso. Ya no tendrá que mantener contraseñas ni administrar los ciclos de vida de la cuenta.

Identificación de atributos únicos para UserType

Antes de permitir la sincronización del atributo UserType, primero debe decidir cómo obtener el atributo UserType de Active Directory local. En otras palabras, ¿qué parámetros del entorno local son únicos para los colaboradores externos? Determine un parámetro que distinga estos colaboradores externos de los miembros de su propia organización.

Los dos enfoques comunes para ello son los siguientes:

- Designe un atributo de Active Directory local sin usar (por ejemplo, Atributodeextensión1) que se usará como el atributo de origen.
- Como alternativa, obtenga el valor del atributo UserType de otras propiedades. Por ejemplo, querrá sincronizar todos los usuarios como Invitado si su atributo UserPrincipalName de Active Directory local finaliza con el dominio `@partners.contoso.com`.

Para conocer los requisitos detallados de atributos, consulte [Habilitar la sincronización de UserType](#).

Configuración de Azure AD Connect para sincronizar los usuarios con la nube

Después de identificar el atributo único, puede configurar Azure AD Connect para sincronizar estos usuarios con

la nube, lo que crea cuentas de usuario con UserType = Guest. Desde un punto de vista de autorización, estos usuarios no se distinguen de los usuarios B2B creados mediante el proceso de invitación a la colaboración B2B de Azure AD.

Para obtener instrucciones de implementación, consulte [Habilitar la sincronización de UserType](#).

Pasos siguientes

- [Colaboración B2B de Azure Active Directory para organizaciones híbridas](#)
- [Conceder a los usuarios B2B de Azure AD acceso a las aplicaciones locales](#)
- Para información general sobre Azure AD Connect, consulte [Integración de los directorios locales con Azure Active Directory](#).

Conceder a los usuarios B2B de Azure AD acceso a las aplicaciones locales

18/02/2021 • 10 minutes to read • [Edit Online](#)

Las organizaciones que usan las funcionalidades de colaboración B2B de Azure Active Directory (Azure AD) para invitar a los usuarios invitados de organizaciones asociadas a su instancia de Azure AD, ahora pueden proporcionar a estos usuarios B2B acceso a las aplicaciones locales. Estas aplicaciones locales pueden usar la autenticación basada en SAML o la autenticación de Windows integrada (IWA) con la delegación limitada de kerberos (KCD).

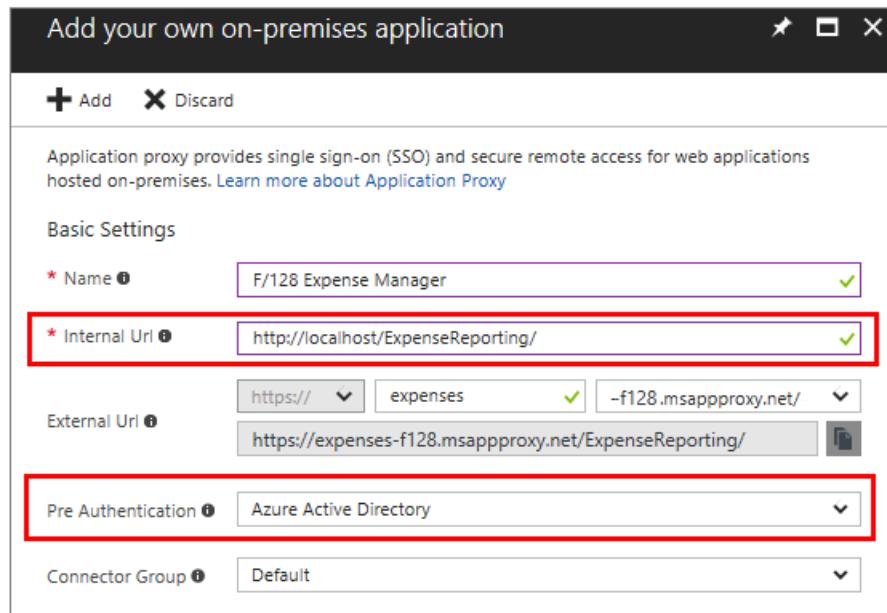
Acceso a las aplicaciones SAML

Si la aplicación local usa la autenticación basada en SAML, estas aplicaciones pueden estar fácilmente disponibles para los usuarios de colaboración B2B de Azure AD mediante Azure Portal.

Deberá realizar las dos acciones siguientes:

- Integre la aplicación mediante SAML tal y como se describe en [Configuración del inicio de sesión único basado en SAML](#). Asegúrese de anotar el valor que usa para la dirección URL de inicio de sesión.
- Use Azure AD Application Proxy para publicar la aplicación local y tenga configurado **Azure Active Directory** como origen de autenticación. Para instrucciones, consulte [Publicación de aplicaciones mediante Azure AD Application Proxy](#).

Al configurar la **dirección URL interna**, use la dirección URL de inicio de sesión que especificó en la plantilla de aplicación que no es de la galería. De esta manera, los usuarios pueden acceder a la aplicación desde fuera de los límites de la organización. Application Proxy realiza el inicio de sesión único de SAML de la aplicación local.



Acceso a aplicaciones IWA y KCD

Para proporcionar a los usuarios B2B acceso a las aplicaciones locales que están protegidas con la autenticación integrada de Windows y la delegación restringida de Kerberos, necesita los siguientes componentes:

- **Autenticación mediante Azure AD Application Proxy.** Los usuarios B2B deben poder autenticarse en la aplicación local. Para ello, debe publicar la aplicación local a través de Azure AD Application Proxy. Para más información, consulte el [Tutorial: Adición de una aplicación local para el acceso remoto mediante Application Proxy](#).
- **Autorización mediante un objeto de usuario B2B en el directorio local.** La aplicación debe poder realizar comprobaciones de acceso de usuario y conceder acceso a los recursos correctos. IWA y KCD requieren un objeto de usuario en Windows Server Active Directory local para realizar esta autorización. Como se describe en [Cómo funciona el inicio de sesión único con KCD](#), Application Proxy necesita este objeto de usuario para suplantar al usuario y obtener un token de Kerberos para la aplicación.

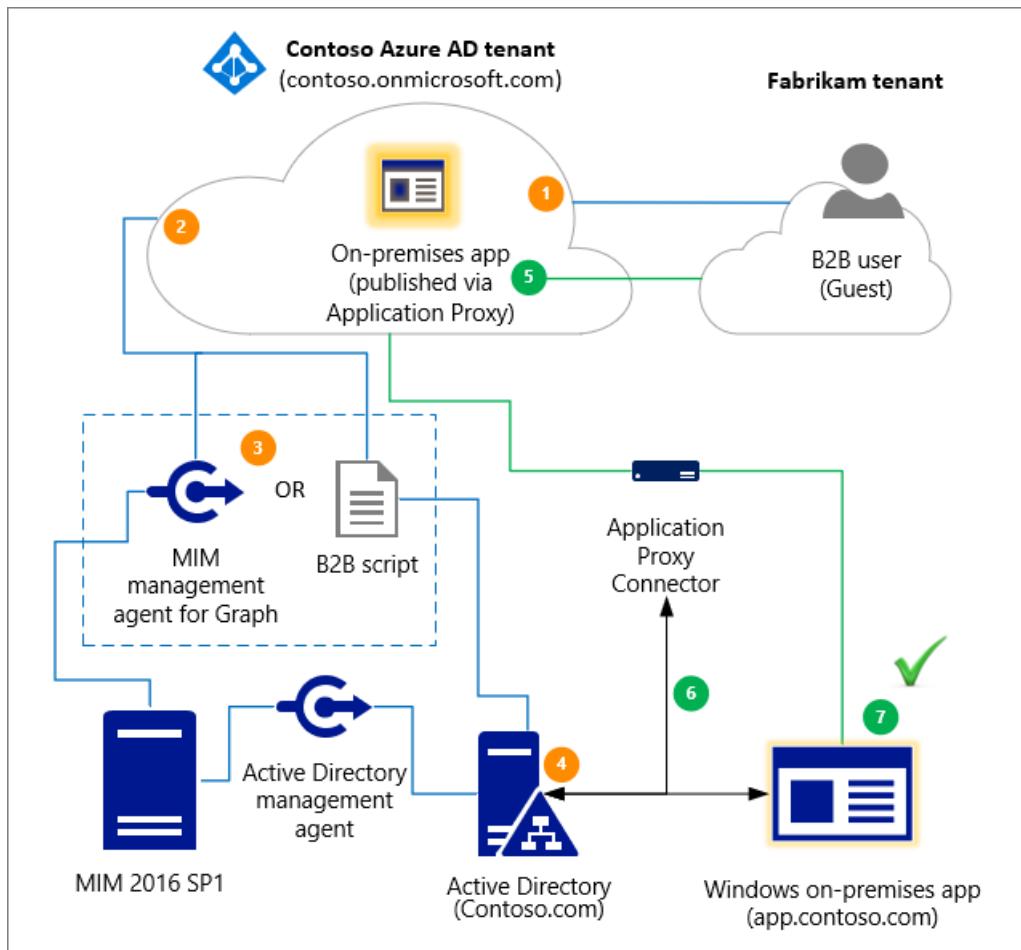
NOTE

Al configurar Application Proxy de Azure AD, asegúrese de que la opción **Identidad de inicio de sesión delegada** esté establecida en **Nombre principal del usuario** (valor predeterminado) en la configuración de Autenticación integrada de Windows (IWA).

En el escenario de usuario B2B, hay dos métodos disponibles que se pueden usar para crear los objetos de usuario invitado que son necesarios para la autorización en el directorio local:

- Microsoft Identity Manager (MIM) y el agente de administración de MIM para Microsoft Graph.
- [Un script de PowerShell](#). El uso del script es una solución más ligera que no requiere MIM.

En el siguiente diagrama se proporciona información general de alto nivel de cómo funcionan juntos Azure AD Application Proxy y la generación del objeto de usuario B2B en el directorio local para conceder a los usuarios B2B acceso a sus aplicaciones locales IWA y KCD. Los pasos numerados se describen en detalle más adelante en el diagrama.



1. Se invita a un usuario de una organización asociada (el inquilino de Fabrikam) al inquilino de Contoso.

2. Se crea un objeto de usuario invitado en el inquilino de Contoso (por ejemplo, un objeto de usuario con un UPN de guest_fabrikam.com#EXT#@contoso.onmicrosoft.com).
3. El invitado de Fabrikam se importa desde Contoso mediante MIM o el script de PowerShell para B2B.
4. Se crea una representación o "huella" del objeto de usuario invitado de Fabrikam (Guest#EXT#) en el directorio local, Contoso.com, mediante MIM o el script de PowerShell para B2B.
5. El usuario invitado accede a la aplicación local, app.contoso.com.
6. La solicitud de autenticación se autoriza mediante Application Proxy, por medio de la delegación restringida de Kerberos.
7. Dado que el objeto de usuario invitado existe localmente, la autenticación se realiza correctamente.

Directivas de administración del ciclo de vida

Puede administrar los objetos de usuario B2B locales mediante directivas de administración del ciclo de vida.

Por ejemplo:

- Puede configurar directivas de autenticación multifactor (MFA) para el usuario invitado para usar MFA durante la autenticación de Application Proxy. Para más información, consulte [Acceso condicional para usuarios de colaboración B2B](#).
- Cualquier patrocinio, revisión de acceso, verificación de cuenta, etc. que se realice sobre el usuario B2B en la nube se aplica a los usuarios locales. Por ejemplo, si se elimina el usuario en la nube mediante las directivas de administración del ciclo de vida, también se elimina el usuario local mediante la sincronización MIM o la sincronización de Azure AD Connect. Para más información, consulte [Administración del acceso de los invitados con las revisiones de acceso de Azure AD](#).

Creación de objetos de usuario invitado B2B mediante MIM

Si necesita información acerca de cómo usar MIM 2016 Service Pack 1 y el agente de administración de MIM para Microsoft Graph a fin de crear los objetos del usuario invitado en el directorio local, consulte [Colaboración de negocio a negocio \(B2B\) de Azure AD con Microsoft Identity Manager\(MIM\) 2016 SP1 con el proxy de aplicación de Azure](#).

Creación de objetos de usuario invitado B2B mediante un script (versión preliminar)

Hay un script de ejemplo de PowerShell que puede usar como punto de partida para crear los objetos de usuario invitado en su instancia local de Active Directory.

Puede descargar el script y el archivo Léame en [Conectores para Microsoft Identity Manager 2016 y Forefront Identity Manager 2010 R2](#). En el paquete de descarga, elija el archivo **Script and Readme to pull Azure AD B2B users on-prem.zip**.

Antes de usar el script, asegúrese de revisar los requisitos previos y las consideraciones importantes en el archivo Léame asociado. Además, debe saber que el script solo está disponible como ejemplo. El equipo de desarrollo o el asociado deben personalizar y revisar el script antes de que lo ejecuten los usuarios.

Consideraciones sobre licencias

Asegúrese de que dispone de las licencias de acceso cliente (CAL) correctas para los usuarios invitados externos que acceden a las aplicaciones locales. Para más información, consulte la sección "External Connector" de [Licencias de acceso de cliente y licencias de administración](#). Hable con su representante o distribuidor local de Microsoft para informarse sobre sus necesidades concretas de licencia.

Pasos siguientes

- [Colaboración B2B de Azure Active Directory para organizaciones híbridas](#)
- Para información general sobre Azure AD Connect, consulte [Integración de los directorios locales con Azure Active Directory](#).

Salir de una organización como usuario invitado

18/02/2021 • 4 minutes to read • [Edit Online](#)

Es posible que un usuario invitado de Azure Active Directory (Azure AD) B2B decida salir de una organización en cualquier momento si ya no necesita usar las aplicaciones de dicha organización ni mantener ninguna asociación. Un usuario puede salir de una organización por su cuenta, sin ponerse en contacto con un administrador.

NOTE

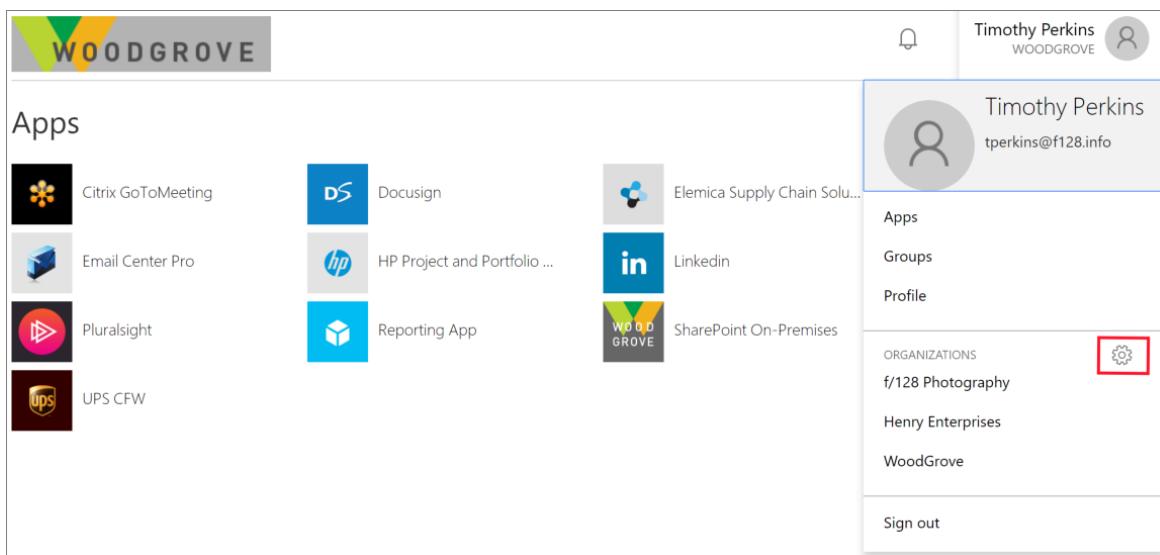
Un usuario invitado no puede abandonar una organización si su cuenta está deshabilitada en el inquilino principal o el inquilino del recurso. Si su cuenta está deshabilitada, el usuario invitado debe ponerse en contacto con el administrador de inquilinos, que puede eliminar la cuenta de invitado o habilitar la cuenta de invitado para que el usuario pueda abandonar la organización.

Salir de una organización

Para salir de una organización, siga estos pasos.

1. Siga uno de estos pasos para ir a la página Perfil del Panel de acceso:

- En [Azure Portal](#), haga clic en su nombre en la esquina superior derecha y seleccione **Ver cuenta**.
- Abra su [Panel de acceso](#), haga clic en su nombre en la esquina superior derecha y, junto a **Organizaciones**, seleccione el icono de configuración (engranaje).



NOTE

Si aún no ha iniciado sesión en la organización de la que quiere salir, en **Organizaciones**, haga clic en el vínculo **Inicie sesión para salir de la organización** situado junto al nombre de la organización. Después de iniciar sesión, vuelva a hacer clic en su nombre en la esquina superior derecha y, junto a **Organizaciones**, seleccione el icono de configuración (engranaje).

2. En **Organizaciones**, busque la organización que quiere abandonar y seleccione **Salir de la organización**.

3. Cuando se le pida que confirme, seleccione Salir.

Eliminar cuenta

Cuando un usuario sale de una organización, la cuenta de usuario se "elimina temporalmente" en el directorio. De forma predeterminada, el objeto de usuario se mueve al área **Usuarios eliminados** en Azure AD, pero no se elimina permanentemente durante 30 días. Esta eliminación temporal permite que el administrador restaure la cuenta de usuario (incluidos los grupos y permisos) si el usuario lo solicita en el plazo de 30 días.

Si lo desea, un administrador de inquilinos puede eliminar permanentemente la cuenta en cualquier momento durante el período de 30 días. Para ello, siga estos pasos:

1. En [Azure Portal](#), seleccione **Azure Active Directory**.
2. En **Administrar**, seleccione **Usuarios**.
3. Seleccione **Usuarios eliminados**.
4. Active la casilla de verificación situada junto a un usuario eliminado y, luego, seleccione **Eliminar de forma permanente**.

Si elimina permanentemente un usuario, esta acción es irrevocable.

NOTE

Para más información sobre cómo ver o eliminar datos personales, consulte [Solicitudes de interesados de datos de Azure para el RGPD](#). Para más información sobre el Reglamento general de protección de datos, consulte la [sección sobre RGPD del Portal de confianza de servicios](#).

Pasos siguientes

- Para información general sobre B2B de Azure AD, consulte [¿Qué es la colaboración B2B de Azure AD?](#)

Auditoría y generación de informes para usuarios de colaboración 2B

18/02/2021 • 2 minutes to read • [Edit Online](#)

Con usuarios invitados, cuenta con funcionalidades de auditoría similares a las que tiene con los usuarios miembros.

Revisiones de acceso

Puede utilizar revisiones de acceso para comprobar periódicamente si los usuarios invitados necesitan todavía acceso a los recursos. La característica **Revisiones de acceso** está disponible en **Azure Active Directory** en **External Identities > Revisiones de acceso**. También puede buscar "revisiones de acceso" en **Todos los servicios** en Azure Portal. Para aprender a usar las revisiones de acceso, consulte [Administración del acceso de los invitados con las revisiones de acceso de Azure AD](#).

Registros de auditoría

Los registros de auditoría de Azure AD proporcionan registros de las actividades del sistema y de los usuarios, incluidas las actividades iniciadas por los usuarios invitados. Para acceder a los registros de auditoría, en **Azure Active Directory**, en **Supervisión**, seleccione **Registros de auditoría**. A continuación, se muestra un ejemplo del historial de canje e invitación de los usuario Sam Oogle al que se acaba de invitar:

The screenshot shows the 'Audit logs' section for user 'Sam Oogle - Audit logs'. The left sidebar includes links for Overview, Manage (Profile, Directory role, Groups, Licenses, Devices, Azure resources), and Activity (Sign-ins, Audit logs). The 'Audit logs' link is highlighted. The main area displays a table of audit log entries with columns: DATE, ACTOR, ACTIVITY, and TARGET(S). The table lists 18 entries from January 23, 2017, at 5:09:05 AM, showing various update events for the user, such as 'Update user' and 'Add user'.

DATE	ACTOR	ACTIVITY	TARGET(S)
1/23/2017, 5:09:05 AM	Microsoft Invitation Acceptance Portal	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:02:03 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:02:01 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:59 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:57 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:54 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:52 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:50 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:48 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:45 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:43 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:40 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:38 AM	JDoe@WoodGroveOnline.com	Update user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...
1/23/2017, 5:01:37 AM	JDoe@WoodGroveOnline.com	Add user	User : gsamoogle_gmail.com#EXT#@WoodGroveAzureAD.onmic...

Puede profundizar en cada uno de estos eventos para obtener los detalles. Por ejemplo, echemos un vistazo a los detalles de aceptación.

Activity Details: Audit log

PREVIEW

TARGET(S)	Activity
User : gsamoole_gmail.com#EXT...	Date : 1/23/2017, 5:09:05 AM Name : Update user CorrelationId : 102653e0-3806-48a2-a5f6-b28d4041b9f3
User : gsamoole_gmail.com#EXT...	Activity Status Status : N/A Reason : N/A
User : gsamoole_gmail.com#EXT...	Actor Type : Application Name : Microsoft Invitation Acceptance Portal Objectld : 0f91fa9a-7e52-4331-9713-5332b5df1f37 Spn : 4660504c-45b3-4674-a709-71951a6b0763
User : gsamoole_gmail.com#EXT...	Target(s) Target Type : User Objectld : a7bb2cfa-8e04-4108-9662-e89ef64fff61 Upn : gsamoole_gmail.com#EXT#@WoodGroveAzureAD.onmicrosoft.com
User : gsamoole_gmail.com#EXT...	Modified Properties Name : AcceptedAs Old Value : [] New Value : [gsamoole@gmail.com]; Name : AcceptedOn Old Value : [] New Value : [2017-01-23T13:09:05Z]; Name : AlternativeSecurityId Old Value : [] New Value : [[Type=1,IdentityProvider=,Key=AAN//gK4uO4=]]; Name : UserState Old Value : [PendingAcceptance] New Value : [Accepted]; Name : UserStateChangedOn Old Value : [2017-01-23T13:01:37Z] New Value : [2017-01-23T13:09:05Z];

También puede exportar estos registros de Azure AD y utilizar la herramienta de informes que prefiera para obtener informes personalizados.

Pasos siguientes

- [Propiedades de usuario de la colaboración B2B](#)

Solución de problemas de colaboración B2B de Azure Active Directory

18/02/2021 • 13 minutes to read • [Edit Online](#)

Estos son algunos de los recursos para solucionar problemas comunes relacionados con la colaboración B2B de Azure Active Directory (Azure AD).

IMPORTANT

- A partir del 4 de enero de 2021, Google [retira la compatibilidad con el inicio de sesión en WebView](#). Si usa Google Federation o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).
- A partir del 31 de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

He agregado un usuario externo, pero no lo veo en mi libreta de direcciones global o en el selector de personas

En los casos donde los usuarios externos no se rellenan en la lista, el objeto puede tardar unos minutos en replicarse.

Un usuario invitado de B2B no aparece en el selector de personas de SharePoint Online/OneDrive

La posibilidad de buscar usuarios invitados existentes en el selector de personas de SharePoint Online (SPO) está desactivada de manera predeterminada para así coincidir con el comportamiento heredado.

Para habilitarla, use la configuración "ShowPeoplePickerSuggestionsForGuestUsers" en el nivel de inquilino y colección de sitios. Para configurarla, use los cmdlets Set-SPOTenant y Set-SPOSite, que permiten que los miembros busquen a todos los usuarios invitados existentes en el directorio. Los cambios en el ámbito del inquilino no afectan los sitios de SPO que ya se aprovisionaron.

Las invitaciones se han deshabilitado para el directorio

Si recibe una notificación de que no tiene permisos para invitar a usuarios, vaya a Azure Active Directory > Configuración de usuario > Usuarios externos > Administrar la configuración de la colaboración externa y compruebe que la cuenta de usuario está autorizada para invitar a usuarios externos.

External Users

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

Si hace poco ha modificado estos valores o asignado el rol de invitador invitado a un usuario, podría haber un retraso de 15 a 60 minutos para que los cambios surtan efecto.

El usuario al que he invitado está recibiendo un error durante el canje

Estos son algunos de los errores comunes:

El administrador del invitado no permite que los usuarios de EmailVerified se creen en su inquilino

Cuando se invita a usuarios cuya organización usa Azure Active Directory, pero donde no existe la cuenta de usuario en concreto (por ejemplo, el usuario no existe en Azure AD contoso.com). El administrador de contoso.com puede tener una directiva en lugar de evitar que se creen usuarios. El usuario debe consultar al administrador y determinar si se permiten los usuarios externos. Es posible que el administrador del usuario externo necesite permitir usuarios comprobados por correo electrónico en el dominio (consulte este [artículo](#) sobre cómo permitir usuarios comprobados por correo electrónico).

Set up your account with Microsoft

Check your email for your verification code. Didn't get the email? Check your Junk folder or [try again](#).

985684

Note: when you use a work or school email address to set up an account with Microsoft, your IT department may later control your data and restrict what you can do with your account.

By clicking **Finish** you agree to the [Privacy Statement](#) and [Microsoft Services Agreement](#).

Finish

This tenant does not allow email verified users to be added due to an admin-defined policy. Contact the person who invited you to report the error.

El usuario externo no se encuentra ya en un dominio federado

Si va a usar la autenticación de federación y el usuario no existe en Azure Active Directory, no se puede invitar al usuario.

Para resolver este problema, el administrador del usuario externo debe sincronizar la cuenta del usuario con Azure Active Directory.

¿Cómo "#", que habitualmente no es un carácter válido, se sincroniza con Azure AD?

"#" es un carácter reservado en los UPN para la colaboración B2B de Azure AD o los usuarios externos, porque la cuenta de invitado user@contoso.com se convierte en user_contoso.com#EXT#@fabrikam.onmicrosoft.com. Por lo tanto, los UPN con # que proceden del entorno local no tienen permiso para iniciar sesión en Azure Portal.

Recibo un error al agregar los usuarios externos a un grupo sincronizado

Los usuarios externos pueden agregarse únicamente a los grupos "Seguridad" o "Asignado", y no a aquellos que se controlan localmente.

Mi usuario externo no ha recibido un correo electrónico para realizar el canje

El invitado debe ponerse en contacto con su ISP o comprobar su filtro de correo no deseado para asegurarse de que se permite la siguiente dirección: Invites@microsoft.com

Tenga en cuenta que, en ocasiones, el mensaje personalizado no se incluye en los mensajes de invitación

Para cumplir con las leyes de privacidad, nuestras API no incluye mensajes personalizados en la invitación por correo electrónico cuando:

- El invitador no tiene una dirección de correo electrónico en el inquilino que invita.
- Cuando una entidad de seguridad de App Service envía la invitación

Si este escenario es importante para usted, puede suprimir nuestro correo electrónico de invitación de API y enviarlo a través del mecanismo de correo electrónico de su elección. Consulte al asesor legal de su organización para asegurarse de que cualquier correo electrónico que envíe de esta forma también cumple las leyes de privacidad.

Se produce un error "AADSTS65005" al intentar iniciar sesión en un recurso de Azure

Un usuario con una cuenta de invitado no puede iniciar sesión y recibe el mensaje de error siguiente:

```
AADSTS65005: Using application 'AppName' is currently not supported for your organization contoso.com because it is in an unmanaged state. An administrator needs to claim ownership of the company by DNS validation of contoso.com before the application AppName can be provisioned.
```

El usuario tiene una cuenta de usuario de Azure y es un inquilino viral no administrado o que se ha abandonado. Además, no hay administradores globales en el inquilino.

Para resolver este problema, debe asumir el inquilino abandonado. Consulte [Adquisición de un directorio no administrado como administrador en Azure Active Directory](#). También debe tener acceso al DNS accesible desde Internet para el sufijo de dominio en cuestión con el fin de proporcionar pruebas directas de que controla el espacio de nombres. Después de que el inquilino se devuelva a un estado administrado, hable con el cliente para ver si abandonar a los usuarios y al nombre de dominio comprobado es la mejor opción para su organización.

Un usuario invitado con un inquilino Just-In-Time o "viral" no puede restablecer su contraseña

Si el inquilino de la identidad es un inquilino Just-In-Time (JIT) o un inquilino "viral" (es decir, un inquilino de Azure que es independiente y no está administrado), solamente el usuario invitado podrá restablecer su contraseña. A veces, una organización [asumirá la administración de los inquilinos virales](#) que se crean cuando los empleados usan sus direcciones de correo electrónico del trabajo para registrarse en los servicios. Después de que la organización se haga cargo de un inquilino viral, solo un administrador de dicha organización puede restablecer la contraseña del usuario o habilitar SSPR. Si es necesario, como la organización que invita, puede quitar la cuenta del usuario invitado del directorio y volver a enviar una invitación.

Un usuario invitado no puede usar el módulo de PowerShell v1 de Azure AD.

A partir del 18 de noviembre de 2019, los usuarios invitados del directorio (definidos como cuentas de usuario en las que la propiedad **userType** es igual a **Invitado**) no pueden usar el módulo de PowerShell v1 de Azure AD. En el futuro, un usuario deberá ser un usuario miembro (aquellos en los que **userType** es igual a **Miembro**) o usar el módulo de PowerShell V2 de Azure AD.

En un inquilino de Azure Gobierno de EE. UU., no se puede invitar a un usuario invitado de colaboración B2B

Dentro de la nube de Azure Gobierno de EE. UU., la colaboración B2B solo se admite actualmente entre los inquilinos que se encuentran ambos dentro de la nube de Azure Gobierno de EE. UU. y que admiten ambos la colaboración B2B. Si invita a un usuario de un inquilino que no forma parte de la nube de Azure Gobierno de EE. UU. o que todavía no admite la colaboración B2B, se producirá un error. Para más información sobre limitaciones, consulte las [variaciones P1 y P2 de Azure Active Directory Premium](#).

Aparece un error que indica que Azure AD no puede encontrar la aplicación aad-extensions-app en mi inquilino

Al usar las características de registro de autoservicio, como los flujos de usuario o los atributos de usuario personalizados, se crea automáticamente una aplicación llamada

`aad-extensions-app. Do not modify. Used by AAD for storing user data.`. Lo utilizan las identidades externas de Azure AD para almacenar información acerca de los usuarios que se registran y los atributos personalizados recopilados.

Si ha eliminado la aplicación `aad-extensions-app` accidentalmente, tiene 30 días para recuperarla. Puede restaurar la aplicación mediante el módulo de PowerShell de Azure AD.

1. Inicie el módulo de PowerShell de Azure AD y ejecute `Connect-AzureAD`.
2. Inicie sesión como administrador global del inquilino de Azure AD para el que desea restaurar la aplicación eliminada.
3. Ejecute el comando de PowerShell `Get-AzureADDeletedApplication`.
4. Busque la aplicación en la lista cuyo nombre para mostrar comienza por `aad-extensions-app` y copie el valor de la propiedad `ObjectId`.
5. Ejecute el comando de PowerShell `Restore-AzureADDeletedApplication -ObjectId {id}`. Reemplace la parte `{id}` del comando por el valor de `ObjectId` del paso anterior.

Ahora debería ver la aplicación restaurada en Azure Portal.

Pasos siguientes

Obtención de soporte técnico para la colaboración B2B

Personalización y API de colaboración B2B de Active Directory Azure

18/02/2021 • 5 minutes to read • [Edit Online](#)

Hemos tenido muchos clientes que nos han dicho que querían personalizar el proceso de invitación de una forma que se adapte menor a sus organizaciones. Con nuestra API, pueden hacer justamente eso.

<https://developer.microsoft.com/graph/docs/api-reference/v1.0/resources/invitation>

Funcionalidades de la API de invitación

La API ofrece las siguientes funcionalidades:

1. Invite a un usuario externo con *cualquier* dirección de correo electrónico.

```
"invitedUserDisplayName": "Sam"  
"invitedUserEmailAddress": "gsamoogle@gmail.com"
```

2. Personalice a qué página desea que lleguen los usuarios finales después de aceptar la invitación.

```
"inviteRedirectUrl": "https://myapps.microsoft.com/"
```

3. Seleccione enviar el correo electrónico de invitación estándar por medio de nosotros

```
"sendInvitationMessage": true
```

con un mensaje al destinatario que pueda personalizar.

```
"customizedMessageBody": "Hello Sam, let's collaborate!"
```

4. Luego, ponga en copia a los usuarios a los que informar de que ha invitado a este colaborador.

5. También puede personalizar completamente su invitación y el flujo de trabajo de incorporación decidiendo no enviar notificaciones a través de Azure AD.

```
"sendInvitationMessage": false
```

En este caso, obtendrá una URL de canje a través de la API, que puede incrustar en una plantilla de correo electrónico, mensaje instantáneo u otro método de distribución que prefiera.

6. Finalmente, si es administrador, puede invitar al usuario como miembro.

```
"invitedUserType": "Member"
```

Determinación de si ya se invitó a un usuario a su directorio

Puede usar la API de invitación para determinar si ya existe un usuario en el inquilino de recursos. Esto puede ser útil cuando está desarrollando una aplicación que usa la API de invitación para invitar a un usuario. Si el

usuario ya existe en el directorio de recursos, no recibirá una invitación, por lo que puede ejecutar primero una consulta para determinar si el correo electrónico ya existe como nombre principal de usuario u otra propiedad de inicio de sesión.

1. Asegúrese de que el dominio de correo electrónico del usuario no forma parte del dominio comprobado del inquilino de recursos.
2. En el inquilino de recursos, use la consulta get user siguiente, donde {0} es la dirección de correo electrónico a la que va a invitar:

```
"userPrincipalName eq '{0}' or mail eq '{0}' or proxyAddresses/any(x:x eq 'SMTP:{0}') or signInNames/any(x:x eq '{0}') or otherMails/any(x:x eq '{0}')"
```

Modelo de autorización

La API se puede ejecutar en los siguientes modos de autorización:

Aplicación y modo de usuario

En este modo, el usuario que usa la API debe tener los permisos necesarios para crear invitaciones de B2B.

Modo de solo aplicación

En el contexto de solo aplicación, la aplicación necesita el ámbito User.Invite.All para que la invitación se realice correctamente.

Para más información, consulte: https://developer.microsoft.com/graph/docs/authorization/permission_scopes

PowerShell

Puede usar PowerShell para agregar e invitar a usuarios externos a una organización fácilmente. Cree una nueva invitación mediante el cmdlet:

```
New-AzureADMSInvitation
```

Puede utilizar las siguientes opciones:

- -InvitedUserDisplayName
- -InvitedUserEmailAddress
- -SendInvitationMessage
- -InvitedUserMessageInfo

Estado de la invitación

Después de enviar una invitación a un usuario externo, puede usar el cmdlet **Get-AzureADUser** para ver si ya la ha aceptado. Cuando se envía una invitación a un usuario externo, se rellenan las propiedades siguientes de **Get-AzureADUser**:

- **UserState** indica si la invitación está en el estado **PendingAcceptance** o **Accepted**.
- **UserStateChangedOn** muestra la marca de tiempo del cambio más reciente de la propiedad **UserState**.

Puede usar la opción **Filter** para filtrar los resultados por **UserState**. En el ejemplo siguiente se muestra cómo filtrar resultados para mostrar solo a los usuarios que tienen una invitación pendiente. En el ejemplo también se muestra la opción **Format-List**, que le permite especificar las propiedades que se van a mostrar.

```
Get-AzureADUser -Filter "UserState eq 'PendingAcceptance'" | Format-List -Property  
DisplayName,UserPrincipalName,UserState,UserStateChangedOn
```

NOTE

Asegúrese de que tiene la versión más reciente del módulo de AzureAD PowerShell o del módulo AzureADPreview PowerShell.

Consulte también

Consulte la referencia de API de invitación en <https://developer.microsoft.com/graph/docs/api-reference/v1.0/resources/invitation>.

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Los elementos del correo electrónico de invitación de colaboración B2B](#)
- [Canje de invitación de colaboración B2B](#)
- [Incorporación de usuarios de colaboración B2B sin invitación](#)

Preguntas más frecuentes acerca de la colaboración B2B de Azure Active Directory

18/02/2021 • 20 minutes to read • [Edit Online](#)

Las preguntas más frecuentes (P+F) acerca de la colaboración negocio a negocio (B2B) de Azure Active Directory (Azure AD) se actualizan periódicamente para incluir nuevos temas.

IMPORTANT

- A partir del 4 de enero de 2021, Google deja [en desuso el soporte de inicio de sesión de WebView](#). Si usa Google Federation o el registro de autoservicio con Gmail, debería [comprobar la compatibilidad de las aplicaciones nativas de línea de negocio](#).
- A partir del 31 de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure AD no administradas e inquilinos para escenarios de colaboración B2B. Como preparación, se recomienda a los clientes que opten por la [autenticación de código de acceso de un solo uso por correo electrónico](#). Agradecemos sus comentarios sobre esta característica en vista previa pública. Nos alegra poder crear más formas de colaborar.

¿Se puede personalizar la página de inicio de sesión de forma que resulte más intuitiva para los usuarios invitados a la colaboración B2B?

Por supuesto. Consulte nuestra [entrada del blog relativa a esta característica](#). Para más información acerca de cómo personalizar la página de inicio de sesión de una organización, consulte [Incorporación de la personalización de marca de empresa a sus páginas de inicio de sesión y panel de acceso](#).

¿Pueden acceder los usuarios de colaboración B2B a SharePoint Online y OneDrive?

Sí. Sin embargo, la capacidad de buscar usuarios invitados existentes en SharePoint Online mediante el uso del selector de personas está [desactivada](#). Para activar la opción de búsqueda de usuarios invitados existentes, establezca `ShowPeoplePickerSuggestionsForGuestUsers` en [Activado](#). Esta configuración se puede activar en el nivel del inquilino o en el nivel de colección de sitios. Esta configuración se puede cambiar mediante los cmdlets `Set-SPOTenant` y `SPOSite`. Con estos cmdlets, los miembros pueden buscar todos los usuarios invitados existentes en el directorio. Los cambios en el ámbito del inquilino no afectan a los sitios de SharePoint Online que ya se han aprovisionado.

¿Aún se admite la característica de carga de CSV?

Sí. Para más información acerca de cómo utilizar la característica de carga de archivos .csv, vea [este ejemplo de PowerShell](#).

¿Cómo puedo personalizar mis correos electrónicos de invitación?

Mediante las [API de invitación de B2B](#) puede personalizar casi todos los elementos del proceso del invitador.

¿Pueden restablecer los usuarios invitados su método de Multi-Factor Authentication?

Sí. Los usuarios invitados pueden restablecer su método de Multi-Factor Authentication de la misma manera que los usuarios normales.

¿Qué organización es la responsable de las licencias de Multi-Factor Authentication?

La organización que invita realiza la autenticación multifactor. La organización que invita debe asegurarse de que la organización tiene suficientes licencias para sus usuarios B2B que utilizan Multi-Factor Authentication.

¿Qué ocurre si una organización asociada ya tiene Multi-Factor Authentication configurado? ¿Podemos confiar en su Multi-Factor Authentication y no utilizar nuestro propio Multi-Factor Authentication?

Actualmente, esta característica no se admite. Si el acceso a los recursos de la organización requiere la autenticación multifactor, la organización del partner tendrá que registrarse para la autenticación multifactor en la organización que invita.

¿Cómo se usan las invitaciones diferidas?

Algunas organizaciones pueden desear agregar usuarios de colaboración B2B, aprovisionarlos en las aplicaciones cuando sea necesario y, luego, enviar las invitaciones. Puede usar la API de invitación de colaboración B2B para personalizar el flujo de trabajo de incorporación.

¿Puedo hacer visibles a los usuarios invitados en la lista global de direcciones de Exchange?

Sí. De manera predeterminada, los objetos de invitado no aparecen en la lista global de direcciones de la organización (GAL), pero puede usar Azure Active Directory PowerShell para que figuren. Consulte [¿Puedo hacer que los objetos de invitado sean visibles en la lista global de direcciones?](#).

¿Puedo hacer que un usuario invitado sea un administrador limitado?

Totalmente. Para más información, consulte [Asignación de roles de administrador en la versión preliminar de Azure Active Directory](#).

¿Permite la colaboración B2B de Azure AD que los usuarios B2B accedan a Azure Portal?

Salvo que a un usuario se le asigne el rol de administrador limitado, los usuarios de colaboración B2B no necesitarán acceso a Azure Portal. Sin embargo, los usuarios de colaboración B2B a los que se asigna el rol de administrador limitado pueden acceder al portal. Además, si un usuario invitado al que no se le han asignado estos roles de administrador tuviera acceso al portal, podría acceder a determinadas partes de la experiencia. El rol de usuario invitado tiene algunos permisos en el directorio.

¿Puedo bloquear el acceso a Azure Portal a los usuarios invitados?

Sí. Puede crear una directiva de acceso condicional que impida a todos los usuarios invitados y externos tener acceso a Azure Portal. Cuando configure esta directiva tenga cuidado de evitar que se bloquee accidentalmente el acceso a los administradores y miembros.

1. Inicie sesión en [Azure Portal](#) como administrador de seguridad o administrador de acceso condicional.
2. En Azure Portal, seleccione **Azure Active Directory**.
3. En **Administrar**, seleccione **Seguridad**.
4. En **Proteger**, seleccione **Acceso condicional**. Seleccione **Nueva directiva**.
5. En la página **Nuevo**, en el cuadro de texto **Nombre**, escriba un nombre para la directiva (por ejemplo, "Impedir que los invitados accedan al portal").
6. En **Asignaciones**, seleccione **Usuarios y grupos**.
7. En la pestaña **Incluir**, elija **Seleccionar usuarios y grupos** y, a continuación, seleccione **Todos los usuarios externos e invitados (versión preliminar)**.
8. Seleccione **Listo**.
9. En la página **Nuevo**, en la sección **Asignaciones**, seleccione **Aplicaciones en la nube o acciones**.
10. En la página **Aplicaciones en la nube o acciones**, haga clic en **Seleccionar aplicaciones** y después haga clic en **Seleccionar**.
11. En la página **Seleccionar**, elija **Administración de Microsoft Azure** y después haga clic en **Seleccionar**.
12. En la página **Aplicaciones en la nube o acciones**, seleccione **Listo**.

¿Admite la colaboración B2B de Azure AD admitir la autenticación multifactor y las cuentas de correo electrónico de consumidor?

Sí. Tanto la autenticación multifactor como las cuentas de correo electrónico de consumidor admiten para la colaboración B2B de Azure AD.

¿Va a admitir el restablecimiento de contraseñas con los usuarios de la colaboración B2B de Azure AD?

Si el inquilino de Azure AD es el directorio principal de un usuario, puede [restablecer la contraseña del usuario](#)

en Azure Portal. Sin embargo, no puede restablecer directamente la contraseña de los usuarios invitados que inician sesión con una cuenta administrada por otro proveedor de identidades externo o por otro directorio de Azure AD. En ese caso, solo podrá restablecer la contraseña el usuario invitado o un administrador del directorio principal del usuario. A continuación, se incluyen algunos ejemplos de cómo funciona el restablecimiento de contraseñas con los usuarios invitados:

- Los usuarios invitados que inicien sesión con una cuenta Microsoft (por ejemplo guestuser@live.com) podrán restablecer sus propias contraseñas con el autoservicio de restablecimiento de contraseñas (SSPR) de la cuenta Microsoft. Consulte [Cómo restablecer la contraseña de tu cuenta Microsoft](#).
- Los usuarios invitados que inicien sesión con una cuenta de Google u otro proveedor de identidades externo podrán restablecer sus propias contraseñas mediante el método de SSPR de su proveedor de identidades. Por ejemplo, un usuario invitado con la cuenta de Google guestuser@gmail.com puede restablecer su contraseña siguiendo las instrucciones acerca de [cómo cambiar o restablecer la contraseña](#).
- Si el inquilino de la identidad es un inquilino Just-In-Time (JIT) o un inquilino "viral" (es decir, un inquilino de Azure que es independiente y no está administrado), solamente el usuario invitado podrá restablecer su contraseña. A veces, una organización [asumirá la administración de los inquilinos virales](#) que se crean cuando los empleados usan sus direcciones de correo electrónico del trabajo para registrarse en los servicios. Después de que la organización se haga cargo de un inquilino viral, solo un administrador de dicha organización puede restablecer la contraseña del usuario o habilitar SSPR. Si es necesario, como la organización que invita, puede quitar la cuenta del usuario invitado del directorio y volver a enviar una invitación.
- Si el directorio principal del usuario invitado es su inquilino de Azure AD, usted podrá restablecer la contraseña del usuario. Por ejemplo, es posible que haya creado o sincronizado un usuario desde la instancia local de Active Directory y que haya establecido UserType en Guest (invitado). Como este usuario estará alojado en su directorio, podrá restablecer su contraseña desde Azure Portal.

¿Proporciona Microsoft Dynamics 365 compatibilidad en línea con la colaboración B2B de Azure AD?

Sí, Dynamics 365 (en línea) admite la colaboración B2B de Azure AD. Para más información, consulte el artículo de Dynamics 365 [Invitar a usuarios con colaboración B2B de Azure Active Directory](#).

¿Cuál es la duración de una contraseña inicial para un usuario de colaboración B2B recién creado?

Azure AD tiene un conjunto fijo de requisitos de bloqueo de cuentas, seguridad de la contraseña y caracteres que se aplican igualmente a todas las cuentas de usuario en la nube de Azure AD. Las cuentas de usuario en la nube son cuentas que no están federadas con otro proveedor de identidades, como:

- Cuenta Microsoft
- Facebook
- Servicios de federación de Active Directory
- Otro inquilino de nube (para la colaboración B2B)

En el caso de las cuentas federadas, la directiva de contraseñas depende de la directiva que se aplica en el inquilino local y la configuración de la cuenta Microsoft del usuario.

Una organización puede tener distintas experiencias en sus aplicaciones para los usuarios inquilinos y los usuarios invitados. ¿Hay instrucciones estándar para esto? ¿La presencia de la notificación del proveedor de identidades es el modelo más adecuado para usarlo?

Un usuario invitado puede utilizar cualquier proveedor de identidades para realizar la autenticación. Para más información, consulte [Propiedades de un usuario de colaboración B2B de Azure Active Directory](#). Use la propiedad **UserType** para determinar la experiencia del usuario. La notificación **UserType** no está incluida actualmente en el token. Las aplicaciones deben usar Microsoft Graph API para consultar el usuario en el directorio y obtener UserType.

¿Dónde puedo encontrar una comunidad de colaboración B2B para compartir soluciones y enviar ideas?

Escuchamos constantemente sus comentarios para mejorar la colaboración B2B. Comparta escenarios de usuario, procedimientos recomendados y todo lo que le guste de la colaboración B2B de Azure AD. Únase al debate en [Microsoft Tech Community](#).

También le invitamos a enviar sus ideas y a votar las características futuras en el sitio de [ideas para la colaboración B2B](#).

¿Podemos enviarle una invitación que se canjee automáticamente para que el usuario pueda empezar en cualquier momento? ¿O bien, el usuario siempre tiene que hacer clic para desplazarse a la dirección URL de canje?

Puede invitar a otros usuarios de la organización asociada utilizando la interfaz de usuario, los scripts de PowerShell o las API. Después, puede enviar al usuario invitado un vínculo directo a una aplicación compartida. En la mayoría de los casos, ya no es necesario abrir la invitación de correo electrónico y hacer clic en una dirección URL de canje. Consulte [Experiencia de invitación de colaboración B2B de Azure Active Directory](#).

¿Cómo funciona la colaboración B2B cuando el asociado invitado utiliza la federación para agregar su propia autenticación local?

Si el asociado tiene un inquilino de Azure AD que está federado en la infraestructura de autenticación local, se consigue automáticamente el inicio de sesión único (SSO) local. Si el asociado no tiene ningún inquilino de Azure AD, se crea una cuenta de Azure AD para los usuarios nuevos.

Creía que B2B de Azure AD no aceptaba direcciones de correo electrónico gmail.com y outlook.com, y que se usaba B2C para esos tipos de cuentas

Estamos eliminando las diferencias entre B2B y colaboración de negocio al consumidor (B2C) en cuanto a las identidades que se admiten. La identidad utilizada no es una buena razón para decidir si se va a utilizar B2B o B2C. Para obtener información acerca de cómo elegir la opción de colaboración, consulte [Comparación de la colaboración B2B y B2C de Azure Active Directory](#).

¿Se puede invitar a una cuenta local de Azure AD B2C a un inquilino de Azure AD para la colaboración B2B?

No. Solo se puede usar una cuenta local de Azure AD B2C para iniciar sesión en el inquilino de Azure AD B2C. No se puede usar la cuenta para iniciar sesión en un inquilino de Azure AD. No se admite la invitación de una cuenta local de Azure AD B2C a un inquilino de Azure AD para la colaboración B2B.

¿Qué aplicaciones y los servicios admiten los usuarios invitados de Azure B2B?

Todas las aplicaciones integradas en Azure AD pueden admitir usuarios invitados de B2B de Azure, pero deben usar un punto de conexión configurado como inquilino para autenticar a los usuarios invitados. También es posible que necesite [personalizar las notificaciones](#) del token SAML que se emite cuando un usuario invitado se autentica en la aplicación.

¿Podemos forzar la autenticación multifactor para usuarios invitados de B2B si nuestros asociados no la tienen?

Sí. Para más información, consulte [Acceso condicional para usuarios de colaboración B2B](#).

En SharePoint puede definir una lista de "permitidos" o "denegados" para usuarios externos. ¿Se puede hacer esto en Azure?

Sí. La colaboración B2B de Azure AD admite listas de permitidos y de denegados.

¿Qué licencias se necesitan para usar B2B de Azure AD?

Para información sobre las licencias que su organización necesita para usar Azure AD B2B, consulte [Precios de identidades externas](#).

Pasos siguientes

- [¿Qué es la colaboración B2B de Azure AD?](#)

Instrucciones para buscar ayuda y abrir una incidencia de soporte técnico para Azure Active Directory

18/02/2021 • 6 minutes to read • [Edit Online](#)

Microsoft proporciona internacionalmente soporte técnico de preventa, facturación y suscripción para Azure Active Directory (Azure AD). El soporte técnico está disponible tanto en línea como por teléfono para las suscripciones de prueba y de pago de Microsoft Azure. El soporte técnico por teléfono y el soporte técnico para la facturación en línea están disponibles en otros idiomas.

Recibir ayuda sin abrir una incidencia de soporte técnico

Antes de crear una incidencia de soporte técnico, consulte los recursos siguientes para obtener información y respuestas.

- Para consultar contenido como información de procedimientos o ejemplos de código para profesionales de TI y desarrolladores, vea la [documentación técnica en docs.microsoft.com](#).
- La [Comunidad técnica de Microsoft](#) es el lugar en el que nuestros asociados profesionales de TI y los clientes colaboran, comparten información y aprenden. El [Centro de información de la Comunidad técnica de Microsoft](#) se usa para anuncios, entradas de blog, interacciones AMA ("pregunta lo que quieras") con expertos y mucho más. También puede [unirse a la comunidad para enviar sus ideas](#).

Abrir una incidencia de soporte técnico

Si no encuentra una respuesta en estos recursos de autoayuda, puede abrir una incidencia de soporte técnico en línea. Debe abrir una incidencia de soporte técnico por problema, para que podamos ponerle en contacto con ingenieros que sean expertos en la materia en cuestión. Además, los equipos de ingeniería de Azure Active Directory dan prioridad a su trabajo en función de los incidentes que se generan, por lo que usted puede contribuir a mejorar el servicio.

Cómo abrir una incidencia de soporte técnico de Azure AD en Azure Portal

NOTE

- Si se trata de problemas relativos a la facturación o la suscripción, debe usar el [Centro de administración de Microsoft 365](#).
- Si usa Azure AD B2C, abra una incidencia de soporte técnico y cambie primero a un inquilino de Azure AD que tenga asociada una suscripción de Azure. Normalmente, se trata del inquilino del empleado o del inquilino predeterminado que se creó cuando se registró para una suscripción de Azure. Para más información, consulte [Asociación de las suscripciones de Azure con Azure Active Directory](#).

1. Inicie sesión en [Azure Portal](#) y abra **Azure Active Directory**.
2. Desplácese hasta **Solución de problemas y soporte técnico** y seleccione **Nueva solicitud de soporte técnico**.
3. En la hoja **Básico**, en **Tipo de problema**, seleccione **Técnico**.
4. Seleccione su **suscripción**.

5. En Servicio, seleccione Azure Active Directory.
6. Cree un **resumen** de la solicitud. El resumen debe tener menos de 140 caracteres.
7. Seleccione un **tipo de problema** y una categoría. En este momento, se le ofrecerá información de autoayuda para la categoría del problema.
8. Agregue el resto de información relativa al problema y haga clic en **Siguiente**.
9. En ese punto, aparecerán soluciones de autoayuda y documentación en la hoja **Soluciones**. Si ninguna de las soluciones resuelven el problema, haga clic en **Siguiente**.
10. En la hoja **Detalles**, rellene los datos necesarios y seleccione un valor en **Gravedad**.

The screenshot shows the Microsoft Azure Active Directory support request interface. The top navigation bar includes 'All services' and 'Microsoft | New support request'. The left sidebar lists various management categories like Users, Groups, and Enterprise applications. The main content area has tabs for 'Basics', 'Solutions', 'Details' (which is selected), and 'Review + create'. The 'Details' tab contains fields for 'When did the problem start?' (MM/DD/YYYY), 'Description' (a large text area for providing information about the issue), 'File upload' (a file selection input), 'Consent' (a checkbox for sharing diagnostic information), and 'Support method' (a dropdown set to 'Azure Support Plan - Internal'). Below these are sections for 'Severity' (set to 'C - Minimal impact') and 'Preferred contact method' (with options for 'Email' and 'Phone'). At the bottom, there are buttons for 'Previous: Solutions' and 'Next: Review + create >'.

11. Proporcione la información de contacto y seleccione **Siguiente**.
12. Proporcione su información de contacto y seleccione **Crear**.

The screenshot shows the Microsoft Azure Active Directory 'New support request' interface. The left sidebar contains a list of administrative tools. The main content area is divided into several sections: 'BASICS' (Issue type: Technical, Subscription: IBIZA - Test (76cb77fa-8b17-4eab-9493-b65dace99813), Service: Azure Active Directory App Integration and Development, Problem type: Issues Signing In to Applications, Problem subtype: On-premises apps via Azure AD application proxy, Summary: testing); 'TERMS, CONDITIONS AND PRIVACY POLICY' (Accept terms and conditions, View privacy policy); 'DETAILS' (Full Error Message: AAD0505 - Error message, Consent: Share diagnostic information); 'SUPPORT METHOD' (Severity: B - Moderate impact, Support plan: Azure Support Plan - Internal, Your availability: Business Hours, Support language: English, Contact method: Email); 'CONTACT INFO' (Contact name: [redacted], Email: [redacted]). At the bottom right, a blue 'Create' button is highlighted with a red border.

Cómo abrir una incidencia de soporte técnico de Azure AD en el Centro de administración de Microsoft 365

NOTE

En el [Centro de administración de Microsoft 365](#) solo se ofrece soporte técnico de Azure AD para administradores.

1. Inicie sesión en el [Centro de administración de Microsoft 365](#) con una cuenta que tenga una licencia de Enterprise Mobility + Security (EMS).
2. En el ícono **Soporte técnico**, seleccione **Nueva solicitud de servicio**:
3. En la página **Información general de soporte técnico**, seleccione **Administración de identidades** o **User and domain management** (Administración de usuarios y dominios):
4. En **Característica**, seleccione la característica de Azure AD para la que quiere recibir soporte técnico.
5. En **Síntoma**, seleccione un síntoma adecuado, resuma el problema e incluya los detalles pertinentes. Después, seleccione **Siguiente**.
6. Seleccione uno de los recursos de autoayuda que se proporcionan, o bien seleccione **Sí, continuar** o **No, cancel request** (No, cancelar la solicitud).
7. Si continúa, se le pedirán más detalles. Puede adjuntar archivos en los que se vea el problema. Después, seleccione **Siguiente**.
8. Proporcione su información de contacto y seleccione **Enviar solicitud**.

Obtener soporte técnico por teléfono

Vea la página [Póngase en contacto con Microsoft para obtener soporte técnico](#) para consultar los números de teléfono de soporte técnico.

Pasos siguientes

- [Comunidad tecnológica de Microsoft](#)
- [Documentación técnica en docs.microsoft.com](#)