**Introducción**

Este módulo se centra en administrar de forma eficaz las identidades y mejorar la seguridad en Microsoft Entra ID, lo que garantiza que los usuarios, grupos e identidades externas están protegidos contra amenazas de seguridad y acceso no autorizado.

**Escenario**

Imagine que es un administrador de identidades y seguridad responsable de proteger las cuentas de usuario y el acceso a los recursos en el entorno de Microsoft Entra ID de su organización. Su organización utiliza Microsoft Entra ID para la autenticación y el control de acceso, y debe asegurarse de que las identidades están protegidas, ya sean internas o externas, y que están protegidas contra posibles brechas de seguridad.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Proteger las identidades de usuario en Microsoft Entra ID para evitar el acceso no autorizado y proteger las cuentas de usuario.
* Implementar medidas de seguridad para proteger grupos en Microsoft Entra ID, lo que garantiza un control de acceso adecuado y la administración de grupos.
* Realizar recomendaciones informadas sobre cuándo usar identidades externas y cómo administrarlas de forma segura.
* Implementar medidas de seguridad para proteger las identidades externas, manteniendo la confidencialidad y la integridad.
* Implementar Microsoft Entra ID Protection para identificar y responder proactivamente a las amenazas y vulnerabilidades de seguridad relacionadas con la identidad.

**Objetivos**

El módulo tiene como objetivo proporcionar a los participantes los conocimientos y aptitudes necesarios para administrar identidades y mejorar la seguridad dentro de Microsoft Entra ID. Los participantes aprenderán a proteger las cuentas de usuario, los grupos y las identidades externas, y podrán implementar Microsoft Entra ID Protection para detectar y mitigar los riesgos de seguridad relacionados con la identidad, y en última instancia reforzarán la posición de seguridad general de la organización.

**¿Qué es Microsoft Entra ID?**

Microsoft Entra ID es un servicio de administración de identidades y acceso basado en la nube que permite a los empleados acceder a recursos externos. Entre los recursos de ejemplo se incluyen Microsoft 365, Azure Portal y miles de otras aplicaciones SaaS.

Microsoft Entra ID también les ayuda a acceder a recursos internos, como las aplicaciones de la red corporativa de intranet, junto con las aplicaciones en la nube desarrolladas para su propia organización.

**¿Quién usa Microsoft Entra ID?**

Microsoft Entra ID proporciona diferentes beneficios a los miembros de su organización en función de su función:

* Administradores de TI: pueden usar Microsoft Entra ID para controlar el acceso a las aplicaciones y a los recursos de estas en función de los requisitos de la empresa. Por ejemplo, como administrador de TI, puede usar Microsoft Entra para requerir la autenticación multifactor al acceder a recursos importantes de la organización. También puede usar Microsoft Entra ID para automatizar el aprovisionamiento de usuarios entre la instancia de Windows Server existente y las aplicaciones en la nube, incluido Microsoft 365. Finalmente, Microsoft Entra ID le brinda potentes herramientas para ayudar a proteger automáticamente las identidades y credenciales de los usuarios y para cumplir con sus requisitos de gobierno de acceso. Para empezar, regístrese para una prueba gratuita de 30 días de Microsoft Entra ID P1 o P2 .
* Los desarrolladores de aplicaciones pueden usar Microsoft Entra ID como proveedor de autenticación basado en estándares que les ayuda a agregar un inicio de sesión único (SSO) a las aplicaciones que funcionan con las credenciales existentes de un usuario. Los desarrolladores también pueden usar las API de Microsoft Entra para crear experiencias personalizadas utilizando datos de la organización. Para empezar, regístrese para una prueba gratuita de 30 días de Microsoft Entra ID P1 o P2 . Para obtener más información, también puede ver Microsoft Entra ID para desarrolladores.
* Los suscriptores de Microsoft 365, Office 365, Azure o Dynamics CRM Online ya usan Microsoft Entra ID, ya que cada inquilino de Microsoft 365, Office 365, Azure y Dynamics CRM Online es automáticamente un inquilino de Microsoft Entra. Puede empezar de inmediato a administrar el acceso a las aplicaciones en la nube integradas.

**¿Cuáles son las licencias de identificador de Microsoft Entra?**

Los servicios empresariales de Microsoft Online, como Microsoft 365 o Microsoft Azure, utilizan Microsoft Entra ID para las actividades de inicio de sesión y para ayudar a proteger sus identidades. Si se suscribe a cualquier servicio empresarial de Microsoft Online, tendrá acceso automáticamente a Microsoft Entra ID Free.

Para mejorar la implementación de Microsoft Entra, también puede agregar características de pago mediante la actualización a las licencias Microsoft Entra Premium P1 o Premium P2. Las licencias de pago de Microsoft Entra se construyen sobre su directorio gratuito existente. Las licencias proporcionan autoservicio, supervisión mejorada, informes de seguridad y acceso seguro para los usuarios móviles.

* Microsoft Entra ID Gratis. Proporciona administración de grupos y usuarios, sincronización de directorios locales, informes básicos, cambio de contraseñas de autoservicio para usuarios en la nube e inicio de sesión único en Azure, Microsoft 365 y muchas aplicaciones SaaS populares.
* Microsoft Entra ID P1. Además de las características de la versión Free, P1 también permite a los usuarios de entornos híbridos acceder a recursos locales y en la nube. También admite la administración avanzada, como grupos dinámicos, administración de grupos de autoservicio, Microsoft Identity Manager y funcionalidades de reescritura en la nube, que permiten el restablecimiento de contraseña de autoservicio a los usuarios locales.
* Microsoft Entra ID P2. Además de las funciones gratuitas y P1, P2 también ofrece Microsoft Entra ID Protection para ayudar a proporcionar acceso condicional basado en el riesgo a sus aplicaciones y datos críticos de la empresa y Privileged Identity Management para ayudar a descubrir, restringir y supervisar a los administradores y su acceso a los recursos y para proporcionar acceso justo a tiempo cuando sea necesario.
* Licencias de la característica de "Pago por uso". También puede obtener licencias para funciones como Microsoft Entra Business-to-Customer (B2C). B2C puede ayudarle a proporcionar soluciones de administración de acceso y de identidad para las aplicaciones orientadas al cliente.

**¿Qué características funcionan en el identificador de Microsoft Entra ID?**

Después de elegir su licencia de Microsoft Entra ID, obtendrá acceso a algunas de las características siguientes:

| **Categoría** | **Descripción** |
| --- | --- |
| Administración de aplicaciones | Administre las aplicaciones en la nube y locales mediante Application Proxy, el inicio de sesión único, el portal Mis aplicaciones y aplicaciones de software como servicio (SaaS). |
| Autenticación | Administre el autoservicio de restablecimiento de contraseña de Microsoft Entra, la autenticación multifactor, la lista de contraseñas prohibidas personalizadas y el bloqueo inteligente. |
| Microsoft Entra ID para desarrolladores | Cree aplicaciones que inicie sesión en todas las identidades de Microsoft, obtenga tokens para llamar a Microsoft Graph, otras API de Microsoft API o API personalizadas. |
| Negocio a negocio (B2B) | Administre los usuarios invitados y los asociados externos sin perder el control sobre sus propios datos corporativos. |
| Negocio a cliente (B2C) | Personalice y controle la forma en que los usuarios se suscriben, inician sesión y administran sus perfiles al usar sus aplicaciones. |
| Acceso condicional | Administre el acceso a sus aplicaciones en la nube. |
| Administración de dispositivos | Administre la forma en que los dispositivos en la nube o locales acceden a los datos corporativos. |
| Servicios de dominio | Combine máquinas virtuales de Azure en un dominio sin controladores de dominio. |
| Usuarios de empresa | Administre las asignaciones de licencias, el acceso a las aplicaciones y configure delegados mediante grupos y roles de administrador. |
| Identidad híbrida | Use Microsoft Entra Connect y Connect Health para proporcionar una identidad de usuario individual para la autenticación y autorización en todos los recursos, independientemente de la ubicación (nube o local). |
| Gobernanza de identidades | Administre la identidad de su organización a través de controles de acceso a empleados, asociados comerciales, proveedores, servicios y aplicaciones. También puede realizar revisiones de acceso. |
| Protección de identidad | Detecte posibles puntos vulnerables que afecten a identidades de su organización, configure directivas para responder a acciones sospechosas y, después, realice las acciones adecuadas para resolverlas. |
| Identidades administradas de recursos de Azure | Proporcione a sus servicios de Azure una identidad administrada automáticamente en Microsoft Entra ID que pueda autenticar cualquier servicio de autenticación compatible con Microsoft Entra ID, incluido Key Vault. |
| Privileged Identity Management (PIM) | Administre, controle y supervise el acceso dentro de su organización. Esta característica incluye el acceso a los recursos de Microsoft Entra ID y Azure, así como a otros servicios Microsoft Online Services, como Microsoft 365 o Intune. |
| Supervisión y estado | Obtenga información acerca de los patrones de seguridad y de uso del entorno. |
| Identidades de cargas de trabajo | Proporcione una identidad a su carga de trabajo de software (como una aplicación, un servicio, un script o un contenedor) para autenticar otros servicios y recursos y acceder a ellos. |

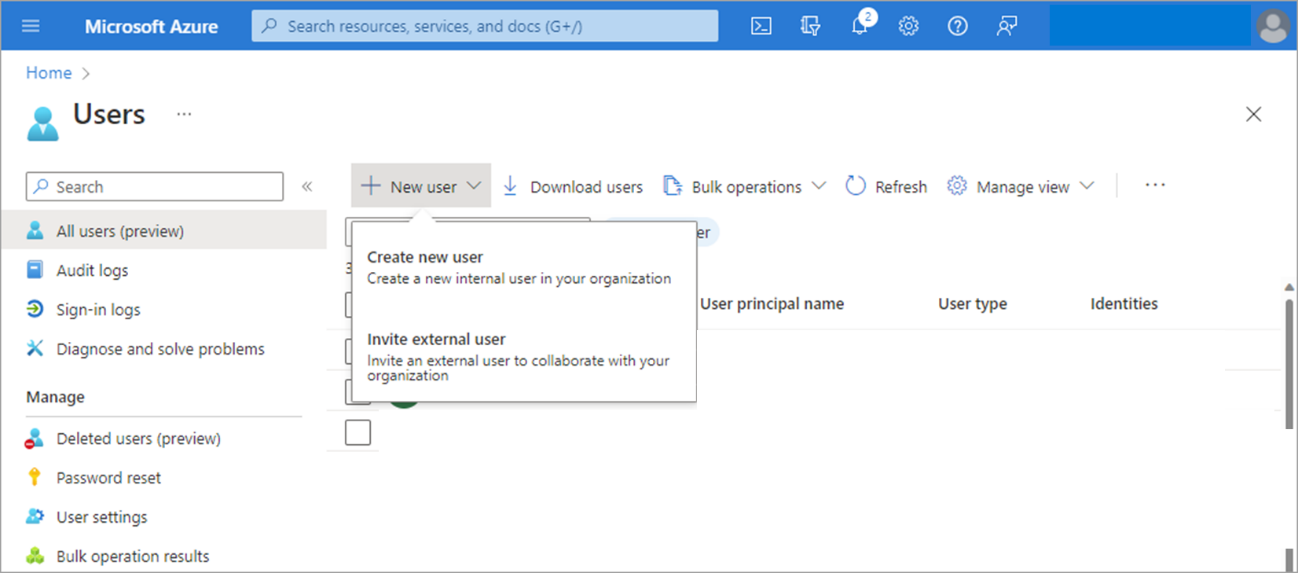
**Protección de usuarios en Microsoft Entra ID**

Agregue nuevos usuarios o elimine los usuarios existentes del inquilino de Microsoft Entra ID. Para **agregar** o **eliminar** usuarios debe ser **administrador de usuarios** o **global**.

**Agregar un nuevo usuario**

Puede crear un nuevo usuario para su organización o invitar a un usuario externo desde el mismo punto de partida.

1. Inicie sesión en **Azure Portal** como administrador de usuarios.
2. Vaya a **Microsoft Entra ID**>**Usuarios**.
3. Seleccione **Crear nuevo usuario** o **Invitar a un usuario externo** en el menú.



1. En la página **Nuevo usuario**, proporcione la información del nuevo usuario:
   * **Identidad:** agregue un nombre de usuario y un nombre para mostrar para el usuario. **El nombre de usuario** y el **nombre** son necesarios y no pueden contener tildes. También puede agregar un nombre y apellidos.

La parte de dominio del nombre de usuario debe usar el nombre de dominio predeterminado inicial, **<nombre de dominio>.onmicrosoft.com** o un nombre de dominio personalizado, como **contoso.com**.

* + **Grupos y roles:** opcional. Agregue el usuario a uno o más grupos existentes. La pertenencia a grupos se puede establecer en cualquier momento.
  + **Configuración:** opcional. Cambie la opción para bloquear el inicio de sesión del usuario o establecer la ubicación predeterminada del usuario.
  + **Información del trabajo:** opcional. Agregue el puesto de trabajo del usuario, el departamento, el nombre de la empresa y su director. Estos detalles se pueden actualizar en cualquier momento.

1. Copie la contraseña generada automáticamente proporcionada en el cuadro de texto **Contraseña**. Deberá proporcionar esta contraseña al usuario para iniciar sesión por primera vez.
2. Seleccione **Crear**.

El usuario se crea y se agrega a la organización de Microsoft Entra ID.

**Incorporación de un usuario invitado nuevo**

También puede invitar a un usuario invitado nuevo a colaborar con su organización si selecciona **Invitar usuario** en la página **Nuevo usuario**. Si la configuración de colaboración externa de la organización está configurada para invitar a otros usuarios, el usuario recibirá una invitación por correo electrónico que debe aceptar para empezar a colaborar.

**Agregar otros usuarios**

Puede haber escenarios en los que quiera crear manualmente cuentas de consumidor en el directorio de Microsoft Entra B2B. Si tiene un entorno con Microsoft Entra ID (**nube**) y Windows Server Active Directory (**local**), puede agregar nuevos usuarios mediante la sincronización de los datos de la cuenta de usuario existentes.

**Eliminación de usuarios**

Puede eliminar un usuario existente mediante el portal de Microsoft Entra ID.

* Debe tener una asignación de roles de administrador global, administrador de autenticación con privilegios o administrador de usuarios para eliminar usuarios de la organización.
* Los administradores globales y los administradores de autenticación con privilegios pueden eliminar cualquier usuario, entre los que se incluyen otros administradores.
* Los administradores de usuarios pueden eliminar cualquier usuario que no sea administrador, administradores del departamento de soporte técnico y otros administradores de usuarios.

1. Inicie sesión en **Azure Portal** mediante uno de los roles apropiados indicados anteriormente.
2. Vaya a **Microsoft Entra ID**>**Usuarios**.
3. Busque y seleccione el usuario que desea eliminar del inquilino de Microsoft Entra ID.
4. Seleccione **Eliminar usuario**.

El usuario se elimina y ya no aparece en la página**Usuarios** - **Todos los usuarios**. El usuario se puede ver en la página **Usuarios eliminados** durante los próximos **30 días** y puede restaurarse durante ese tiempo.

Cuando se elimina un usuario, las licencias consumidas por el usuario se ponen a disposición de otros usuarios.

**Nota**

Para actualizar la identidad, la información de contacto o la información del trabajo de los usuarios cuyo origen de autoridad es Windows Server Active Directory, debe usar Windows Server Active Directory. Después de completar la actualización, debe esperar a que se complete el ciclo de sincronización siguiente para poder ver los cambios.

**Protección de grupos en Microsoft Entra ID**

Microsoft Entra ID proporciona varias maneras para administrar el acceso a recursos, aplicaciones y tareas. Con los grupos de Microsoft Entra ID, puede conceder acceso y permisos a un grupo de usuarios en lugar de hacerlo para cada usuario individual. Uno de los principales principios de seguridad de Confianza cero consiste en limitar el acceso a los recursos de Microsoft Entra ID solo a aquellos usuarios que necesiten dicho acceso.

Microsoft Entra ID permite usar grupos para administrar el acceso a aplicaciones, datos y recursos. Los recursos pueden:

* Parte de la organización de Microsoft Entra ID, como permisos para administrar objetos a través de roles en Microsoft Entra ID
* Externo a la organización, como para aplicaciones de software como servicio (SaaS)
* Servicios de Azure
* Sitios de SharePoint
* Recursos locales

Algunos grupos no se pueden administrar en el Portal de Microsoft Entra ID:

* Los grupos sincronizados desde Microsoft Entra ID local solo se pueden administrar en Microsoft Entra ID local.
* Las listas de distribución y los grupos de seguridad habilitados para correo, solo se administran en el centro de administración de Exchange o en el centro de administración de Microsoft 365. Debe iniciar sesión en el centro de administración de Exchange o en el Centro de administración de Microsoft 365 para administrar estos grupos.

**Antes de crear un grupo debe saber que:**

Existen **dos tipos de grupos** y **tres tipos de pertenencia a grupos**.

**Tipos de grupo:**

**Seguridad:** se usa para administrar el acceso de usuarios y equipos a los recursos compartidos.

Por ejemplo, puede crear un grupo de seguridad para que todos los miembros del grupo tengan el mismo conjunto de permisos de seguridad. Entre los miembros de un grupo de seguridad pueden incluirse usuarios, dispositivos, otros grupos y entidades de servicio, que definen la directiva de acceso y los permisos. Entre los propietarios de un grupo de seguridad pueden incluirse usuarios y entidades de servicio.

**Microsoft 365:** proporciona oportunidades de colaboración al conceder a los miembros del grupo acceso a un buzón compartido, calendarios, archivos, sitios de SharePoint y mucho más.

Esta opción también permite ofrecer acceso al grupo a personas de fuera de la organización. Entre los miembros de un grupo de Microsoft 365 solo pueden incluirse usuarios. Entre los propietarios de un grupo de Microsoft 365 pueden incluirse usuarios y entidades de servicio.

**Tipos de pertenencia:**

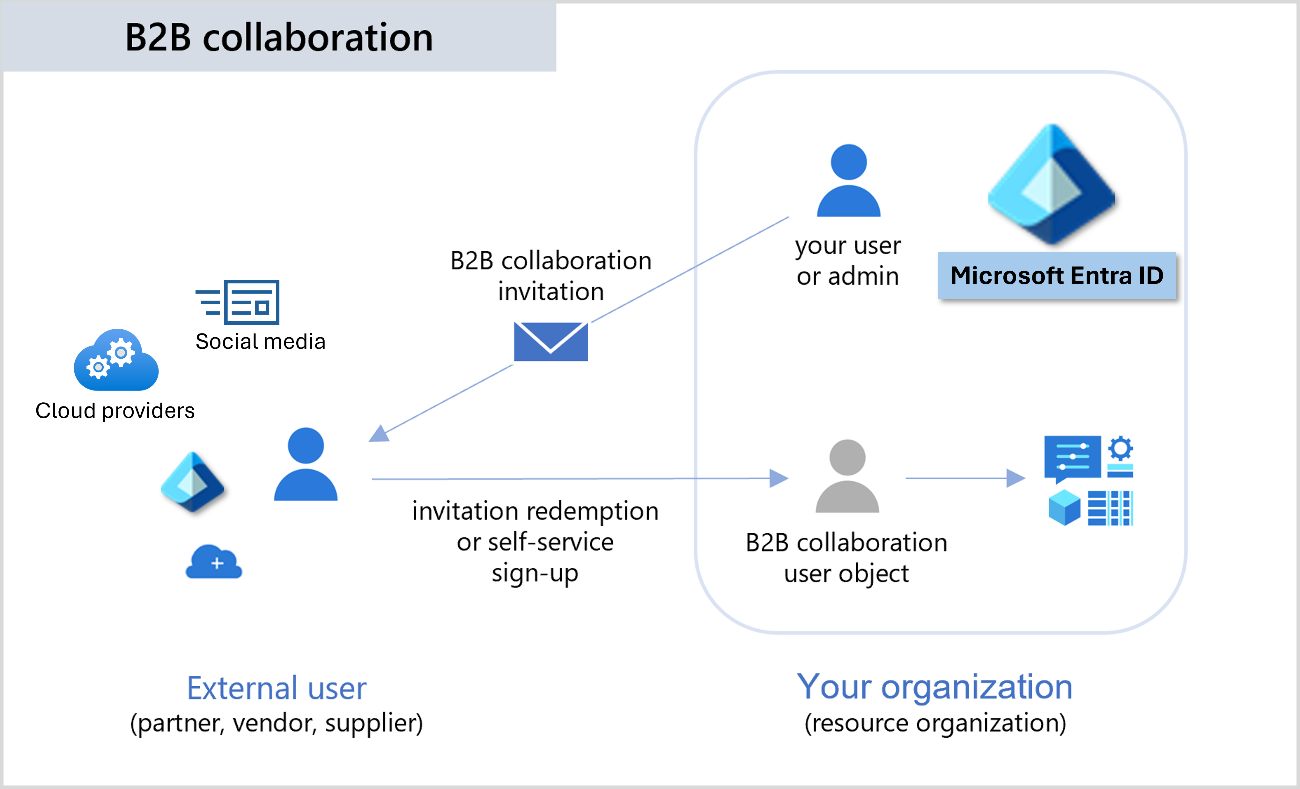
* **Asignado:** permite agregar usuarios específicos como miembros de un grupo y que tengan permisos exclusivos.
* **Usuario dinámico**: permite usar reglas de pertenencia dinámicas para agregar y quitar miembros automáticamente. Si los atributos de un miembro cambian, el sistema examina las reglas del grupo dinámico del directorio para comprobar si el miembro cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).
* **Dispositivo dinámico:** permite usar reglas de grupo dinámico para agregar y quitar dispositivos automáticamente. Si los atributos de un dispositivo cambian, el sistema examina las reglas del grupo dinámico del directorio para comprobar si el dispositivo cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).

**Importante**

Puede crear un grupo dinámico para dispositivos o usuarios, pero no para ambos. No se puede crear un grupo de dispositivos basado en los atributos de los propietarios de los dispositivos. Las reglas de pertenencia de dispositivo solo pueden hacer referencia a atribuciones de dispositivos.

**Recomendación de cuándo usar identidades externas**

La colaboración B2B es una función de Microsoft Entra External ID que le permite invitar a usuarios invitados a colaborar con su organización. La colaboración B2B le permite compartir de forma segura las aplicaciones y los servicios de la empresa con usuarios externos, 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 Microsoft Entra ID 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. También puede habilitar los flujos de usuario de registro de autoservicio para permitir que los usuarios externos se suscriban a aplicaciones o recursos por sí mismos. Una vez que el usuario externo ha canjeado su invitación o completado el registro, se representa en el directorio como un objeto de usuario. El tipo de usuario para estos usuarios de colaboración B2B normalmente se establece en "invitado" y su nombre principal de usuario contiene el identificador #EXT#.

Los desarrolladores pueden usar las API de negocio a negocio de Microsoft Entra para personalizar el proceso de invitación o escribir aplicaciones como los portales de suscripción de autoservicio.

**Colaboración con cualquier asociado mediante sus identidades**

Con B2B de Microsoft Entra, 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 asociado usa sus propias identidades y credenciales, independientemente de que tengan o no una cuenta de Microsoft Entra.
* 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.

Administración de la colaboración con otras organizaciones y nubes

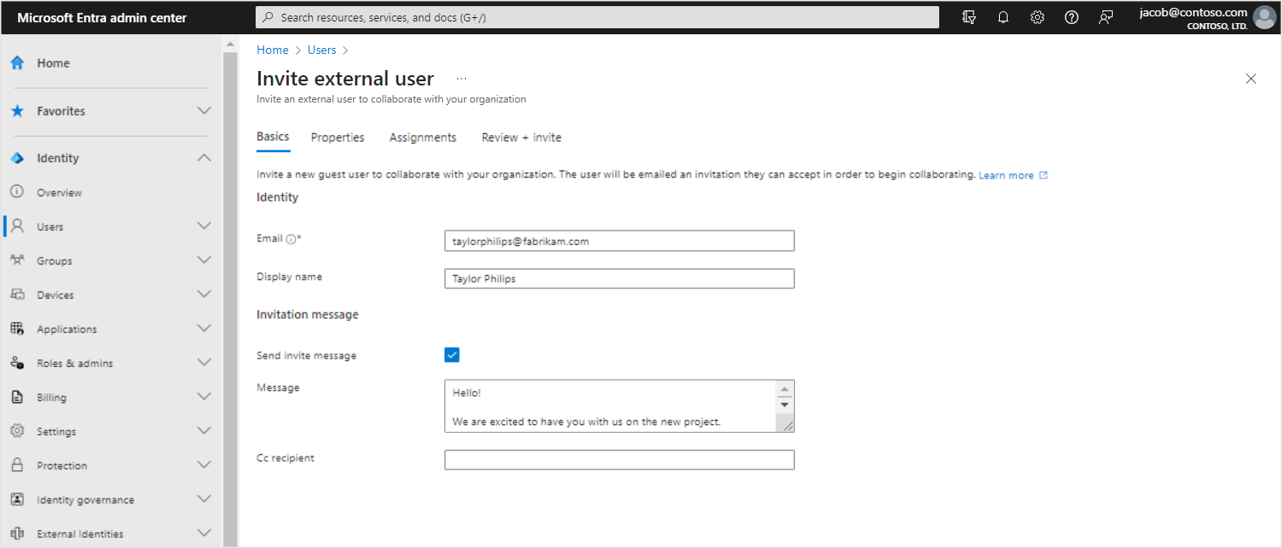
La colaboración B2B está habilitada de forma predeterminada, pero una configuración de administración completa le permite controlar la colaboración B2B entrante y saliente con asociados y organizaciones externos:

* Para la colaboración B2B con otras organizaciones de Microsoft Entra, use la configuración de acceso entre inquilinos. Administre la colaboración B2B entrante y saliente, y limite el acceso a usuarios, grupos y aplicaciones específicos. Establezca una configuración predeterminada que se aplique a todas las organizaciones externas y, luego, cree configuraciones individuales específicas de la organización según sea necesario. Mediante la configuración de acceso entre inquilinos, también puede confiar en la autenticación multifactor (MFA) y las notificaciones de dispositivo (notificaciones de compatibilidad y notificaciones de unión a Microsoft Entra híbrido) de otras organizaciones de Microsoft Entra.
* Use la configuración de colaboración externa para definir quién puede invitar a usuarios externos, permitir o bloquear dominios específicos de B2B y establecer restricciones en el acceso de los usuarios invitados al directorio.
* Utilice Configuración de la nube de Microsoft para establecer una colaboración B2B mutua entre la nube global de Microsoft Azure y Microsoft Azure Government o Microsoft Azure operada por 21Vianet.

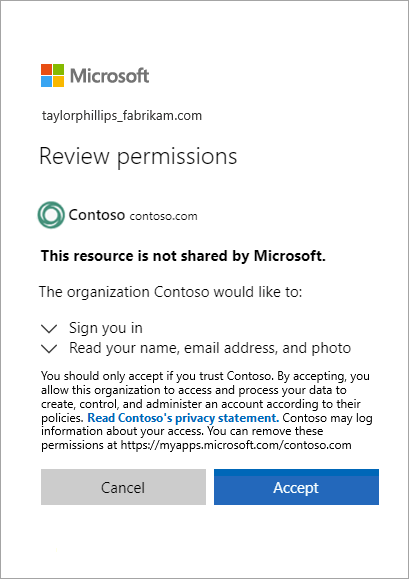
**Invitar fácilmente usuarios invitados desde el Azure Portal**

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

* Cree un usuario invitado en Microsoft Entra ID, 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 envíe un vínculo directo a una aplicación que desee compartir.



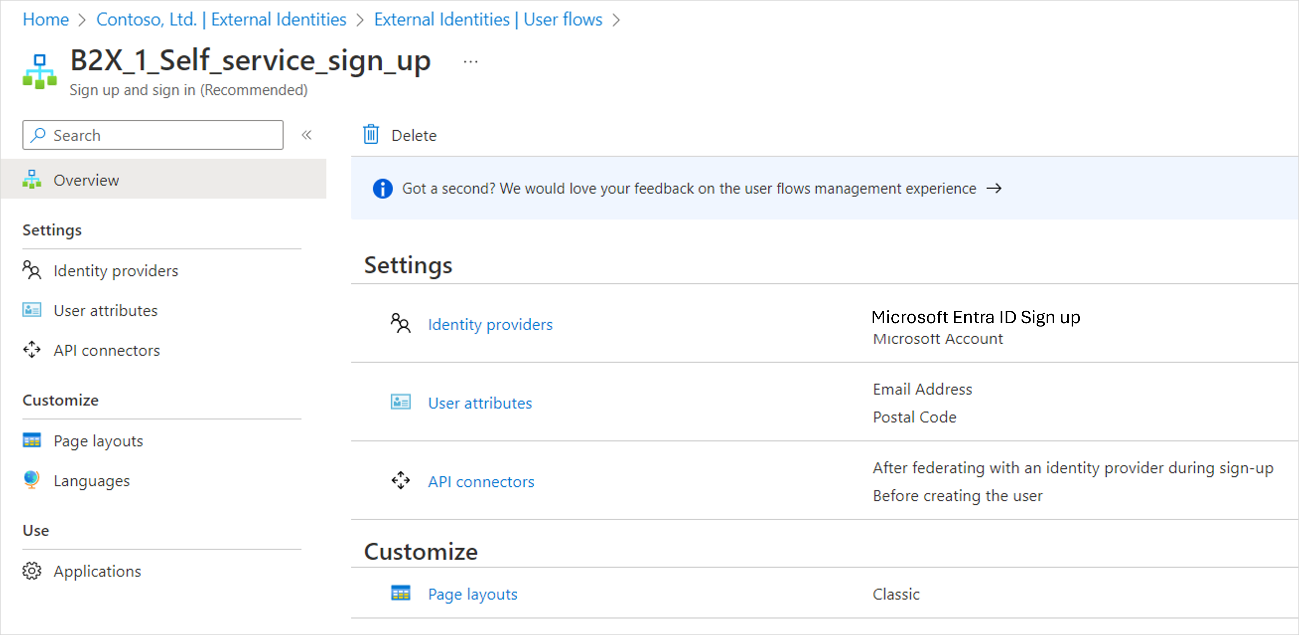
* Los usuarios invitados siguen unos pasos de canje sencillos para iniciar sesión.



**Concesión de permiso del registro de autoservicio**

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.

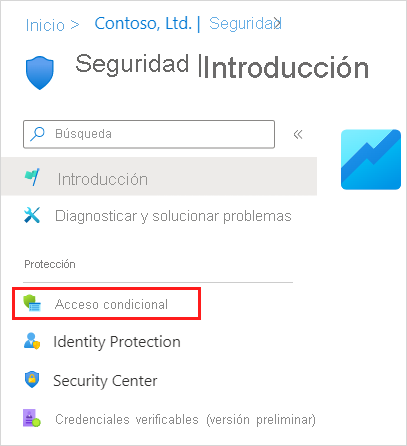
También puede usar conectores de API para integrar los flujos de usuarios de registro de autoservicio con sistemas en la nube externos. Puede conectarse con flujos de trabajo de aprobación personalizados, realizar la comprobación de identidades y validar la información proporcionada por el usuario.



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

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

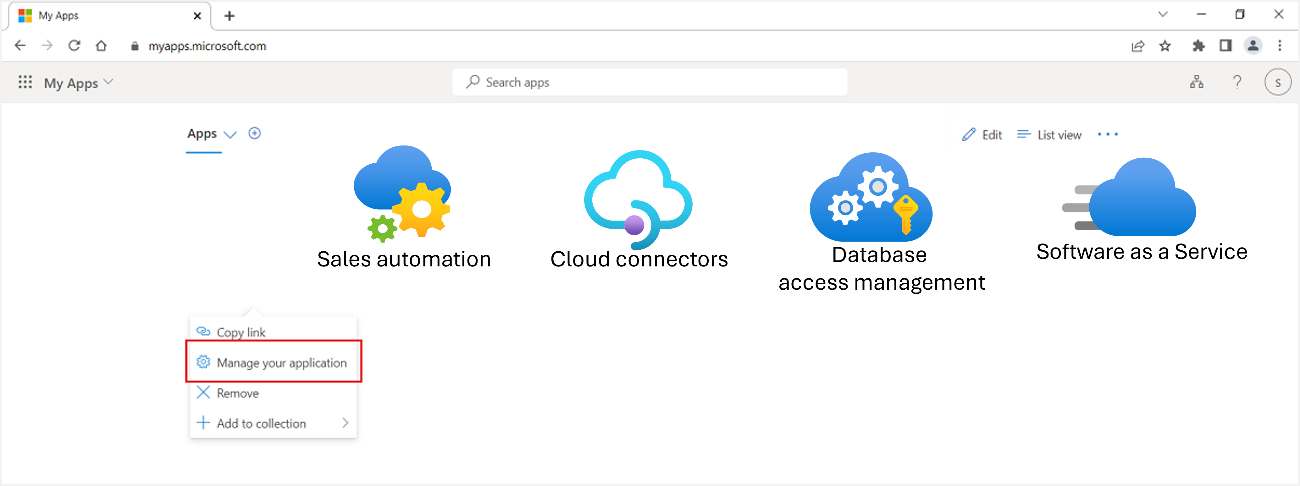
* En el nivel de inquilino.
* En el nivel de aplicación.
* A usuarios invitados específicos para proteger los datos y las aplicaciones empresariales.



**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.



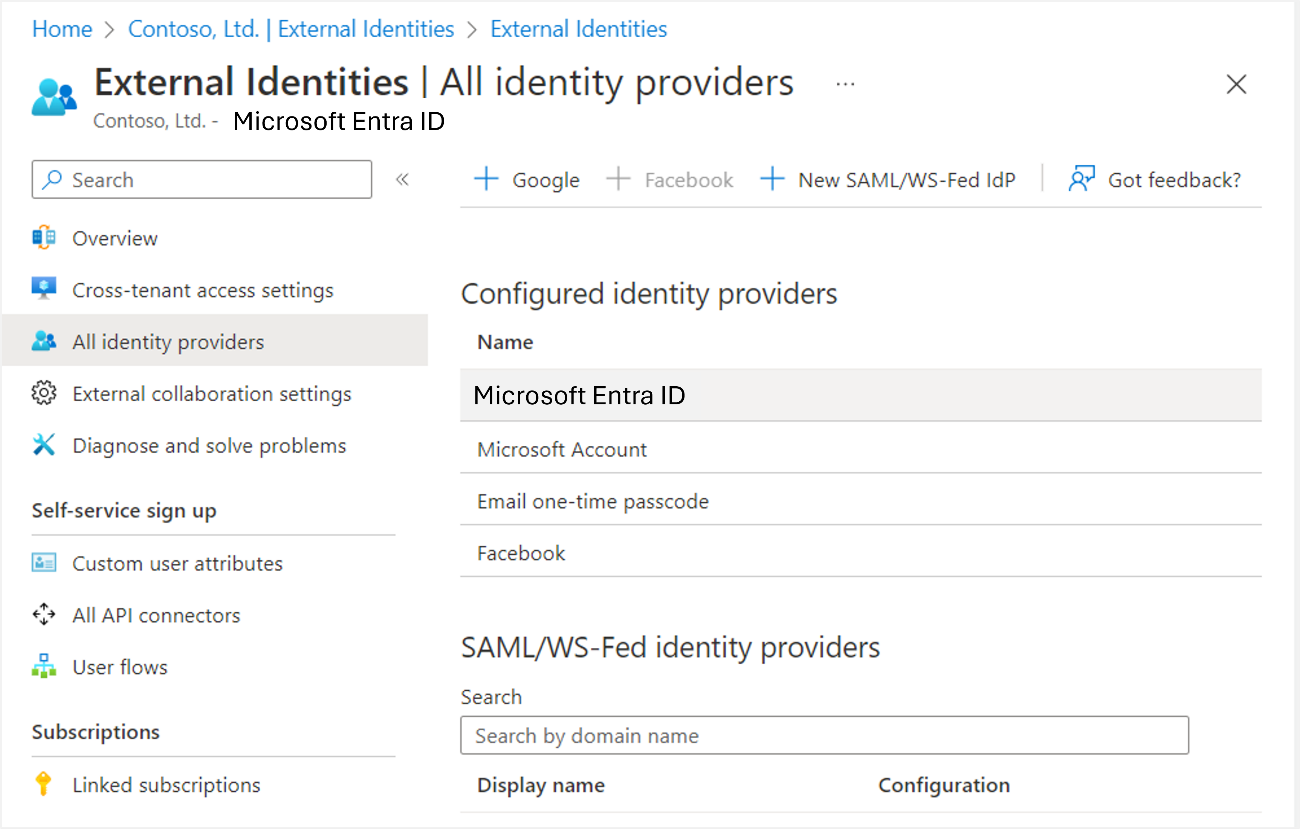
**Personalización de la experiencia de incorporación de usuarios invitados de B2B**

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

* Use la administración de derechos de Microsoft Entra 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.

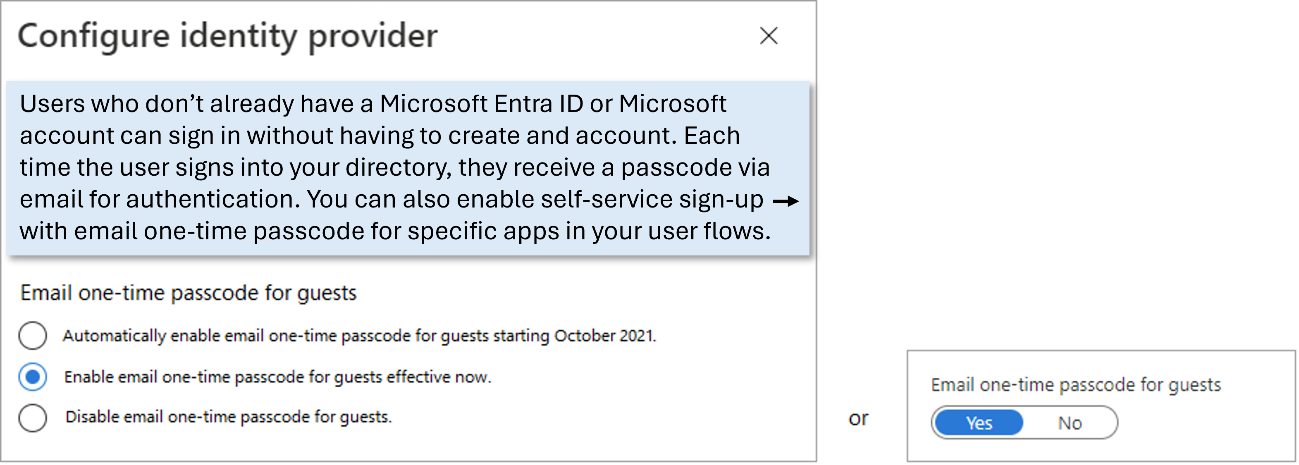
**Integración con proveedores de identidades**

Id. externa de Microsoft Entra admite proveedores de identidades externos, como servicios de redes sociales, cuentas de Microsoft, proveedores de servicios en la nube o proveedores de identidades empresariales. Puede configurar la federación con proveedores de identidades. De este modo, los usuarios externos puedan iniciar sesión con sus cuentas empresariales o sociales existentes en lugar de crear una nueva cuenta solo para la aplicación.



**Integración con SharePoint y OneDrive**

Puede habilitar la integración con SharePoint y OneDrive para compartir archivos, carpetas, elementos de lista, bibliotecas de documentos y sitios con personas ajenas a la organización, mientras usa Azure B2B para la autenticación y administración. Los usuarios con los que comparte recursos suelen ser típicamente usuarios invitados en el directorio, y los permisos y grupos funcionan de la misma manera para estos invitados que como lo hacen para los usuarios internos. Al habilitar la integración con SharePoint y OneDrive, también habilitará la característica de código de acceso de un solo uso de correo electrónico en B2B de Microsoft Entra para que sirva como método de autenticación de reserva.



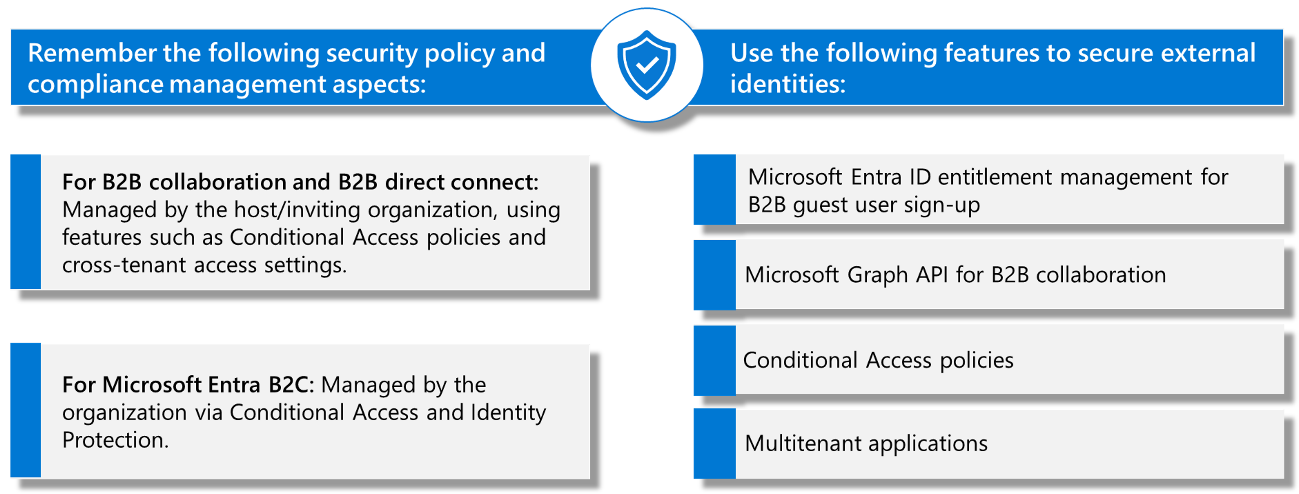
**Protección de identidades externas**

Microsoft Entra External ID hace referencia a todas las formas en las que puede interactuar de forma segura con usuarios fuera de su organización. Si quiere colaborar con asociados, distribuidores o proveedores, puede compartir los recursos y definir cómo los usuarios internos pueden acceder a organizaciones externas. Si es un desarrollador que crea aplicaciones orientadas al consumidor, puede administrar las experiencias de identidad de los clientes.

Con External ID, los usuarios externos pueden "traer sus propias identidades". Tanto si tienen una identidad digital corporativa o gubernamental, como 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 Microsoft Entra ID o Microsoft Entra B2C para mantener protegidos los recursos.

Las siguientes funcionalidades componen External Identities:

* Colaboración B2B: colabore con usuarios externos y permítales usar su identidad preferida para iniciar sesión en las aplicaciones de Microsoft u otras aplicaciones empresariales (aplicaciones SaaS, aplicaciones desarrolladas de forma personalizada, etc.). Los usuarios de colaboración B2B se representan en el directorio, normalmente como usuarios invitados.
* Conexión directa B2B: Establezca una confianza mutua y de dos sentidos con otra organización de Microsoft Entra para una colaboración sin problemas. La conexión directa B2B actualmente es compatible con los canales compartidos de Teams, lo que permite a los usuarios externos acceder a sus recursos desde sus instancias principales de Teams. Los usuarios de conexión directa B2B no se representan en el directorio, pero son visibles desde el canal compartido de Teams y se pueden supervisar en Teams informes del centro de administración.
* Empresa a cliente B2C: publique aplicaciones SaaS modernas o aplicaciones desarrolladas de forma personalizada (excepto aplicaciones de Microsoft) para consumidores y clientes, mientras usa Microsoft Entra B2C para la administración de identidades y acceso.
* Organización multiinquilino de Microsoft Entra: colabore con varios inquilinos en una sola organización de Microsoft Entra a través de la sincronización entre inquilinos.

En función de cómo quiera interactuar con organizaciones externas y los tipos de recursos que necesite compartir, puede usar una combinación de estas funcionalidades. 

**Colaboración B2B**

Con la colaboración B2B, puede invitar a cualquier persona a iniciar sesión en su organización de Microsoft Entra con sus propias credenciales para que puedan acceder a las aplicaciones y los recursos que quiera compartir con ellas. Use la colaboración B2B cuando necesite permitir que los usuarios externos accedan a las aplicaciones de Office 365, las aplicaciones de software como servicio (SaaS) y las aplicaciones de línea de negocio, especialmente cuando el asociado no usa Microsoft Entra ID o es poco práctico para los administradores configurar una conexión mutua a través de la conexión directa B2B. No hay credenciales asociadas a los usuarios de colaboración B2B. Lo que hacen es autenticarse con su organización principal o proveedor de identidades y, luego, su organización comprueba la idoneidad del usuario invitado para la colaboración B2B.

Hay varias maneras de agregar usuarios externos a su organización para la colaboración B2B:

* Invitar a los usuarios a la colaboración B2B mediante sus cuentas de Microsoft Entra, cuentas Microsoft o identidades sociales que habilite, como Google. Un administrador puede usar Azure Portal o PowerShell para invitar a los usuarios a la colaboración B2B. Los usuarios inician sesión en los recursos compartidos con un proceso sencillo de canje con su cuenta profesional o educativa o con cualquier cuenta de correo electrónico.
* Usar flujos de usuario de autoservicio de registro para permitir que los usuarios externos se suscriban ellos mismos a 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.
* Usar la administración de derechos de Microsoft Entra, una característica de gobernanza de identidades que le permite administrar la identidad y el acceso de los usuarios externos a gran escala mediante la automatización de los flujos de trabajo de solicitud de acceso, las asignaciones de acceso, la revisiones y la expiración.

Se crea un objeto de usuario para el usuario de colaboración B2B en el mismo directorio que los empleados. Este objeto de usuario se puede administrar como otros objetos de usuario en el directorio, agregarse a grupos, etc. Puede asignar permisos al objeto de usuario (para la autorización) y permitirles usar sus credenciales existentes (para la autenticación).

Puede usar la configuración de acceso entre inquilinos para administrar la colaboración B2B con otras organizaciones de Microsoft Entra y en las nubes de Microsoft Azure. Para la colaboración B2B con usuarios y organizaciones que no son de Id. externa de Microsoft Entra, use la configuración de colaboración externa.

**Conexión directa B2B**

Conexión directa B2B es una nueva manera de colaborar con otras organizaciones de Microsoft Entra. Actualmente, esta característica funciona con canales compartidos Microsoft Teams. Con conexión directa B2B, se crean relaciones de confianza de dos vías con otras organizaciones de Microsoft Entra para permitir que los usuarios inicien sesión sin problemas en los recursos compartidos y viceversa. Los usuarios de conexión directa B2B no se agregan como invitados a su directorio Microsoft Entra. Cuando dos organizaciones habilitan mutuamente la conexión directa B2B, los usuarios se autentican en su organización principal y reciben un token de la organización de recursos para el acceso. Obtenga más información sobre la conexión directa B2B en Microsoft Entra External ID.

Actualmente, la conexión directa B2B habilita la característica de canales compartidos de Teams Connect, que permite a sus usuarios colaborar con usuarios externos de varias organizaciones con un canal compartido de Teams para chat, llamadas, uso compartido de archivos y uso compartido de aplicaciones. Una vez que haya configurado la conexión directa B2B con una organización externa, las siguientes capacidades de canales compartidos de Teams estarán disponibles:

* Dentro de Teams, el propietario de un canal compartido puede buscar usuarios permitidos de la organización externa y agregarlos al canal compartido.
* Los usuarios externos pueden acceder al canal compartido de Teams sin tener que cambiar de organización o iniciar sesión con una cuenta diferente. Desde Teams, el usuario externo puede acceder a archivos y aplicaciones a través de la pestaña Archivos. El acceso del usuario está determinado por las políticas del canal compartido.

Use la configuración de acceso entre inquilinos para administrar las relaciones de confianza con otras organizaciones de Microsoft Entra y defina las directivas de entrada y salida para la conexión directa B2B.

**Microsoft Entra B2C**

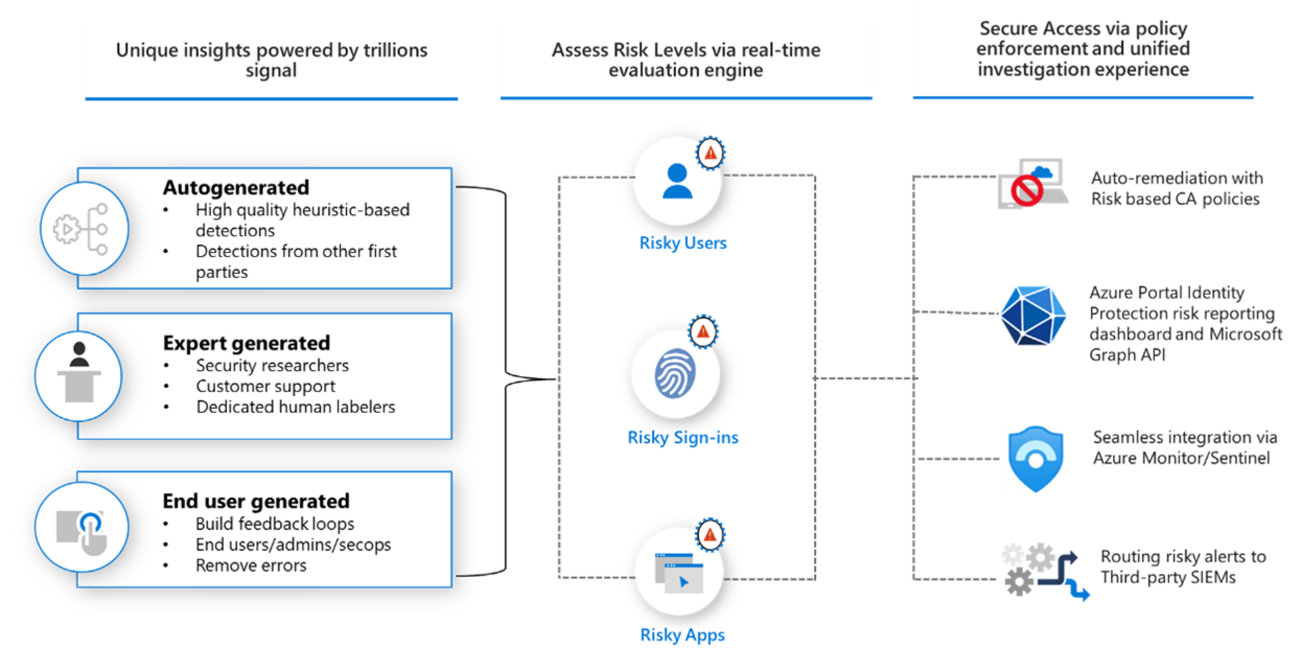
Microsoft Entra B2C es una solución de Administración de identidad y acceso de clientes (CIAM) que le permite desarrollar recorridos de usuario para aplicaciones orientadas al consumidor y al cliente. Si es un desarrollador empresarial o individual que crea aplicaciones orientadas a clientes, puede escalar a millones de consumidores, clientes o ciudadanos mediante Microsoft Entra B2C. Los desarrolladores pueden usar Microsoft Entra B2C como sistema CIAM completo para sus aplicaciones.

Con Microsoft Entra B2C, los clientes pueden iniciar sesión con una identidad que ya han establecido (como redes sociales o plataformas en la nube pública). Puede personalizar y controlar el modo en que los clientes se suscriben, inician sesión y administran sus perfiles al usar las aplicaciones.

Aunque Microsoft Entra B2C se basa en la misma tecnología que la Id. externa de Microsoft Entra, es un servicio independiente con algunas diferencias de características.

**Implementación de Microsoft Entra Identity Protection**

Microsoft Entra ID Protection ayuda a las organizaciones a detectar, investigar y corregir los riesgos relacionados con las identidades. Los riesgos basados en identidades se pueden insertar posteriormente en herramientas como Acceso condicional para tomar decisiones de acceso o alimentar una herramienta de administración de eventos e información de seguridad (SIEM) para realizar una investigación más detallada.



**Detección de riesgos**

Microsoft agrega continuamente y actualiza las detecciones en nuestro catálogo para proteger a las organizaciones. Estas detecciones proceden de nuestros aprendizajes basados en el análisis de billones de señales cada día de Active Directory, Cuentas de Microsoft y juegos de Xbox. Esta amplia gama de señales ayuda a Identity Protection a detectar comportamientos de riesgo como:

* Uso de una dirección IP anónima
* Ataques de difusión de contraseña
* Credenciales con fugas

Durante cada inicio de sesión, Identity Protection ejecuta todas las detecciones de inicio de sesión en tiempo real que generan un nivel de riesgo de inicio de sesión, lo que indica la probabilidad de que el inicio de sesión se haya puesto en peligro. En función de este nivel de riesgo, las directivas se aplican para proteger al usuario y a la organización.

**Investigación**

Se realiza un seguimiento de los riesgos detectados en una identidad con los informes. Identity Protection proporciona tres informes clave para que los administradores investiguen los riesgos y tomen medidas:

* **Detecciones de riesgo:** Cada riesgo detectado se notifica como detección de riesgos.
* **Inicios de sesión de riesgo:** Se notifica un inicio de sesión de riesgo cuando hay una o varias detecciones de riesgo notificadas para ese inicio de sesión.
* **Usuarios de riesgo:** Se notifica un usuario de riesgo cuando se cumple uno o ambos de los siguientes elementos:
  + El usuario tiene uno o varios inicios de sesión de riesgo.
  + Se han notificado una o varias detecciones de riesgo.

**Corrección automática**

Las directivas de acceso condicional basadas en riesgos se pueden habilitar para requerir controles de acceso, como proporcionar un método de autenticación seguro, realizar la autenticación multifactor o realizar un restablecimiento de contraseña seguro en función del nivel de riesgo detectado. Si el usuario completa correctamente el control de acceso, el riesgo se corrige automáticamente.

**Corrección manual**

Cuando la corrección del usuario no está habilitada, un administrador debe revisarlos manualmente en los informes del portal, a través de la API o en Microsoft 365 Defender. Los administradores pueden realizar acciones manuales para descartar, confirmar la seguridad o confirmar el riesgo.

**Uso de los datos**

Los datos de Identity Protection se pueden exportar a otras herramientas para su archivo, posterior investigación y correlación.

Las organizaciones pueden almacenar datos durante más tiempo cambiando la configuración de diagnóstico de Microsoft Entra ID. Pueden optar por enviar datos a un área de trabajo de Log Analytics, archivar datos en una cuenta de almacenamiento, transmitir datos a Event Hubs o enviar datos a otra solución.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. Una empresa quiere colaborar con un proveedor fuera de su organización. ¿Qué funcionalidad de Id. externa de Microsoft Entra deben usar?**

1. Colaboración B2C
2. Autenticación de miembro interno
3. Colaboración B2B

**2. Una organización quiere habilitar la corrección automática para los riesgos basados en identidades detectados por Microsoft Entra ID Protection. ¿Qué controles de acceso se pueden requerir en función del nivel de riesgo detectado?**

1. Bloquear la cuenta del usuario
2. Requerir al usuario que cambie su nombre de usuario
3. Proporcionar un método de autenticación seguro, realizar la autenticación multifactor o realizar un restablecimiento de contraseña seguro

**3. Un administrador de usuarios quiere agregar un nuevo usuario a su organización de Microsoft Entra ID. ¿Qué pasos deben seguir?**

1. Seleccione Invitar a un usuario externo en el menú y proporcione la dirección de correo electrónico del usuario.
2. Vaya a Usuarios de Microsoft Office y seleccione Crear nuevo usuario en el menú.
3. Inicie sesión en Azure Portal en el rol Administrador de usuarios, vaya a Usuarios de Microsoft Entra ID y seleccione Crear nuevo usuario o Invitar a un usuario externo en el menú.

**4. Una empresa quiere gestionar la identidad y el acceso de los usuarios externos a gran escala mediante la automatización de los flujos de trabajo de solicitudes de acceso, las asignaciones de acceso, las revisiones y la caducidad. ¿Qué característica debe usar?**

1. Conexión directa B2B
2. Microsoft Entra B2C
3. Administración de derechos de Microsoft Entra

**5. Una empresa quiere crear una experiencia de registro para usuarios externos que quieran acceder a sus aplicaciones. ¿Qué opciones puede proporcionar como parte del flujo de registro?**

1. La recopilación de información sobre el usuario no es posible en un flujo de usuario de registro de autoservicio.
2. No se pueden usar conectores de API para integrar flujos de usuario de registro de autoservicio con sistemas en la nube externos.
3. Proporcionar opciones para diferentes proveedores de identidades sociales o empresariales.
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, ha aprendido a proteger las identidades de usuario en Microsoft Entra ID, a implementar medidas de seguridad de grupo, a administrar identidades externas de forma segura, a mantener la confidencialidad y a usar Microsoft Entra ID Protection para la identificación y respuesta proactivas frente amenazas.