**Introducción**

Completado100 XP

* 1 minuto

Tradicionalmente, la protección del acceso a los sistemas y los datos significaba establecer controles de acceso físicos en el perímetro de la red local.

Con el aumento del número de usuarios que trabajan desde cualquier lugar, más el auge de las estrategias BYOD (uso de dispositivos personales), las aplicaciones para dispositivos móviles y en la nube, muchos de esos puntos de acceso ya no se encuentran en las redes físicas de la empresa.

La *identidad* se ha convertido en el nuevo límite de seguridad principal. Para mantener el control de los datos, es fundamental que el usuario demuestre con exactitud que es un usuario válido del sistema y que cuenta con un nivel de acceso adecuado. Ahora, los ataques van más dirigidos a esta capa de identidad que a la red.

**Tailwind Traders**

[Tailwind Traders](https://www.tailwindtraders.com/) es una empresa ficticia que distribuye productos para la remodelación del hogar. Esta empresa cuenta con ferreterías minoristas en todo el mundo y en línea.



Tailwind Traders está especializada en precios competitivos, envío rápido y una amplia gama de artículos. Va a examinar las tecnologías en la nube para mejorar las operaciones comerciales y apoyar el crecimiento en nuevos mercados. Al migrar a la nube, la empresa tiene previsto mejorar su experiencia de compra para diferenciarse de sus competidores.

**¿Cómo protege Tailwind Traders el acceso a sus aplicaciones en la nube?**

Los recursos móviles de Tailwind Traders están aumentando, al igual que el número de aplicaciones que la empresa ejecuta en la nube.

A los empleados de las tiendas repartidas por todo el mundo se les entregan tabletas desde las que pueden crear pedidos para los clientes, realizar el seguimiento de las entregas y planear su agenda de trabajo.

Los repartidores pueden usar sus propios dispositivos móviles para acceder a las aplicaciones de logística y programación. Algunos repartidores son empleados fijos de Tailwind Traders. Otros son empleados temporales.

Tailwind Traders usa Active Directory para proteger su entorno local. Necesitan asegurarse de que solo los empleados pueden iniciar sesión y acceder a sus aplicaciones empresariales. También deben asegurarse de que los empleados temporales solo pueden acceder a las aplicaciones cuando están contratados.

¿Cómo puede Azure Active Directory (Azure AD) ayudar a Tailwind Traders a proteger de una manera coherente todas sus aplicaciones, tanto cuando se accede a ellas desde la intranet como desde redes públicas?

**Objetivos de aprendizaje**

Después de completar este módulo, podrá:

* explicar la diferencia entre autenticación y autorización;
* Describir cómo se administran las identidades y el acceso con Azure AD.
* Explicar el papel que desempeñan el inicio de sesión único (SSO), la autenticación multifactor y el acceso condicional en la administración de identidades de usuario.

**Requisitos previos**

* Debe estar familiarizado con la terminología y los conceptos básicos relacionados con la informática.
* Es útil estar familiarizado con la informática en la nube, pero no es necesario.

**Diferencias entre autenticación y autorización**

Completado100 XP

* 2 minutos

Recuerde que Tailwind Traders debe asegurarse de que solo los empleados pueden iniciar sesión y acceder a sus aplicaciones empresariales.

Tailwind Traders también necesita asegurarse de que los empleados solo pueden acceder a las aplicaciones autorizadas. Por ejemplo, todos los empleados pueden acceder al software de inventario y precios, pero solo los directores de tienda pueden acceder al software de nóminas y de cierta contabilidad.

Hay dos conceptos fundamentales que deben entenderse al hablar sobre identidad y acceso: la *autenticación* (AuthN) y la *autorización* (AuthZ).

La autenticación y la autorización admiten todo lo demás que se produzca. Aparecen de manera secuencial en el proceso de identidad y acceso.

Echemos un vistazo a cada una de ellas.

**¿Qué es la autenticación?**

La autenticación es el proceso de establecimiento de la identidad de una persona o servicio que quiere acceder a un recurso. Implica el acto de solicitar a un usuario credenciales legítimas y proporciona la base para la creación de una entidad de seguridad para el control de identidad y de acceso. Determina si el usuario es quien dicen ser.

**¿Qué es la autorización?**

La autenticación establece la identidad del usuario, pero la autorización es el proceso de establecer el nivel de acceso que tiene una persona o un servicio autenticados. Especifica a qué datos puede acceder y qué puede hacer con ellos.

**¿Qué relación existe entre la autenticación y la autorización?**

En este diagrama se muestra la relación entre la autenticación y la autorización:



La tarjeta de identificación representa las credenciales que el usuario tiene para demostrar su identidad. Obtendrá más información sobre los tipos de credenciales más adelante en este módulo. Una vez efectuada la autenticación, la autorización define a qué tipos de aplicaciones, recursos y datos puede acceder el usuario.

**¿Qué es Azure Active Directory?**

Completado100 XP

* 5 minutos

En esta sección, obtendrá información sobre cómo Azure Active Directory (Azure AD) proporciona servicios de identidad que permiten a los usuarios iniciar sesión y acceder tanto a las aplicaciones en la nube de Microsoft como a las que desarrolle personalmente. También verá cómo admite Azure AD el inicio de sesión único (SSO).

Tailwind Traders ya usa Active Directory para proteger sus entornos locales. La empresa no quiere que los usuarios tengan que recordar un nombre de usuario y una contraseña diferentes para acceder a las aplicaciones y los datos en la nube. ¿Puede la empresa integrar sus servicios de identidad existentes de Active Directory con los de la nube a fin de crear una experiencia sin problemas para los usuarios?

Empecemos por ver las diferencias entre Azure AD y Active Directory.

**¿Qué diferencia hay entre Azure AD y Active Directory?**

Active Directory está relacionado con Azure AD, pero hay algunas diferencias importantes.

Microsoft presentó Active Directory en Windows 2000 para ofrecer a las empresas la capacidad de administrar varios sistemas y componentes de la infraestructura local mediante una única identidad por usuario.

En el caso de los entornos locales, Active Directory ejecutado en Windows Server proporciona un servicio de administración de acceso e identidades administrado por su propia organización. Azure AD es un servicio de administración de acceso e identidades basado en la nube de Microsoft. Con Azure AD, usted controla las cuentas de identidad, pero Microsoft garantiza que el servicio esté disponible globalmente. Si ya ha trabajado con Active Directory, Azure AD le resultará familiar.

Si protege las identidades de forma local con Active Directory, Microsoft no supervisa los intentos de inicio de sesión. Si conecta Active Directory con Azure AD, Microsoft puede detectar intentos de inicio de sesión sospechosos para ayudarle a proteger su entorno sin costo adicional. Por ejemplo, Azure AD puede detectar intentos de inicio de sesión desde ubicaciones inesperadas o dispositivos desconocidos.

**¿Quién usa Azure AD?**

Azure AD es para:

* **Administradores de TI**

Los administradores pueden usar Azure AD para controlar el acceso a las aplicaciones y los recursos en función de sus requisitos empresariales.

* **Desarrolladores de aplicaciones**

Con Azure AD, los desarrolladores pueden agregar funcionalidad a las aplicaciones que compilan mediante un enfoque basado en estándares. Por ejemplo, pueden agregar funcionalidad de SSO a una aplicación o habilitar una aplicación para que funcione con las credenciales existentes de un usuario.

* **Usuarios**

Los usuarios pueden administrar sus identidades. Por ejemplo, el autoservicio de restablecimiento de contraseña permite a los usuarios cambiar o restablecer su contraseña sin intervención de un administrador de TI ni del departamento de soporte técnico.

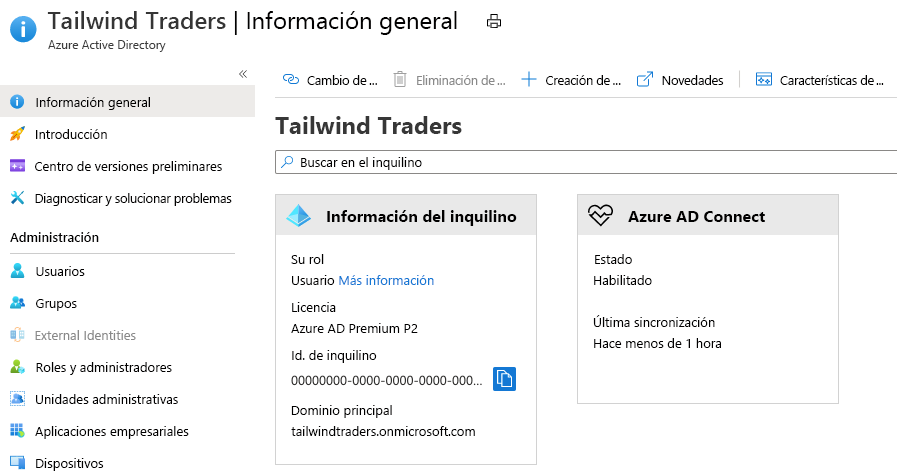
* **Suscriptores de servicios en línea**

Los suscriptores de Microsoft 365, Microsoft Office 365, Azure y Microsoft Dynamics CRM Online ya usan Azure AD.

Un *inquilino* es la representación de una organización. Suele estar separado de otros inquilinos y tiene su propia identidad.

Cada inquilino de Microsoft 365, Office 365, Azure y Dynamics CRM Online es automáticamente un inquilino de Azure AD.

Esta es una captura de pantalla de lo que un administrador de TI podría ver en Azure Portal al trabajar con Active Directory:



**¿Qué servicios proporciona Azure AD?**

Azure AD proporciona servicios como:

* **Autenticación**

Esto incluye la comprobación de la identidad para acceder a aplicaciones y recursos. También incluye funciones como el autoservicio de restablecimiento de contraseña, la autenticación multifactor, una lista personalizada de contraseñas prohibidas y servicios de bloqueo inteligente.

* **Inicio de sesión único**

Gracias al SSO, los usuarios tienen que recordar un solo identificador y una sola contraseña para acceder a varias aplicaciones. Una sola identidad está asociada a un usuario, lo que simplifica el modelo de seguridad. Cuando los usuarios cambian de rol o dejan una organización, las modificaciones de acceso se asocian a esa identidad, lo que reduce considerablemente el esfuerzo necesario para cambiar o deshabilitar cuentas.

* **Administración de aplicaciones**

Con Azure AD, puede administrar las aplicaciones en la nube y locales. Características como Application Proxy, las aplicaciones SaaS, el portal Aplicaciones (también denominado *panel de acceso*) y el inicio de sesión único proporcionan una mejor experiencia de usuario.

* **Administración de dispositivos**

Además de cuentas de usuarios individuales, Azure AD admite el registro de dispositivos. El registro permite administrar los dispositivos a través de herramientas como Microsoft Intune. También permite que las directivas de acceso condicional basadas en dispositivos limiten los intentos de acceso a solo aquellos que proceden de dispositivos conocidos, independientemente de la cuenta de usuario solicitante.

**¿Qué tipos de recursos se pueden proteger con Azure AD?**

Azure AD ayuda a los usuarios a acceder a recursos tanto internos como externos.

Los recursos externos podrían ser Microsoft Office 365, Azure Portal y miles de aplicaciones de software como servicio (SaaS).

Los recursos internos podrían ser aplicaciones de la red corporativa y la intranet, junto con las aplicaciones en la nube desarrolladas por la organización.

**¿Qué es el inicio de sesión único?**

El inicio de sesión único permite a los usuarios iniciar sesión una vez y utilizar esa credencial para acceder a varios recursos y aplicaciones de distintos proveedores.

Más identidades significan más contraseñas para recordar y cambiar. Las directivas de contraseñas pueden variar entre las aplicaciones. A medida que aumentan los requisitos de complejidad, cada vez resultan más difíciles de recordar para los usuarios. Cuantas más contraseñas tenga que administrar un usuario, mayor será el riesgo de que se produzca alguna incidencia de seguridad relacionada con las credenciales.

Piense en el proceso de administrar todas estas identidades. Se ejerce una mayor presión en el departamento de soporte técnico cuando se tienen que ocupar de los bloqueos de cuentas y las solicitudes de restablecimiento de contraseñas. Si un usuario deja una organización, puede resultar complicado hacer un seguimiento de todas las identidades y asegurarse de que están deshabilitadas. Si se pasa por alto una identidad, es posible que se permita el acceso cuando debería haberse eliminado.

Con SSO, tan solo debe recordar un ID y una contraseña. El acceso a todas las aplicaciones se concede a una única identidad que está asociada a un usuario, lo que simplifica el modelo de seguridad. A medida que los usuarios cambian los roles o dejan una organización, el acceso está asociado a una única identidad. Este cambio reduce considerablemente el esfuerzo necesario para cambiar o deshabilitar cuentas. Usar SSO en las cuentas permite a los usuarios administrar más fácilmente su identidad y aumenta la capacidad en términos de seguridad.

Al final de este módulo encontrará recursos sobre cómo habilitar SSO a través de Azure AD.

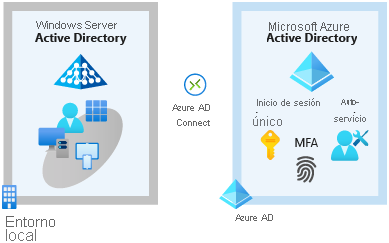
**¿Cómo se puede conectar Active Directory con Azure AD?**

La conexión de Active Directory con Azure AD permite proporcionar una experiencia de identidad coherente a los usuarios.

Hay varias maneras de conectar la instalación de Active Directory existente con Azure AD. Quizás el método más popular es usar Azure AD Connect.

Azure AD Connect sincroniza las identidades de usuario entre la instalación local de Active Directory y Azure AD. Azure AD Connect sincroniza los cambios entre ambos sistemas de identidades, para que pueda usar características como SSO, la autenticación multifactor y el autoservicio de restablecimiento de contraseña en ambos sistemas. El autoservicio de restablecimiento de contraseña impide que los usuarios utilicen contraseñas cuya peligrosidad es conocida.

En el diagrama siguiente se muestra cómo encaja Azure AD Connect entre la instalación local de Active Directory y Azure AD:



A medida que en Tailwind Traders integran su instancia existente de Active Directory con Azure AD, crea un modelo de acceso coherente en toda la organización. De este modo, se simplifica enormemente su capacidad para iniciar sesión en diferentes aplicaciones, administrar cambios en las identidades y el control de los usuarios, así como la supervisión y el bloqueo de los intentos de acceso inusuales.

# ¿Qué son la autenticación multifactor y el acceso condicional?

Completado100 XP

* 4 minutos

Tailwind Traders permite a los repartidores usar sus propios dispositivos móviles para acceder a las aplicaciones de logística y programación. Algunos repartidores son empleados fijos de Tailwind Traders. Otros son empleados temporales. ¿Cómo puede asegurarse el departamento de TI de que un intento de acceso procede realmente de un empleado válido de Tailwind Traders?

En esta parte, obtendrá información sobre dos procesos que habilitan la autenticación segura: Azure AD Multi-Factor Authentication y el acceso condicional. Se comenzará con una breve descripción de la autenticación multifactor en general.

## ¿Qué es la autenticación multifactor?

La autenticación multifactor es un proceso en el que durante el inicio de sesión de un usuario se le solicita una forma adicional de identificación. Entre los ejemplos se incluye un código en su teléfono móvil o un examen de las huellas dactilares.

Piense en cómo inicia sesión en los sitios web, el correo electrónico o los servicios de juegos en línea. Además del nombre de usuario y la contraseña, ¿alguna vez ha tenido que escribir un código que ha recibido en el teléfono? Si es así, ha usado la autenticación multifactor para iniciar sesión.

La autenticación multifactor proporciona seguridad adicional a las identidades, ya que se requieren dos o más elementos para una autenticación completa.

Estos elementos se dividen en tres categorías:

* **Algo que el usuario conoce**

Se podría tratar de una dirección de correo electrónico y una contraseña.

* **Algo que el usuario tiene**

Se podría tratar de un código que se envía al teléfono móvil del usuario.

* **Algo que el usuario es**

Suele ser algún tipo de propiedad biométrica, como la huella dactilar o el escaneo facial utilizados en muchos dispositivos móviles.



La autenticación multifactor aumenta la seguridad de las identidades al limitar el impacto de la exposición de credenciales (por ejemplo, nombres de usuario y contraseñas robados). Si la autenticación multifactor está habilitada, los atacantes que tengan la contraseña de un usuario también necesitarán su teléfono o su huella dactilar para completar la autenticación.

Compare la autenticación multifactor con la autenticación de un solo factor. En la autenticación de un solo factor, los atacantes solo necesitarían el nombre de usuario y la contraseña para autenticarse. La autenticación multifactor se debe habilitar siempre que sea posible, ya que aporta enormes ventajas a la seguridad.

## ¿Qué es Azure AD Multi-Factor Authentication?

Azure AD Multi-Factor Authentication es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor. Azure AD Multi-Factor Authentication permite a los usuarios elegir una forma adicional de autenticación durante el inicio de sesión, como una llamada de teléfono o una notificación de aplicación móvil.

Los servicios siguientes proporcionan funcionalidades de Azure AD Multi-Factor Authentication:

* **Azure Active Directory**

La edición gratuita de Azure Active Directory habilita Azure AD Multi-Factor Authentication para los administradores con el nivel de acceso de Administrador global, a través de la aplicación Microsoft Authenticator, una llamada de teléfono o un código por SMS. También puede aplicar Azure AD Multi-Factor Authentication a todos los usuarios solo a través de la aplicación Microsoft Authenticator. Para ello, se deben habilitar los valores predeterminados de seguridad en el inquilino de Azure AD.

Azure Active Directory Premium (licencias P1 o P2) permite una configuración exhaustiva y detallada de Azure AD Multi-Factor Authentication a través de directivas de acceso condicional (como se explicará en breve).

* **Autenticación multifactor para Office 365**

La suscripción a Office 365 incluye un subconjunto de funcionalidades de Azure AD Multi-Factor Authentication.

Para obtener más información sobre las licencias y las funcionalidades de Azure AD Multi-Factor Authentication, consulte [Versiones disponibles de Azure AD Multi-Factor Authentication](https://docs.microsoft.com/es-ES/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication?azure-portal=true).

## ¿Qué es el acceso condicional?

El acceso condicional es una herramienta que usa Azure Active Directory para permitir (o denegar) el acceso a los recursos en función de señales de identidad. Estas señales incluyen quién es el usuario, dónde se encuentra y desde qué dispositivo solicita el acceso.

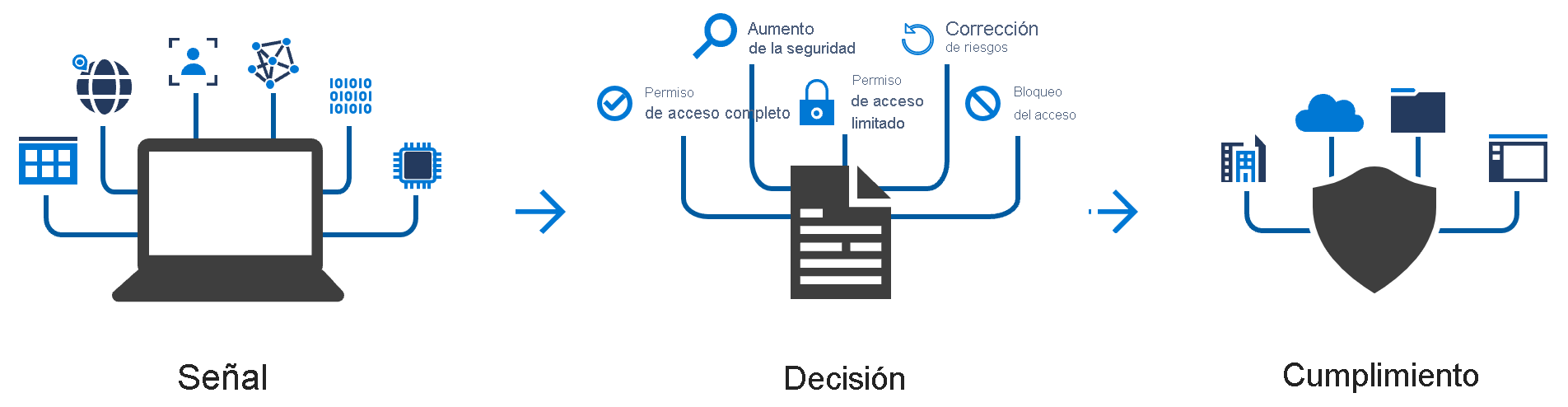
Con el acceso condicional, los administradores de TI pueden:

* permitir a los usuarios ser productivos en cualquier momento y lugar;
* proteger los recursos de la organización.

El acceso condicional también proporciona una experiencia de autenticación multifactor más pormenorizada para los usuarios. Por ejemplo, es posible que al usuario no se le solicite un segundo factor de autenticación si está en una ubicación conocida. Pero si sus señales de inicio de sesión son inusuales o su ubicación es inesperada, es posible que se le exija un segundo factor de autenticación.

Durante el inicio de sesión, el acceso condicional recopila señales del usuario, toma decisiones basadas en esas señales y, después, aplica esa decisión para permitir o denegar la solicitud de acceso, o bien exigir una respuesta de autenticación multifactor.

Este flujo se ilustra en el diagrama siguiente:



En este caso, la señal podría ser la ubicación del usuario, su dispositivo o la aplicación a la que intenta acceder.

En función de estas señales, la decisión puede ser permitir el acceso completo si el usuario inicia sesión desde su ubicación habitual. Si el usuario inicia sesión desde una ubicación inusual o una ubicación marcada como de alto riesgo, el acceso puede bloquearse por completo, o bien podría concederse después de que el usuario proporcione una segunda forma de autenticación.

La aplicación es la acción que lleva a cabo la decisión. Por ejemplo, la acción es permitir el acceso o exigir al usuario que proporcione una segunda forma de autenticación.

### ¿Cuándo se puede usar el acceso condicional?

El acceso condicional resulta útil en los casos siguientes:

* Requerir la autenticación multifactor para acceder a una aplicación.

Puede configurar si todos los usuarios necesitan la autenticación multifactor o solo algunos, como los administradores.

También puede configurar si la autenticación multifactor se aplica al acceso desde todas las redes o solo desde redes que no son de confianza.

* Para requerir el acceso a los servicios solo a través de aplicaciones cliente aprobadas.

Por ejemplo, podría permitir que los usuarios accedan a los servicios de Office 365 desde un dispositivo móvil siempre que usen aplicaciones cliente aprobadas, como Outlook Mobile.

* Exija que los usuarios accedan a la aplicación solo desde dispositivos administrados.

Un dispositivo administrado es un dispositivo que cumple los estándares de seguridad y cumplimiento normativo.

* Para bloquear el acceso desde orígenes que no son de confianza, como ubicaciones desconocidas o inesperadas.

El acceso condicional incluye una herramienta What If que le ayuda a planear las directivas de acceso condicional y a solucionar problemas relacionados con ellas. Puede usar esta herramienta para modelar las directivas de acceso condicional propuestas y aplicarlas en intentos de inicio de sesión recientes de los usuarios para ver cuál sería el efecto de las directivas si se hubieran habilitado. La herramienta What If permite probar las directivas de acceso condicional propuestas antes de implementarlas.

### ¿Dónde está disponible el acceso condicional?

Para usar el acceso condicional, se necesita una licencia Azure AD Premium P1 o P2. Si tiene una licencia de Microsoft 365 Empresa Premium, también tiene acceso a las características de acceso condicional.