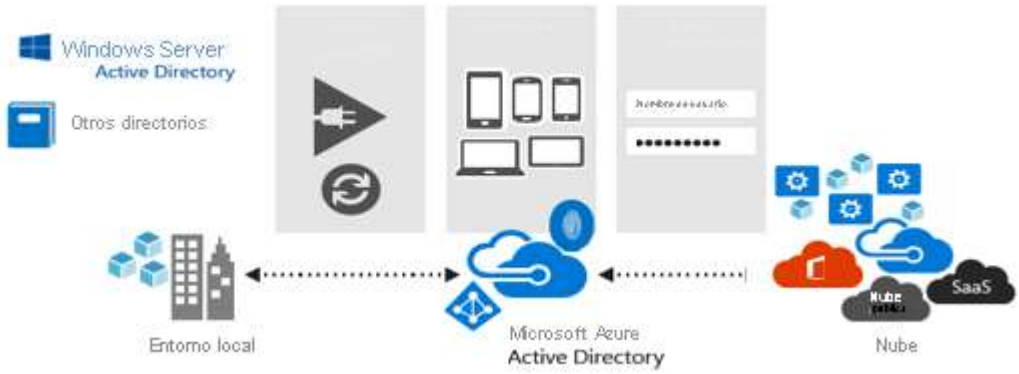
Exploración de las características de Azure Active Directory

Azure Active Directory (Azure AD) es el servicio de administración de identidades y directorios basado en la nube multiinquilino de Microsoft. Para los administradores de TI, Azure AD proporciona una solución asequible y fácil de usar para proporcionar a los empleados y asociados empresariales acceso de inicio de sesión único (SSO) a miles de aplicaciones SaaS en la nube como Office365, Salesforce, DropBox y Concur.

Para los desarrolladores de aplicaciones, Azure AD permite al usuario centrarse en la creación de su aplicación facilitando y acelerando la integración de la misma con una solución de administración de identidades de clase mundial usada por millones de organizaciones de todo el mundo.



Funcionalidades de administración de identidades e integración

Azure AD también incluye un conjunto completo de funcionalidades de administración de identidades, como la autenticación multifactor, el registro de dispositivos, la administración de contraseñas de autoservicio, la administración de grupos de autoservicio, la administración de cuentas con privilegios, el control de acceso basado en roles, la supervisión del uso de aplicaciones, la auditoría y la supervisión de seguridad enriquecidas, y las alertas. Estas funcionalidades pueden ayudar a proteger las aplicaciones basadas en la nube, optimizar los procesos de TI, reducir los costos y ayudar a garantizar que se cumplen los objetivos de cumplimiento corporativo.

Además, Azure AD se puede integrar con un directorio de Windows Server Active Directory existente, lo que proporciona a las organizaciones la capacidad de aprovechar sus inversiones locales en identidad para administrar el acceso a las aplicaciones SaaS basadas en la nube.

Ediciones de Azure AD

Azure Active Directory se presenta en cuatro ediciones: **Gratis**, **Aplicaciones de Microsoft 365**, **Premium P1** y **Premium P2**. La edición Free se incluye con una suscripción de Azure. Las ediciones Premium están disponibles mediante un Contrato Enterprise de Microsoft, el

programa Licencia por volumen abierto y el programa Proveedores de soluciones en la nube. Los suscriptores de Azure y Microsoft 365 también pueden comprar Azure Active Directory Premium P1 y P2 en línea.

Característica	Gratis	Aplicaciones de Microsoft 365	Premium P1	Premium P2
Objetos de directorio	500.000	Sin límite	Sin límite	Sin límite
Inicio de sesión único	Sin límite	Sin límite	Sin límite	Sin límite
Administración de identidades y acceso principales	X	X	X	X
Colaboración de negocio a negocio	X	X	X	X
Administración de identidades y acceso para aplicaciones de Microsoft 365		X	X	X
Características de la edición Premium			X	X
Identidades híbridas			X	X
Administración avanzada de acceso a grupos			X	X
Acceso condicional			X	X
Protección de identidad				X
Identity Governance				X

- **Azure Active Directory Free**: proporciona administración de grupos y usuarios, sincronización de directorios locales, informes básicos e inicio de sesión único en Azure, Microsoft 365 y muchas aplicaciones SaaS populares.
- **Aplicaciones de Microsoft 365 de Azure Active Directory**: esta edición se incluye con O365. Además de incluir las características de la versión Gratis, esta edición proporciona Administración de identidades y acceso para aplicaciones de Microsoft 365, incluida la personalización de marca, MFA, administración de acceso a grupos y autoservicio de restablecimiento de contraseña para los usuarios en la nube.
- **Azure Active Directory Premium P1**: además de las características gratuitas, P1 también permite a los usuarios 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 (un conjunto de administración local de identidades y acceso) y funcionalidades de reescritura en la nube, que permiten el restablecimiento de contraseña de autoservicio a los usuarios locales.

- **Azure Active Directory Premium P2** Además de las características de las licencias Gratis y P1, la licencia P2 ofrece también Azure Active Directory Identity Protection, que proporciona acceso condicional basado en riesgos a las aplicaciones y datos críticos de la compañía, así como Privileged Identity Management, que permite detectar, restringir y supervisar los administradores y su acceso a los recursos, además de proporcionar acceso Just-In-Time cuando sea necesario.

La página de precios de Azure Active Directory contiene información detallada sobre lo que se incluye en cada una de las ediciones. En función de la lista de características, ¿qué edición necesita su organización?

Nota

Si es un cliente de Microsoft 365, Azure o Dynamics CRM Online, es posible que no se dé cuenta de que ya está usando Azure AD. Cada inquilino de Microsoft 365, Azure y Dynamics CRM ya es un inquilino de Azure AD. Siempre que quiera, puede empezar a usar ese inquilino para administrar el acceso a miles de otras aplicaciones en la nube con las que se integra Azure AD.

Comparación de Azure AD y Active Directory Domain Services

Azure AD es diferente de AD DS: aunque Azure AD tiene muchas semejanzas con AD DS, también hay muchas diferencias. Es importante tener en cuenta que el uso de Azure AD es distinto de implementar un controlador de dominio de Active Directory en una máquina virtual de Azure y agregarlo a su dominio local. Estas son algunas de las características de Azure AD que lo hacen diferente.

- **Solución de identidad.** Azure AD es principalmente una solución de identidad y está diseñado para aplicaciones basadas en Internet al usar las comunicaciones HTTP y HTTPS.
- **Consulta de API REST.** Dado que Azure AD está basado en HTTP o HTTPS, no se puede consultar mediante LDAP. En su lugar, Azure AD usa la API REST sobre HTTP y HTTPS.
- **Protocolos de comunicación.** Debido a que Azure AD está basado en HTTP o HTTPS, no usa la autenticación Kerberos. En su lugar, usa los protocolos HTTP y HTTPS, como SAML, WS-Federation y OpenID Connect para la autenticación, así como OAuth para la autorización.
- **Servicios de autenticación.** Incluya SAML, WS-Federation o bien OpenID.
- **Servicio de autorización.** Usa OAuth.
- **Servicios de federación.** Azure AD incluye servicios de federación y muchos servicios de terceros (como Facebook).

- **Estructura plana.** Los usuarios y grupos de Azure AD se crean en una estructura plana y no hay unidades organizativas (UO) ni objetos de directiva de grupo (GPO).

En la tabla siguiente se resumen las diferencias

Azure Active Directory	Active Directory Domain Services
Nube	Local
Diseñado para HTTP y HTTPS	Consulta a través de LDAP
Consultado a través de la API REST	Usa Kerberos para la autenticación
Usa SAML, WS-Federation o bien OpenID para la autenticación	Sin servicios federados
Usa OAuth para la autorización	Unidades organizativas (UO)
Incluye servicios de federación	Directiva de grupo (GPO)
Estructura plana	

Investigación de roles en Azure AD

Con Azure Active Directory (Azure AD), puede designar administradores limitados que administren tareas de identidad en roles con menos privilegios. Los administradores se pueden asignar para realizar tareas como agregar usuarios o cambiarlos, asignar roles administrativos, restablecer contraseñas de usuario, administrar licencias de usuario y administrar nombres de dominio. **Los permisos de usuario predeterminados solo se pueden cambiar en la configuración de usuario de Azure AD**.

Limitación del uso de administradores globales

Los usuarios que tienen asignado el rol Administrador global pueden leer y modificar cada configuración administrativa de la organización de Azure AD. De manera predeterminada, a la persona que se suscribe a Azure se le asigna el rol Administrador global para la organización de Azure AD. Solo los administradores globales y los que tengan un rol con privilegios pueden delegar roles de administrador. Para reducir el riesgo para su negocio, le recomendamos asignar este rol a la menor cantidad posible de personas de su organización.

Como procedimiento recomendado, se recomienda asignar este rol a menos de cinco personas de la organización. Si tiene más de cinco usuarios asignados al rol Administrador global en la organización, estas son algunas maneras de reducir el uso.

Roles disponibles

- **Administrador de aplicaciones**: los usuarios con este rol pueden crear y administrar todos los aspectos de las aplicaciones empresariales, los registros de aplicaciones y la configuración del proxy de aplicación.
- **Desarrollador de aplicaciones**: los usuarios con este rol pueden crear registros de aplicación cuando el valor "Los usuarios pueden registrar aplicaciones" está establecido en Sí.
- **Administrador de autenticación**: los usuarios con este rol pueden establecer o restablecer credenciales sin contraseña para algunos usuarios y pueden actualizar las contraseñas de todos los usuarios.
- **Administrador de Azure DevOps**: los usuarios con este rol pueden administrar la directiva de Azure DevOps para restringir la creación de nuevas organizaciones de Azure DevOps organización a un conjunto de usuarios o grupos configurables.
- **Administrador de Azure Information Protection**: los usuarios con este rol tienen todos los permisos en el servicio Azure Information Protection.
- **Administrador de flujos de usuario de B2C**: los usuarios con este rol pueden crear y administrar flujos de usuario de B2C (también llamados directivas "integradas") en Azure Portal.
- **Administrador de atributos de flujos de usuario de B2C**: los usuarios con este rol agregan o eliminan atributos personalizados disponibles para todos los flujos de usuario del inquilino.
- **Administrador de conjuntos de claves IEF de B2C**: el usuario puede crear y administrar claves de directiva y secretos para el cifrado de tokens, las firmas de token y el cifrado y descifrado de notificaciones.
- **Administrador de directivas IEF de B2C**: los usuarios con este rol pueden crear, leer, actualizar y eliminar todas las directivas personalizadas de Azure AD B2C y, por tanto, tener control total sobre Identity Experience Framework en el inquilino de Azure AD B2C correspondiente.
- **Administrador de facturación**: realiza compras, administra suscripciones e incidencias de soporte técnico, y supervisa el estado del servicio.
- **Administrador de aplicaciones en la nube**: los usuarios con este rol tienen los mismos permisos que el rol de administrador de la aplicación, excluida la capacidad de administrar el proxy de aplicación.

- **Administrador de dispositivos en la nube**: los usuarios con este rol pueden habilitar, deshabilitar y eliminar dispositivos en Azure AD y leer las claves de BitLocker de Windows 10 (si están presentes) en Azure Portal.
- **Administrador de cumplimiento**: los usuarios con este rol tienen permisos para administrar características relacionadas con el cumplimiento en el centro de cumplimiento de Microsoft 365, el centro de administración de Microsoft 365 y el centro de seguridad y cumplimiento de Microsoft 365.
- **Administrador de datos de cumplimiento**: los usuarios con este rol tienen permisos para realizar el seguimiento de los datos del centro de cumplimiento de Microsoft 365, el centro de administración de Microsoft 365 y Azure. Los usuarios también pueden realizar un seguimiento de los datos de cumplimiento en Exchange centro de administración.
- **Administrador del acceso condicional**: los usuarios con este rol pueden administrar la configuración de acceso condicional de Azure Active Directory.
- **Administrador de Exchange**: los usuarios con este rol tienen permisos globales en Microsoft Exchange Online, cuando el servicio está presente.
- **Lectores de directorios**: los usuarios de este rol pueden leer información básica del directorio.
- **Administrador global/Administrador de empresa**: los usuarios con este rol tienen acceso a todas las características administrativas de Azure Active Directory, así como a los servicios que usan identidades de Azure Active Directory como el centro de seguridad de Microsoft 365, el centro de cumplimiento de Microsoft 365, Exchange Online, SharePoint Online y Skype Empresarial Online.
- **Administrador de grupos**: los usuarios de este rol pueden crear o administrar grupos y su configuración, como las directivas de nomenclatura y expiración.
- **Administrador de seguridad**: los usuarios con este rol tienen permisos para administrar características relacionadas con la seguridad en el centro de seguridad de Microsoft 365, Azure Active Directory Identity Protection, Azure Information Protection y el centro de seguridad y cumplimiento de Microsoft 365.

En la mayoría de las organizaciones, la seguridad de los recursos empresariales depende de la integridad de las cuentas con privilegios que administran los sistemas de TI. Los ciberatacantes se centran en el acceso con privilegios a los sistemas de la infraestructura (como Active Directory y Azure Active Directory) para obtener acceso a información confidencial de una organización.

Los enfoques tradicionales que se centran en proteger los puntos de entrada y salida de una red como perímetro de seguridad principal son menos eficaces debido al aumento del uso de aplicaciones SaaS y dispositivos personales en Internet. La sustitución natural del perímetro de seguridad de red en las complejas empresas modernas son los controles de autenticación y autorización en la capa de identidad de una organización.

Las cuentas administrativas con privilegios controlan eficazmente este nuevo **perímetro de seguridad**. Es fundamental proteger el acceso con privilegios, independientemente de si el entorno es local, en la nube o en servicios híbridos locales y hospedados en la nube. La protección del acceso contra determinados adversarios requiere que se adopte un enfoque global y bien analizado para proteger los sistemas de su organización de todo riesgo.

Implementación de Azure AD Domain Services

Azure Active Directory Domain Services (Azure AD DS) proporciona servicios de dominio administrados como, por ejemplo, unión a un dominio, directiva de grupo, protocolo ligero de acceso a directorios (LDAP) y autenticación Kerberos/NTLM, que son totalmente compatibles con Windows Server Active Directory. Puede usar estos servicios de dominio sin necesidad de implementar o administrar los controladores de dominio de la nube, ni de aplicarles revisiones. Azure AD DS se integra con el inquilino de Azure AD existente, lo que posibilita que los usuarios inicien sesión con sus credenciales existentes. También puede usar los grupos y las cuentas de usuario existentes para proteger el acceso a los recursos, lo que ofrece una mejor migración mediante lift-and-shift de los recursos en el entorno local a Azure.

Azure AD DS replica la información de identidad desde Azure AD, por lo que funciona con los inquilinos de Azure AD que solo están en la nube o se sincronizan con un entorno de Active Directory Domain Services (AD DS) local. El mismo conjunto de características de Azure AD DS existen para ambos entornos.

- Si tiene un entorno de AD DS local, puede sincronizar la información de las cuentas de usuario para proporcionar una identidad coherente para los usuarios.
- En el caso de los entornos solo en la nube, no se necesita un entorno de AD DS local tradicional para usar los servicios de identidad centralizados de Azure AD DS.

Características y ventajas de Azure AD DS

Para proporcionar servicios de identidad a aplicaciones y máquinas virtuales en la nube, Azure AD DS es totalmente compatible con un entorno de AD DS tradicional para las operaciones como la unión a un dominio, LDAP seguro (LDAPS), la administración de DNS y directiva de grupo, y el enlace LDAP y la compatibilidad con la lectura. La compatibilidad con la escritura LDAP está

disponible para los objetos creados en el dominio administrado con Azure AD DS, pero no los recursos sincronizados desde Azure AD. Las siguientes características de Azure AD DS simplifican las operaciones de implementación y administración:

- **Experiencia de implementación simplificada**: Azure AD DS está habilitado para el inquilino de Azure AD mediante un único asistente en Azure Portal.
- **Integrado con Azure AD**: las cuentas de usuario, las pertenencias a grupos y las credenciales están disponibles automáticamente en el inquilino de Azure AD. Los nuevos usuarios, grupos o cambios de atributos que se producen en el inquilino o en el directorio en el entorno local de Azure AD se sincronizan automáticamente con Azure AD DS.
- **Uso de sus credenciales/contraseñas corporativas**: las contraseñas de los usuarios en Azure AD DS son las mismas que en su inquilino de Azure AD. Los usuarios pueden utilizar sus credenciales corporativas para las máquinas de unión al dominio, iniciar sesión de forma interactiva o a través de escritorio remoto y autenticarse en el dominio administrado de Azure AD DS.
- **Autenticación NTLM y Kerberos**: con la compatibilidad con la autenticación NTLM y Kerberos, puede implementar aplicaciones que dependen de la autenticación integrada en Windows.
- **Alta disponibilidad**: Azure AD DS incluye varios controladores de dominio, que proporcionan alta disponibilidad para el dominio administrado. Esta alta disponibilidad garantiza el tiempo de actividad del servicio y la resistencia a los errores.

En las regiones que admiten Azure Availability Zones, estos controladores de dominio también se distribuyen entre zonas para obtener resistencia adicional.

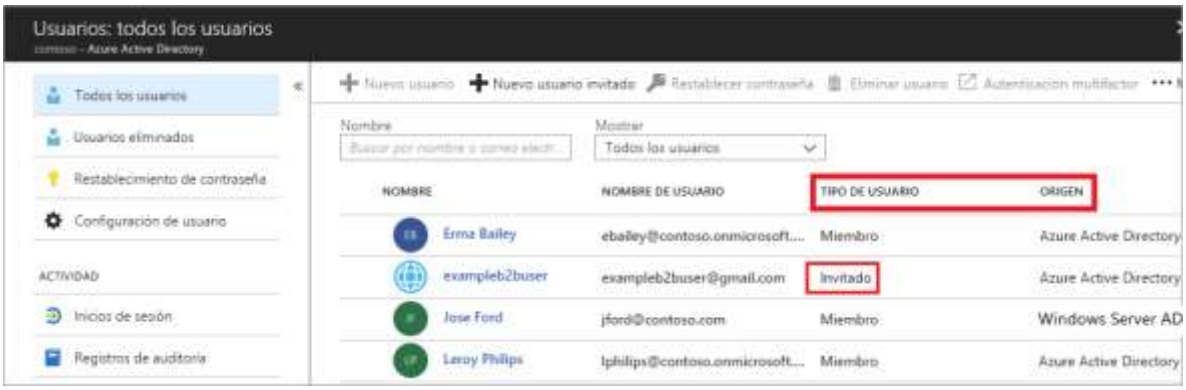
Importante

Azure AD DS se integra con Azure AD, que se puede sincronizar con un entorno de AD DS local. Esta capacidad amplía los casos de uso de identidad central a las aplicaciones web tradicionales que se ejecutan en Azure como parte de una estrategia de migración mediante lift-and-shift.

Creación y administración de usuarios de Azure AD

En Azure AD, cada usuario que necesita acceso a los recursos de Azure precisa una cuenta de usuario. Una cuenta de usuario es un objeto de Active Directory Domain Services (AD DS) o un objeto de usuario de Azure AD sincronizado que contiene toda la información necesaria para autenticar y autorizar al usuario durante el proceso de inicio de sesión y para compilar el token de acceso del usuario.

Para ver los usuarios de Azure AD, acceda a la hoja **Todos los usuarios**. Dedique un minuto a acceder al portal y ver los usuarios. Observe las columnas **TIPO DE USUARIO** y **ORIGEN**, que se ilustran en la imagen siguiente.



Normalmente, Azure AD define usuarios de tres maneras:

- **Identidades de nube**: estos usuarios solo existen en Azure AD. Algunos ejemplos son las cuentas de administrador y los usuarios que usted mismo administra. Su origen es Azure AD.
- **Identidades sincronizadas con Directory**: estos usuarios existen en una instancia de Active Directory local. Una actividad de sincronización que se realiza a través de **Azure AD Connect** lleva a estos usuarios a Azure.
- **Usuarios invitados**: estos usuarios se encuentran fuera de Azure. Algunos ejemplos son las cuentas de otros proveedores de nube y cuentas Microsoft.

Administración de usuarios con grupos de Azure AD

Azure AD permite definir dos tipos de grupos diferentes.

- **Grupos de seguridad**. Son los más comunes y se usan para administrar el acceso de miembros y del equipo a los recursos compartidos de un grupo de usuarios. Por ejemplo, puede crear un grupo de seguridad relativo a una directiva de seguridad específica. De esta forma, puede conceder una serie de permisos a todos los miembros a la vez, en lugar de tener que agregarlos a cada miembro individualmente. Esta opción requiere un administrador de Azure AD.
- **Grupos de Microsoft 365** Estos grupos brindan oportunidades de colaboración al conceder acceso a los miembros a un correo compartido, calendarios, archivos, un sitio de SharePoint y mucho más. Esta opción también permite ofrecer acceso al grupo a personas de fuera de la organización. Esta opción está disponible para los usuarios, así como para los administradores.

Existen diferentes maneras de asignar derechos de acceso a grupos:

- **Asignado**. Le permite agregar usuarios específicos para que sean miembros de este grupo y para 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 revisa las reglas de grupo dinámico del directorio para determinar si el miembro cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de reglas (se quita).
- **Dispositivo dinámico (solo grupos de seguridad)**. Le permite usar reglas de grupo dinámico para agregar y quitar dispositivos automáticamente. Si los atributos de un dispositivo cambian, el sistema revisa las reglas de grupo dinámico del directorio para determinar si el dispositivo cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de reglas (se quita).

Importante

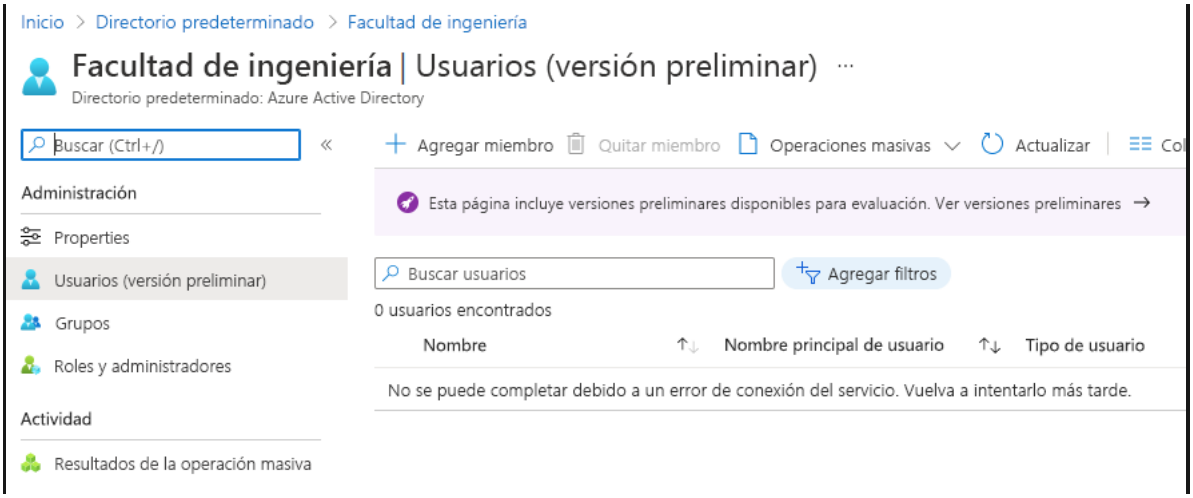
¿Ha pensado en qué grupos debe crear? ¿Asignaría la pertenencia de forma directa o dinámica?

Configuración de unidades administrativas de Azure AD

Una unidad administrativa es un recurso de Azure AD que puede ser un contenedor para otros recursos de Azure AD. Una unidad administrativa solo puede contener usuarios y grupos. Las unidades administrativas restringen los permisos de un rol a cualquier parte de la organización que defina. Por ejemplo, podría usar unidades administrativas para delegar el rol Administrador del departamento de soporte técnico a los especialistas de soporte técnico regionales, para que solo puedan administrar los usuarios de la región en cuestión.

Nota

Para usar unidades administrativas, necesita una licencia de Azure Active Directory Premium para cada administrador de unidad administrativa y licencias gratuitas de Azure Active Directory para los miembros de las unidades administrativas.



Roles disponibles

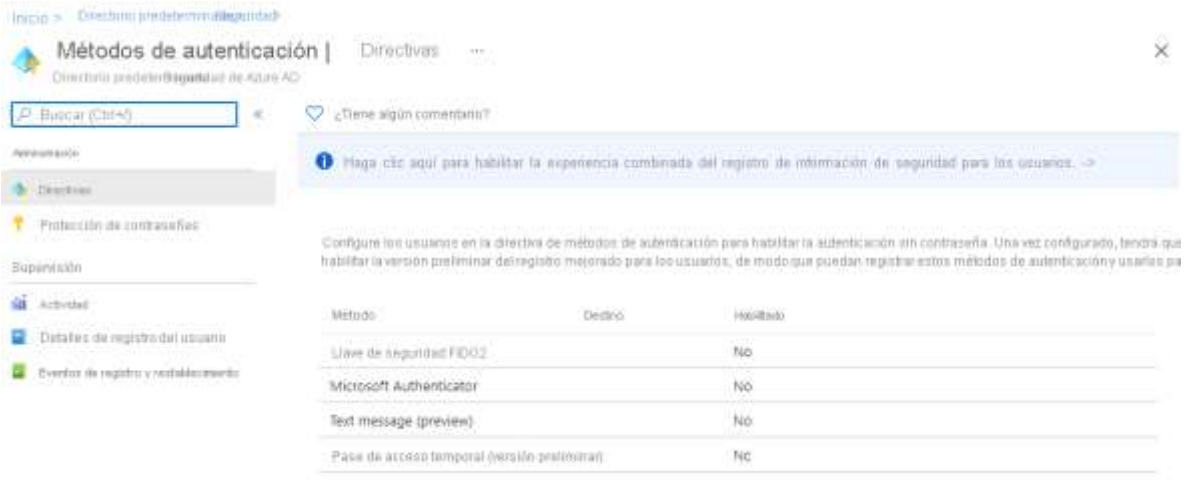
Rol	Descripción
Administrador de autenticación	Tiene acceso para ver, configurar y restablecer la información de los métodos de autenticación de cualquier usuario que no sea administrador solo en la unidad administrativa asignada.
Administrador de grupos	Puede administrar todos los aspectos de los grupos y la configuración de estos, como las directivas de nomenclatura y expiración, solo en la unidad administrativa asignada.
Administrador del departamento de soporte técnico	Puede restablecer contraseñas de usuarios que no son administradores y de administradores del departamento de soporte técnico solo en la unidad administrativa asignada.
Administrador de licencias	Puede asignar, quitar y actualizar las asignaciones de licencia solo dentro de la unidad administrativa.
Administrador de contraseñas	Puede restablecer contraseñas de usuarios que no son administradores y de administradores de contraseña solo en la unidad administrativa asignada.
Administrador de usuarios	Puede administrar todos los aspectos de usuarios y grupos, incluido el restablecimiento de contraseñas para administradores limitados solo en la unidad administrativa asignada.

Implementación de la autenticación sin contraseña

Inicie sesión sin usar nunca una contraseña. Con la autenticación sin contraseña, la contraseña se sustituye por algo que tiene más algo que usted es o algo que conoce. Por ejemplo, en Windows Hello para empresas se puede usar un gesto biométrico, como la cara o la huella digital, o un PIN específico del dispositivo que no se transmite a través de la red.

Métodos de autenticación sin contraseña

- **Windows Hello para empresas**: las credenciales biométricas y el PIN se vinculan directamente al equipo del usuario, lo que impide el acceso de cualquier persona que no sea el propietario.
- **Claves de seguridad FIDO2**: generalmente almacenadas en una unidad USB, las claves de seguridad FIDO2 son un método de autenticación sin contraseña basado en estándares que no permite la suplantación de identidad y que puede venir en cualquier factor de forma.
- **Aplicación Microsoft Authenticator**: la aplicación Authenticator convierte cualquier teléfono iOS o Android en una credencial segura y sin contraseña. Los usuarios pueden iniciar sesión en cualquier plataforma o explorador con este proceso: reciben una notificación en su teléfono, comprueban que el número mostrado en la pantalla coincide con el de su teléfono y, a continuación, usan datos biométricos (reconocimiento táctil o facial) o el PIN para confirmarlo.
- **Tarjetas inteligentes FIDO2 (versión preliminar)**: nuevo método para usar claves FIDO2 para iniciar sesión sin contraseña a través de una tarjeta inteligente.
- **Pase de acceso temporal (versión preliminar)**: el código de acceso de tiempo limitado le permite configurar las claves de seguridad y Microsoft Authenticator sin tener que usar, y mucho menos conocer, su contraseña.



Ventajas de la autenticación sin contraseña

- **Mayor seguridad**: reduzca el riesgo de ataques de suplantación de identidad (phishing) y de difusión de contraseñas eliminando las contraseñas como superficie de ataque.
- **Mejor experiencia del usuario**: proporcione a los usuarios una manera cómoda de acceder a los datos desde cualquier lugar. y ofrezca un acceso móvil sencillo a aplicaciones y servicios como Outlook, OneDrive u Office.
- **Información sólida**: obtenga información sobre la actividad sin contraseña de los usuarios con un registro y una auditoría sólidos.
