

Contents

[Documentación sobre aspectos básicos](#)

[Información general](#)

[¿Qué es Azure Active Directory?](#)

[Comparación entre Azure AD y ADDS](#)

[Novedades de Azure Active Directory](#)

[Novedades de Microsoft 365 Government](#)

[Archivo de novedades de Azure AD](#)

[Guías de inicio rápido](#)

[Acceso al portal y creación de un inquilino](#)

[Visualización de los grupos con miembros asignados](#)

[Conceptos](#)

[Seguridad](#)

[Habilitar MFA](#)

[Valores predeterminados de seguridad](#)

[Bloquear la autenticación heredada](#)

[Puntuación segura de identidad](#)

[Protección de trabajos remotos](#)

[Evaluación continua de acceso](#)

[Grupos y usuarios](#)

[Grupos y administración de accesos](#)

[Licencias basadas en grupos](#)

[Permisos predeterminados de usuario](#)

[Architecture](#)

[Arquitectura de Azure AD](#)

[Guía de implementación](#)

[Implementación de 30, 90 y más](#)

[Planes de implementación de Azure Active Directory](#)

[Almacenamiento de datos](#)

[Almacenamiento de datos de identidad para Europa](#)

Almacenamiento de datos de identidad para Australia y Nueva Zelanda

Referencia de operaciones de Azure AD

Introducción

Administración de identidades y acceso

Administración de la autenticación

Gobernanza de identidades

Operaciones

Guías paso a paso

Organización

Registro en Azure AD como organización

Suscripción a Azure AD Premium

Adición de un dominio personalizado

Adición de personalización de compañía

Configuración de "¿Desea mantener la sesión iniciada?"

Asociación de una suscripción a Azure

Incorporación de la información de privacidad

Grupos

Creación de un grupo e incorporación de miembros

Incorporación o eliminación de miembros del grupo

Eliminación de un grupo y sus miembros

Incorporación o eliminación de un grupo desde otro grupo

Edición de la información del grupo

Incorporación o eliminación de propietarios del grupo

Administración del acceso a los recursos con grupos

Usuarios

Incorporación o eliminación de un nuevo usuario

Incorporación o modificación de la información del perfil de usuario

Restablecimiento de la contraseña del usuario

Asignación de roles a usuarios

Asignación o eliminación de licencias de los usuarios

Restaurar un usuario eliminado

Solución de problemas

Obtención de soporte técnico para Azure Active Directory

P+F de Azure Active Directory

¿Qué es Azure Active Directory?

22/07/2020 • 20 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) es un servicio de administración de identidades y acceso basado en la nube de Microsoft que ayuda a los empleados a iniciar sesión y acceder a recursos en:

- Recursos externos, como Microsoft Office 365, Azure Portal y miles de otras aplicaciones SaaS.
- Recursos internos, como las aplicaciones de la red corporativa y la intranet, junto con todas las aplicaciones en la nube desarrolladas por su propia organización. Para más información sobre la creación de un inquilino para su organización, consulte [Guía de inicio rápido: Creación de un inquilino en Azure Active Directory](#).

Para obtener información sobre la diferencia entre Azure AD y Active Directory Domain Services, consulte [Comparación de Active Directory y Azure Active Directory](#). Puede utilizar los diversos pósteres de la [Serie de Microsoft Cloud para arquitectos empresariales](#) para conocer mejor los servicios de identidad principales de Azure, Azure AD y Office 365.

¿Quién usa Azure AD?

Azure AD va dirigido a:

- **Administradores de TI.** Si es administrador de TI, puede usar Azure AD para controlar el acceso a sus aplicaciones y a los recursos de éstas en función de los requisitos de su empresa. Por ejemplo, puede usar Azure AD para requerir autenticación multifactor al acceder a recursos importantes de la organización. Además, puede usar Azure AD para automatizar el aprovisionamiento de usuarios entre la instancia existente de Windows Server AD y las aplicaciones en la nube, incluida Office 365. Por último, Azure AD proporciona eficaces herramientas que ayudan a proteger automáticamente las identidades y credenciales de los usuarios y a cumplir los requisitos de gobernanza de acceso. Para empezar, regístrate para obtener una [versión de evaluación gratuita durante 30 días de Azure Active Directory Premium](#).
- **Desarrolladores de aplicaciones.** Como desarrollador de aplicaciones, puede usar Azure AD como enfoque basado en estándares para agregar el inicio de sesión único (SSO) a cualquier aplicación, lo que le permite trabajar con las credenciales existentes de un usuario. Azure AD también proporciona varias API que pueden ayudarle a crear experiencias de aplicación personalizadas que usen los datos existentes de la organización. Para empezar, regístrate para obtener una [versión de evaluación gratuita durante 30 días de Azure Active Directory Premium](#). Para más información, también puede consultar [Azure Active Directory para desarrolladores](#).
- **Suscriptores de Microsoft 365, Office 365, Azure o Dynamics CRM Online.** Los suscriptores usan Azure AD. Cada inquilino de Microsoft 365, Office 365, Azure y Dynamics CRM Online es automáticamente un inquilino de Azure AD. Puede empezar de inmediato a administrar el acceso a las aplicaciones en la nube integradas.

¿Qué son las licencias de Azure AD?

Los servicios para la empresa de Microsoft Online, como Office 365 o Microsoft Azure, requieren Azure AD para iniciar sesión y ayudar con la protección de identidad. Por consiguiente, si se suscribe a cualquiera de los servicios de negocio de Microsoft Online, obtendrá automáticamente Azure AD con acceso a todas las características gratuitas.

Para mejorar la implementación de Azure AD, también puede agregar funcionalidades de pago mediante la

actualización a las licencias Azure Active Directory Premium P1 o Premium P2. Las licencias de pago de Azure AD se crean sobre el directorio gratuito existente y proporcionan autoservicio, supervisión mejorada, informes de seguridad y un acceso seguro a sus usuarios móviles.

NOTE

Para ver las opciones de precios de estas licencias, consulte [Precios de Azure Active Directory](#).

Azure Active Directory Premium P1 y Premium P2 no se admiten actualmente en China. Para más información acerca de los precios de Azure AD, póngase en contacto con el [foro de Azure Active Directory](#).

- **Azure Active Directory Free.** 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, Office 365 y muchas aplicaciones SaaS populares.
- **Azure Active Directory Premium 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 (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 Free y P1, la licencia P2 ofrece también [Azure Active Directory Identity Protection](#), que proporciona acceso condicional basado en riesgos a sus aplicaciones y datos críticos de la compañía, y [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.
- **Licencias de la característica de "Pago por uso".** También puede obtener licencias de características adicionales, como Azure Active Directory Business-to-Customer (B2C). B2C puede ayudarle a proporcionar soluciones de administración de acceso y de identidad para las aplicaciones orientadas al cliente. Para más información, consulte [Documentación de Azure Active Directory B2C](#).

Para más información acerca de cómo asociar una suscripción de Azure a Azure AD, consulte [Asociación o adición de una suscripción de Azure a Azure Active Directory](#) y para más información acerca de cómo asignar licencias a usuarios, consulte [Cómo asignar o quitar licencias de Azure Active Directory](#).

¿Qué características funcionan en Azure AD?

Después de elegir su licencia de Azure AD, obtendrá acceso a algunas de las características siguientes para su organización, o a todas ellas:

CATEGORY	DESCRIPCIÓN
Administración de aplicaciones	Administre las aplicaciones en la nube y locales mediante el proxy de aplicación, el inicio de sesión único, el portal Mis aplicaciones (también conocido como Panel de acceso) y aplicaciones de software como servicio (SaaS). Para más información, consulte Provisión de acceso remoto seguro a aplicaciones locales y Documentación sobre la administración de aplicaciones .

CATEGORÍA	DESCRIPCIÓN
Authentication	Administre el restablecimiento de contraseñas de autoservicio de Azure Active Directory, Multi-Factor Authentication, la lista personalizada de contraseñas prohibidas y el bloqueo inteligente. Para más información, consulte la documentación de Autenticación de Azure AD .
Azure Active Directory 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. Para más información, consulte Plataforma de identidad de Microsoft (Azure Active Directory para desarrolladores) .
Negocio a negocio (B2B)	Administre los usuarios invitados y los asociados externos sin perder el control sobre sus propios datos corporativos. Para más información, consulte Documentación de Azure Active Directory B2B .
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. Para más información, consulte Documentación de Azure Active Directory B2C .
Acceso condicional	Administre el acceso a sus aplicaciones en la nube. Para más información, consulte Documentación sobre el acceso condicional de Azure AD .
Administración de dispositivos	Administre la forma en que los dispositivos en la nube o locales acceden a los datos corporativos. Para más información, consulte la documentación de Azure AD Device Management .
Servicios de dominio	Combine máquinas virtuales de Azure en un dominio sin controladores de dominio. Para más información, consulte Documentación de Azure AD Domain Services .
Usuarios de empresa	Administre la asignación de licencias, el acceso a las aplicaciones y configure delegados mediante grupos y roles de administrador. Para más información, consulte Documentación sobre administración de usuarios de Azure Active Directory .
Identidad híbrida	Use Azure Active Directory 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). Para más información, consulte Documentación de identidad híbrida .
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. Para más información, consulte la documentación sobre la gobernanza de identidades en Azure AD y las revisiones de acceso de Azure AD .

CATEGORY	DESCRIPCIÓN
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. Para más información, consulte Azure AD Identity Protection .
Identidades administradas de recursos de Azure	Proporcione a los servicios de Azure una identidad administrada automáticamente en Azure AD que puede autenticar cualquier servicio de autenticación compatible con Azure AD, incluido Key Vault. Para más información, consulte ¿Qué es Managed Identities for Azure Resources?
Privileged Identity Management (PIM)	Administre, controle y supervise el acceso dentro de su organización. Esta característica incluye el acceso a los recursos de Azure AD y Azure, así como a otros servicios de Microsoft Online Services, como Office 365 o Intune. Para obtener más información, vea Azure AD Privileged Identity Management .
Informes y supervisión	Obtenga información acerca de los patrones de seguridad y de uso del entorno. Para más información, consulte Informes y supervisión de Azure Active Directory .

Terminología

Para conocer mejor Azure AD y su documentación, es aconsejable revisar los términos siguientes.

TÉRMINO O CONCEPTO	DESCRIPCIÓN
Identidad	Algo que se puede autenticar. Una identidad puede ser un usuario con un nombre de usuario y una contraseña. Entre las identidades también se incluyen aplicaciones u otros servidores que podrían requerir autenticación a través de claves secretas o certificados.
Cuenta	Una identidad que tiene datos asociados a ella. No puede tener una cuenta sin una identidad.
Cuenta de Azure AD	Una identidad que se crean mediante Azure AD u otro servicio en la nube de Microsoft, como Office 365. Las identidades se almacenan en Azure AD y pueden acceder a ellas las suscripciones de servicio en la nube de su organización. Esta cuenta se denomina a veces también cuenta profesional o educativa.
Administrador de cuenta	Este rol de administrador de suscripción clásica conceptualmente es el propietario de facturación de una suscripción. Este rol tiene acceso al centro de cuentas de Azure y permite administrar todas las suscripciones de una cuenta. Para más información, consulte Roles de administrador de suscripciones clásico de RBAC de Azure y de administrador de Azure AD .

TÉRMINO O CONCEPTO	DESCRIPCIÓN
Administrador de servicios	Este rol de administrador de suscripciones clásico permite administrar todos los recursos de Azure, incluido el acceso. Tiene el acceso equivalente a un usuario al que se le ha asignado la función de propietario en el ámbito de la suscripción. Para más información, consulte Roles de administrador de suscripciones clásico, de RBAC de Azure y de administrador de Azure AD .
Propietario	Este rol ayuda a administrar todos los recursos de Azure, incluido el acceso. Este rol se basa en un sistema de autorización más reciente denominado control de acceso basado en rol (RBAC) que proporciona una administración detallada del acceso a recursos de Azure. Para más información, consulte Roles de administrador de suscripciones clásico, de RBAC de Azure y de administrador de Azure AD .
Administrador global de Azure AD	Este rol de administrador se asigna automáticamente a quien haya creado el inquilino de Azure AD. Los administradores globales pueden realizar todas las funciones administrativas de Azure AD y los servicios que se federan con Azure AD, como Exchange Online, SharePoint Online y Skype Empresarial Online. Puede tener varios administradores globales, pero estos administradores son los únicos que pueden asignar roles de administrador (lo que incluye la asignación de otros administradores globales) a los usuarios. Tenga en cuenta que este rol de administrador se denomina Administrador global en Azure Portal, pero Administrador de empresa en la API de Microsoft Graph y Azure AD PowerShell. Para obtener más información acerca de los distintos roles de administrador, consulte Permisos de roles de administrador en Azure Active Directory .
Suscripción de Azure	Se usa para pagar los servicios en la nube de Azure. Puede tener muchas suscripciones y están vinculadas a una tarjeta de crédito.
Inquilino de Azure	Es una instancia dedicada y de confianza de Azure AD que se crea automáticamente cuando una organización se suscribe a un servicio en la nube de Microsoft, como Microsoft Azure, Microsoft Intune u Office 365. Un inquilino de Azure representa una organización individual.
Un solo inquilino	Los inquilinos de Azure que acceden a otros servicios en un entorno dedicado se consideran inquilino individuales.
Multiinquilino	Los inquilinos de Azure que tienen acceso a otros servicios en un entorno compartido, en varias organizaciones, se consideran varios inquilinos.
Directorio de Azure AD	Todos los inquilinos de Azure tienen un directorio de Azure AD dedicado y de confianza. El directorio de Azure AD incluye los usuarios, grupos y aplicaciones del inquilino y se usa para realizar funciones de administración de acceso y de identidad en los recursos del inquilino.

TÉRMINO O CONCEPTO	DESCRIPCIÓN
Dominio personalizado	Cada directorio nuevo de Azure AD incluye un nombre de dominio inicial, nombre_de_dominio.onmicrosoft.com. Además de dicho nombre inicial, también puede agregar nombres de dominio de la organización, que incluyen los nombres que utiliza para hacer negocios y los que utilizan los usuarios para acceder a los recursos de su organización, a la lista. La adición de nombres de dominio personalizados le ayuda a crear nombres de usuario que resultan familiares a los usuarios, como alain@contoso.com.
Cuenta Microsoft (también denominada MSA)	Las cuentas personales que proporcionan acceso a los productos y servicios en la nube de Microsoft orientados al consumidor, como Outlook, OneDrive, Xbox LIVE u Office 365. Su cuenta Microsoft se crean y almacenan en el sistema de cuentas de identidad de consumidor de Microsoft que ejecuta Microsoft.

Pasos siguientes

- [Suscripción a Azure Active Directory Premium](#)
- [Asociación o adición de una suscripción de Azure a Azure Active Directory](#)
- [Lista de comprobación de la característica de licencia de Azure Active Directory Premium P2](#)

Comparación de Azure Directory y Azure Active Directory

22/07/2020 • 11 minutes to read • [Edit Online](#)

Azure Active Directory es la siguiente evolución de las soluciones de administración de identidades y de acceso para la nube. Microsoft presentó Active Directory Domain Services en Windows 2000 para ofrecer a las organizaciones la capacidad de administrar varios componentes y sistemas de infraestructura locales mediante una única identidad por usuario.

Azure AD lleva este enfoque al siguiente nivel, ya que proporciona a las organizaciones una solución de identidad como servicio (IDaaS) para todas sus aplicaciones en la nube y en el entorno local.

La mayoría de los administradores de TI están familiarizados con los conceptos de Active Directory Domain Services. En la tabla siguiente se describen las diferencias y similitudes entre los conceptos de Active Directory y Azure Active Directory.

CONCEPTO	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Usuarios		
Aprovisionamiento: usuarios	Las organizaciones crean usuarios internos manualmente o utilizan un sistema de aprovisionamiento interno o automatizado, como Microsoft Identity Manager, para integrarse en un sistema de recursos humanos.	Las organizaciones de AD existentes usan Azure AD Connect para sincronizar identidades en la nube. Azure AD agrega compatibilidad para crear usuarios de forma automática a partir de sistemas de recursos humanos en la nube . Azure AD puede aprovisionar identidades de aplicaciones SaaS con SCIM habilitado para proporcionar automáticamente a las aplicaciones los detalles necesarios que permitan acceder a los usuarios.
Aprovisionamiento: identidades externas	Las organizaciones crean usuarios externos manualmente como usuarios normales en un bosque de AD externo dedicado, lo que da lugar a una sobrecarga de administración para administrar el ciclo de vida de las identidades externas (usuarios invitados).	Azure AD proporciona una clase especial de identidad que admite identidades externas. Azure AD B2B administrará el vínculo con la identidad de usuarios externos para asegurarse de que sean válidos.

CONCEPTO	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Administración de derechos y grupos	Los administradores nombran a los usuarios como miembros de grupos. Los propietarios de los recursos y las aplicaciones proporcionan a los grupos acceso a aplicaciones o recursos.	Los grupos también están disponibles en Azure AD y los administradores pueden igualmente utilizar grupos para conceder permisos a recursos. En Azure AD, los administradores pueden asignar la pertenencia a grupos de modo manual o usar una consulta para incluir a los usuarios de forma dinámica en un grupo. Los administradores pueden utilizar Administración de derechos en Azure AD para proporcionar a los usuarios acceso a una colección de aplicaciones y recursos mediante flujos de trabajo y, si es necesario, criterios con duración definida.
Administración de administradores	Las organizaciones usarán una combinación de dominios, unidades organizativas y grupos en AD para delegar derechos administrativos con el fin de administrar el directorio y los recursos que controlan.	Azure AD proporciona roles integrados con su sistema de control de acceso basado en rol (RBAC), con compatibilidad limitada para crear roles personalizados a fin de delegar el acceso con privilegios en el sistema de identidades, las aplicaciones y los recursos que controla. La administración de roles se puede mejorar con Privileged Identity Management (PIM) para proporcionar acceso Just-in-Time, con tiempo restringido o basado en flujo de trabajo a roles con privilegios.
Administración de credenciales	Las credenciales de Active Directory se basan en contraseñas, autenticación de certificados y autenticación de tarjetas inteligentes. Las contraseñas se administran mediante directivas de contraseñas que se basan en la longitud, la expiración y la complejidad de las contraseñas.	Azure AD usa la protección con contraseña inteligente para la nube y el entorno local. La protección incluye el bloqueo inteligente, además del bloqueo de frases y sustituciones de contraseñas comunes y personalizadas. Azure AD aumenta significativamente la seguridad mediante autenticación multifactor y las tecnologías sin contraseñas , como FIDO2. Azure AD reduce los costos de soporte técnico al proporcionar a los usuarios un sistema de autoservicio de restablecimiento de contraseña .
Aplicaciones		
Aplicaciones de infraestructura	Active Directory constituye la base para numerosos componentes locales de infraestructura, por ejemplo, acceso DNS, DHCP, IPSec, WiFi, NPS y VPN.	En un nuevo mundo de la nube, Azure AD es el nuevo plano de control para acceder a las aplicaciones en lugar de basarse en controles de red. Cuando los usuarios se autentiquen, el acceso condicional (CA) controlará qué usuarios tendrán acceso a las aplicaciones en las condiciones requeridas.

CONCEPTO	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Aplicaciones tradicionales y heredadas	La mayoría de las aplicaciones locales usan LDAP, la autenticación integrada de Windows (NTLM y Kerberos) o la autenticación basada en encabezados para controlar el acceso a los usuarios.	Azure AD puede proporcionar acceso a estos tipos de aplicaciones locales con los agentes de Azure AD Application Proxy que se ejecutan de forma local. Con este método, Azure AD puede autenticar los usuarios de Active Directory de forma local mediante Kerberos mientras migra o debe coexistir con aplicaciones heredadas.
Aplicaciones SaaS	Active Directory no es compatible de forma nativa con aplicaciones SaaS y requiere un sistema de federación, como AD FS.	Las aplicaciones SaaS que admiten la autenticación de OAuth2, SAML y WS-* se pueden integrar para usar Azure AD para la autenticación.
Aplicaciones de línea de negocio (LOB) con autenticación moderna	Las organizaciones pueden usar AD FS con Active Directory para admitir aplicaciones LOB que requieran autenticación moderna.	Las aplicaciones LOB que requieran autenticación moderna se pueden configurar para utilizar Azure AD para la autenticación.
Servicios de nivel medio/demonio	Los servicios que se ejecutan en entornos locales suelen usar cuentas de servicio de AD o cuentas de servicio administradas de grupo (gMSA) para ejecutarse. Estas aplicaciones heredarán los permisos de la cuenta de servicio.	Azure AD proporciona identidades administradas para ejecutar otras cargas de trabajo en la nube. El ciclo de vida de estas identidades, que se administra mediante Azure AD y está asociado al proveedor de recursos, no se puede usar con otros fines para obtener acceso de puerta trasera.
Dispositivos		
Móvil	Active Directory no es compatible de forma nativa con dispositivos móviles sin soluciones de terceros.	La solución de administración de dispositivos móviles de Microsoft, Microsoft Intune, está integrado en Azure AD. Microsoft Intune proporciona información sobre el estado del dispositivo al sistema de identidades que se va a evaluar durante la autenticación.
Escritorios de Windows	Active Directory proporciona la capacidad de unir a un dominio dispositivos Windows para administrarlos mediante directiva de grupo, System Center Configuration Manager u otras soluciones de terceros.	Los dispositivos Windows pueden estar unidos a Azure AD . El acceso condicional puede comprobar si un dispositivo está unido a Azure AD como parte del proceso de autenticación. Los dispositivos Windows también se pueden administrar con Microsoft Intune . En este caso, el acceso condicional tendrá en cuenta si un dispositivo es compatible (por ejemplo, revisiones de seguridad y firmas de virus actualizadas) antes de permitir el acceso a las aplicaciones.

CONCEPTO	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Servidores Windows	Active Directory proporciona unas funcionalidades de administración seguras para servidores Windows locales mediante directivas de grupo u otras soluciones de administración.	Las máquinas virtuales de Windows Servers en Azure se pueden administrar con Azure AD Domain Services . Se pueden utilizar identidades administradas cuando las máquinas virtuales necesitan tener acceso al directorio o a los recursos del sistema de identidades.
Cargas de trabajo Linux/Unix	Active Directory no es compatible de forma nativa con aplicaciones que no son de Windows sin soluciones de terceros, aunque se pueden configurar máquinas Linux para autenticarse con Active Directory como un dominio Kerberos.	Las máquinas virtuales Linux/Unix pueden usar identidades administradas para acceder al sistema de identidades o a los recursos. Algunas organizaciones migran estas cargas de trabajo a tecnologías de contenedor en la nube, que también pueden utilizar identidades administradas.

Pasos siguientes

- [¿Qué es Azure Active Directory?](#)
- [Comparación de Active Directory Domain Services autoadministrado, Azure Active Directory y Azure Active Directory Domain Services administrado](#)
- [Preguntas más frecuentes sobre Azure Active Directory](#)
- [¿Cuáles son las novedades de Azure Active Directory?](#)

¿Cuáles son las novedades de Azure Active Directory?

22/07/2020 • 106 minutes to read • [Edit Online](#)

Reciba notificaciones para volver a visitar esta página y obtener actualizaciones; para ello, copie y pegue la dirección URL

<https://docs.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us>
en el  lector de fuentes.

En Azure AD se realizan mejoras de forma continua. Para mantenerse al día de los avances más recientes, este artículo proporciona información acerca de los elementos siguientes:

- Versiones más recientes
- Problemas conocidos
- Corrección de errores
- Funciones obsoletas
- Planes de cambios

Esta página se actualiza mensualmente, por lo que se recomienda visitarla con frecuencia. Si busca elementos que tengan más de 6 meses, puede encontrarlos en el [Archivo de novedades de Azure Active Directory](#).

Junio de 2020

Condición de riesgo de usuario de la directiva de acceso condicional

Tipo: Plan de cambio

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

La compatibilidad con el riesgo de usuario en la directiva de acceso condicional de Azure AD permite crear varias directivas basadas en el riesgo de usuario. Pueden requerirse diferentes niveles de riesgo de usuario mínimo para diferentes usuarios y aplicaciones. En función del riesgo de usuario, puede crear directivas para bloquear el acceso, requerir la autenticación multifactor, proteger el cambio de contraseña o redirigir a Microsoft Cloud App Security para aplicar la directiva de sesión, como la auditoría adicional.

La condición de riesgo de usuario requiere Azure AD Premium P2 porque usa Azure Identity Protection, que es una oferta P2. Para más información sobre el acceso condicional, vea la [documentación sobre el acceso condicional de Azure AD](#).

SSO de SAML admite ahora aplicaciones que requieren establecer SPNameQualifier cuando se solicite

Tipo: Corregido

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Algunas aplicaciones de SAML requieren que se devuelva SPNameQualifier en el sujeto de la aserción cuando se solicita. Ahora Azure AD responde correctamente cuando se solicita un SPNameQualifier en la directiva de NameID de la solicitud. Esto también funciona para el inicio de sesión iniciado por el SP y se seguirá el inicio de sesión iniciado por IdP. Para más información sobre el protocolo de SAML en Azure Active Directory, vea [Protocolo SAML de inicio de sesión único](#).

La colaboración B2B de Azure AD permite invitar a los usuarios de MSA y Google en inquilinos de Azure Government

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Los inquilinos de Azure Government que usan las características de colaboración B2B ahora pueden invitar a los usuarios que tienen una cuenta de Microsoft o Google. Para averiguar si su inquilino puede usar estas funcionalidades, siga las instrucciones que se indican en [¿Cómo puedo saber si la colaboración B2B está disponible en mi inquilino de Azure US Government?](#)

El objeto de usuario de MS Graph v1 ahora incluye las propiedades externalUserState y externalUserStateChangedDateTime

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Las propiedades externalUserState y externalUserStateChangedDateTime se pueden usar para buscar invitados B2B que aún no han aceptado sus invitaciones, así como para crear automatización, como la eliminación de usuarios que no han aceptado sus invitaciones después de un número determinado de días. Estas propiedades están ahora disponibles en MS Graph v1. Para obtener instrucciones sobre el uso de estas propiedades, consulte [Tipo de recurso del usuario](#).

La administración de sesiones de autenticación en el acceso condicional de Azure AD ya está disponible con carácter general

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

Las funcionalidades de administración de sesiones de autenticación permiten configurar la frecuencia con que los usuarios necesitan proporcionar credenciales de inicio de sesión y si necesitan proporcionar credenciales después de cerrar y volver a abrir los exploradores para ofrecer más seguridad y flexibilidad en el entorno.

Además, la administración de sesiones de autenticación se aplicaba solo a la autenticación del primer factor en los dispositivos unidos a Azure AD, unidos a Azure AD híbrido y registrados en Azure AD. Ahora la administración de sesiones de autenticación también se aplicará a MFA. Para más información, vea [Configuración de la administración de las sesiones de autenticación con el acceso condicional](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD, junio de 2020

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En junio de 2020, hemos agregado 29 nuevas aplicaciones a la galería de aplicaciones con compatibilidad de federación:

[Shopify Plus](#), [Ekarda](#), [MailGates](#), [BullseyeTDP](#), [Raketa](#), [Segment](#), [Ai Auditor](#), [Pobuca Connect](#), [Proto.io](#), [Gatekeeper](#), [Hub Planner](#), [Ansira-Partner Go-to-Market Toolbox](#), [IBM Digital Business Automation on Cloud](#), [Kisi Physical Security](#), [ViewpointOne](#), [IntelligenceBank](#), [pymetrics](#), [Zero](#), [InStation](#), [edX for Business SAML 2.0 Integration](#), [MOOC Office 365](#), [SmartKargo](#), [PKIsigning platform](#), [SitelIntel](#), [Field iD](#), [Curricula SAML](#), [Perforce Helix Core - Helix Authentication Service](#), [MyCompliance Cloud](#) y [Smallstep SSH](#)

La documentación de todas las aplicaciones está disponible aquí: <https://aka.ms/AppsTutorial> Para mostrar su aplicación en la galería de aplicaciones Azure AD, lea los detalles aquí: <https://aka.ms/AzureADAppRequest>.

Los conectores de API para el registro de autoservicio de identidades externas ya está disponible en versión preliminar pública

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Los conectores de API para identidades externas permiten utilizar las API web para integrar el registro de autoservicio con sistemas en la nube externos. Esto significa que ahora puede invocar las API web como pasos específicos en un flujo de registro para desencadenar flujos de trabajo personalizados basados en la nube. Por ejemplo, puede usar conectores de API para:

- Integrarse con un flujo de trabajo de aprobación personalizado.
- Realizar correcciones de identidad
- Validar los datos de entrada del usuario
- Sobrescribir atributos de usuario
- Ejecutar una lógica de negocios personalizada

Para más información sobre todas las experiencias posibles con los conectores de API, vea [Uso de conectores de API para personalizar y extender el registro de autoservicio](#) o [Personalización del registro de autoservicio de las identidades externas con las integraciones de API web](#).

Aprovisionamiento a petición e integración de usuarios en las aplicaciones en cuestión de segundos

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

El servicio de aprovisionamiento de Azure AD actualmente funciona de forma cíclica. El servicio se ejecuta cada 40 minutos. La [funcionalidad de aprovisionamiento a petición](#) permite elegir un usuario y aprovisionarlo en segundos. Esta funcionalidad permite solucionar problemas de aprovisionamiento rápidamente, sin tener que reiniciar para forzar el inicio del ciclo de aprovisionamiento.

Nuevo permiso para usar la administración de derechos de Azure AD en Graph

Tipo: Nueva característica

Categoría del servicio: Otros

Funcionalidad del producto: Administración de derechos

Un nuevo permiso delegado EntitlementManagement.Read.All ahora está disponible para su uso con la API de administración de derechos en la versión beta de Microsoft Graph. Para obtener más información sobre las API disponibles, vea [Trabajar con la API de administración de derechos de Azure AD](#).

API de Identity Protection disponibles en la versión 1.0

Tipo: Nueva característica

Categoría del servicio: Protección de identidad

Funcionalidad del producto: Seguridad y protección de la identidad

Las API riskyUsers y riskDetections de Microsoft Graph ahora están disponibles con carácter general. Ahora que están disponibles en el punto de conexión v 1.0, lo invitamos a utilizarlos en producción. Para más información, vea la [documentación de Microsoft Graph](#).

Las etiquetas de confidencialidad para aplicar directivas a grupos de Microsoft 365 ya están disponibles con carácter general

Tipo: Nueva característica

Categoría del servicio: Administración de grupos

Funcionalidad del producto: Colaboración

Ahora puede crear etiquetas de confidencialidad y usar la configuración de la etiqueta para aplicar directivas a grupos de Microsoft 365, incluida la directiva de privacidad (pública o privada) y la directiva de acceso de usuarios externos. Puede crear una etiqueta con la directiva de privacidad para que sea privada y con la directiva de acceso de usuarios externos para no permitir que se agreguen usuarios invitados. Cuando un usuario aplica esta etiqueta a un grupo, este será privado y no se permitirá agregar usuarios invitados al grupo.

Las etiquetas de confidencialidad son importantes para proteger los datos críticos para la empresa y permiten administrar grupos a escala, de manera compatible y segura. Para obtener orientación sobre el uso de las etiquetas de confidencialidad, vea [Asignación de etiquetas de confidencialidad a grupos de Office 365 en Azure Active Directory \(versión preliminar\)](#).

Actualizaciones de compatibilidad con Microsoft Identity Manager para clientes de Azure AD Premium

Tipo: Característica modificada

Categoría del servicio: Microsoft Identity Manager

Funcionalidad del producto: Administración del ciclo de vida de la identidad

El Soporte técnico de Azure ya está disponible para los componentes de integración de Azure AD de Microsoft Identity Manager 2016, hasta el final del soporte extendido para Microsoft Identity Manager 2016. Para más información, vea [Actualización de soporte técnico para clientes de Azure AD Premium que usan Microsoft Identity Manager](#).

Aumento del uso de condiciones de pertenencia a grupos en la configuración de notificaciones de SSO

Tipo: Característica modificada

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Anteriormente, el número de grupos que podía usar al cambiar condicionalmente las notificaciones basadas en la pertenencia a grupos dentro de cualquier configuración de aplicación única estaba limitado a 10. El uso de las condiciones de pertenencia a grupos en la configuración de notificaciones de SSO ahora se ha aumentado a un máximo de 50 grupos. Para más información sobre cómo configurar las notificaciones, vea [Configuración de notificaciones de SSO en aplicaciones empresariales](#).

Habilitar el formato básico en el componente de texto de la página de inicio de sesión para la personalización de marca de empresas

Tipo: Característica modificada

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

La funcionalidad de personalización de marca de la empresa en la experiencia de inicio de sesión de Azure AD/Microsoft 365 se ha actualizado para que el cliente pueda agregar hipervínculos y formatos sencillos, como negrita, subrayado y cursiva. Para obtener orientación sobre el uso de esta funcionalidad, vea [Incorporación de la personalización de marca en la página de inicio de sesión de Azure Active Directory de la organización](#).

Mejoras en el rendimiento de aprovisionamiento

Tipo: Característica modificada

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

El servicio de aprovisionamiento se ha actualizado para reducir el tiempo que tarda un [ciclo incremental](#) en completarse. Esto significa que los usuarios y grupos se aprovisionarán en sus aplicaciones más rápido que antes.

Todos los nuevos trabajos de aprovisionamiento creados después del 10/6/2020 se beneficiarán automáticamente de las mejoras de rendimiento. Las aplicaciones configuradas para el aprovisionamiento antes del 10/6/2020 deberán reiniciarse una vez después del 10/6/2020 para beneficiarse de las mejoras de rendimiento.

Anuncio de desuso de la paridad de ADAL y MS Graph

Tipo: Obsoleto

Categoría del servicio: N/D

Funcionalidad del producto: Administración del ciclo de vida de dispositivos

Ahora que las bibliotecas de autenticación de Microsoft (MSAL) están disponibles, ya no se agregarán nuevas características a las bibliotecas de autenticación de Azure Active Directory (ADAL) y las revisiones de seguridad finalizarán el 30 de junio de 2022. Para más información sobre cómo migrar a MSAL, vea [Migración de aplicaciones a la Biblioteca de autenticación de Microsoft \(MSAL\)](#).

Además, hemos finalizado el trabajo para que toda la funcionalidad de Azure AD Graph esté disponible mediante MS Graph. Por lo tanto, las API de Azure AD solo recibirán correcciones de errores y de seguridad hasta el 30 de junio de 2022. Para más información, vea [Actualización de las aplicaciones para usar la Biblioteca de autenticación de Microsoft y Microsoft Graph API](#).

Mayo de 2020

Retirada de propiedades en las API signIns, riskyUsers y riskDetections

Tipo: Plan de cambio

Categoría del servicio: Protección de identidad

Funcionalidad del producto: Seguridad y protección de la identidad

Actualmente, los tipos enumerados se usan para representar la propiedad `riskType` en `riskDetections` API y `riskyUserHistoryItem` (en versión preliminar). Los tipos enumerados también se usan para la propiedad `riskEventTypes` de `signIns` API. En el futuro, se representarán estas propiedades como cadenas.

Los clientes deben realizar la transición a la propiedad `riskEventType` de la versión beta de `riskDetections` y `riskyUserHistoryItem` API, así como a la propiedad `riskEventTypes_v2` de la versión beta de `signIns` API antes del 9 de septiembre de 2020. En esa fecha, se retirarán las propiedades actuales `riskType` y `riskEventTypes`. Para más información, vea [Cambios en las propiedades de eventos de riesgo y en las API de Identity Protection en Microsoft Graph](#).

Desuso de la propiedad riskEventTypes en signIns v1.0 API en Microsoft Graph

Tipo: Plan de cambio

Categoría del servicio: Notificación

Funcionalidad del producto: Seguridad y protección de la identidad

Los tipos enumerados cambiarán a tipos de cadena al representar las propiedades de evento de riesgo en Microsoft Graph en septiembre de 2020. Además de afectar a las API en versión preliminar, este cambio también afectará a `signIns` API en producción.

Hemos introducido una nueva propiedad `riskEventsTypes_v2` (cadena) en `signIns` v1.0 API. Se retirará la propiedad `riskEventTypes` (enumeración) actual el 11 de junio de 2022 de acuerdo con la directiva de desuso de Microsoft Graph. Los clientes deben realizar la transición a la propiedad `riskEventTypes_v2` de v1.0 `signIns` API antes del 11 de junio de 2022. Para más información, vea [Desuso de la propiedad riskEventTypes en signIns v1.0 API en Microsoft Graph](#).

Próximos cambios en las notificaciones por correo electrónico de MFA

Tipo: Plan de cambio

Categoría del servicio: MFA

Funcionalidad del producto: Seguridad y protección de la identidad

Vamos a realizar los siguientes cambios en las notificaciones por correo electrónico de MFA para MFA:

Las notificaciones por correo electrónico se enviarán desde las siguientes direcciones: azure-noreply@microsoft.com y msonlineservicesteam@microsoftonline.com. Estamos actualizando el contenido de los correos electrónicos de alerta sobre fraudes a fin de explicar mejor los pasos necesarios para desbloquear los usos.

Nuevo registro de autoservicio para usuarios de dominios federados que no pueden acceder a Microsoft Teams porque no están sincronizados con Azure Active Directory.

Tipo: Plan de cambio

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Actualmente, los usuarios que están en dominios federados en Azure AD, pero que no están sincronizados en el inquilino, no pueden acceder a Teams. A partir de finales de junio, esta nueva funcionalidad les permitirá hacerlo gracias a la extensión de la característica de registro con verificación por correo electrónico. Esto permitirá a los usuarios iniciar sesión en un proveedor de identidades (IdP) federado. En el caso de los usuarios que aún no tengan un objeto de usuario en Azure ID, el objeto se creará automáticamente y se autenticará para Teams. El objeto de usuario se marcará como "registro de autoservicio". Se trata de una extensión de la característica existente para que los usuarios de los dominios administrados puedan registrarse mediante la verificación por correo electrónico y se pueda llevar un control utilizando la misma marca. La implementación de este cambio se llevará a cabo durante los dos próximos meses. Vea las actualizaciones de la documentación [aquí](#).

Próxima corrección: El documento de detección de OIDC para la nube de Azure Government se está actualizando para que haga referencia a los puntos de conexión de Graph correctos.

Tipo: Plan de cambio

Categoría del servicio: Nubes soberanas

Funcionalidad del producto: Autenticación de usuarios

A partir de junio, el documento de detección de OIDC [Plataforma de identidad de Microsoft y protocolo OpenID Connect](#) sobre el punto de conexión de la [nube de Azure Government](#) (login.microsoftonline.us), comenzará a devolver el punto de conexión de [Graph de la nube nacional](#) correcto (<https://graph.microsoft.us> o <https://dod-graph.microsoft.us>), según el inquilino proporcionado). Actualmente, proporciona el campo "msgraph_host" del punto de conexión de Graph incorrecto (graph.microsoft.com).

Esta corrección de errores se implementará gradualmente durante 2 meses aproximadamente.

Los usuarios de Azure Government ya no podrán iniciar sesión en login.microsoftonline.com

Tipo: Plan de cambio

Categoría del servicio: Nubes soberanas

Funcionalidad del producto: Autenticación de usuarios

El 1 de junio de 2018, la autoridad oficial de Azure Active Directory (AAD) para Azure Government cambió de <https://login-us.microsoftonline.com> a <https://login.microsoftonline.us>. Si posee una aplicación en un inquilino de Azure Government, tiene que actualizarla para que los usuarios inicien sesión en el punto de conexión .us.

El 5 de mayo, Azure AD comenzó a aplicar el cambio relativo al punto de conexión, por lo que los usuarios de Azure Government no podrán iniciar sesión en aplicaciones hospedadas en inquilinos de Azure Government mediante el punto de conexión público (microsoftonline.com). Las aplicaciones afectadas comenzarán a obtener el error AADSTS900439 - USGClientNotSupportedOnPublicEndpoint.

Este cambio se implementará de forma gradual y se espera que se haya completado para todas las aplicaciones en junio de 2020. Para más información, consulte la [entrada de blog sobre Azure Government](#).

La solicitud de cierre de sesión único de SAML ahora envía el valor de NameID con el formato correcto

Tipo: Corregido

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Cuando un usuario hace clic para cerrar sesión (por ejemplo, en el portal Mis aplicaciones), Azure AD envía un mensaje de cierre de sesión único de SAML a cada aplicación que esté activa en la sesión de usuario y tenga configurada una dirección URL de cierre de sesión. Estos mensajes contienen un valor de NameID con formato persistente.

Si el token de inicio de sesión de SAML original utilizaba un formato diferente para NameID (por ejemplo, correo electrónico o UPN), la aplicación SAML no podía correlacionar el valor de NameID en el mensaje de cierre de sesión para una sesión existente, dado que los valores de NameID utilizados en ambos mensajes eran diferentes. Esto hacía que la aplicación SAML descartara el mensaje de cierre de sesión y que la sesión del usuario se mantuviera activa. Esta corrección hace que el mensaje de cierre de sesión sea coherente con el valor de NameID configurado para la aplicación.

El rol de administrador de identidades híbridas ahora está disponible con aprovisionamiento en la nube

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento en la nube de Azure AD

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Los administradores de TI pueden empezar a usar el nuevo rol de administrador de identidades híbridas como el rol con privilegios mínimos para configurar el aprovisionamiento en la nube de Azure ADConnect. Con este nuevo rol, ya no tiene que usar el rol de administrador global para instalar y configurar el aprovisionamiento en la nube.

[Más información.](#)

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD, mayo de 2020

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En mayo de 2020, hemos agregado 36 nuevas aplicaciones a la galería de aplicaciones con compatibilidad de federación:

[Moula](#), [Surveypal](#), [Kbot365](#), [TackleBox](#), [Powell Teams](#), [Talentsoft Assistant](#), [ASC Recording Insights](#), [GO1](#), [B-Engaged](#), [Competella Contact Center Workgroup](#), [Asite](#), [ImageSoft Identity](#), [My IBISWorld](#), [insuite](#), [Change Process Management](#), [Cyara CX Assurance Platform](#), [Smart Global Governance](#), [Prezi](#), [Mapbox](#), [Datava Enterprise Service Platform](#), [Whimsical](#), [Trelica](#), [EasySSO for Confluence](#), [EasySSO for BitBucket](#), [EasySSO for Bamboo](#), [Torii](#), [Axiad Cloud](#), [Humanage](#), [ColorTokens ZTNA](#), [CCH Tagetik](#), [ShareVault](#), [Vyond](#), [TextExpander](#), [Anyone Home CRM](#), [askSpoke](#), [ice Contact Center](#)

La documentación de todas las aplicaciones está disponible aquí: <https://aka.ms/AppsTutorial>

Para mostrar su aplicación en la galería de aplicaciones Azure AD, lea los detalles aquí:

<https://aka.ms/AzureADAppRequest>

El modo Solo informe para el Acceso condicional ya está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

El [modo Solo informe para el Acceso condicional de Azure AD](#) le permite evaluar el resultado de una directiva sin necesidad de aplicar controles de acceso. Puede probar las directivas del modo Solo informe en toda la

organización y comprender su impacto antes de habilitarlas, lo que hará que la implementación sea más segura y fácil. En los últimos meses, hemos observado una importante adopción del modo de solo informe, y más de 26 millones de usuarios están incluidos en el ámbito de la directiva de solo informe. Con el anuncio de hoy, se crearán nuevas directivas de acceso condicional de Azure AD en el modo de solo informe de forma predeterminada. Esto significa que puede supervisar el impacto de las directivas desde el momento en el que se crean. Además, aquellos usuarios que utilizan Microsoft Graph API, también pueden [administrar directivas de solo informe mediante programación](#).

Registro de autoservicio para usuarios invitados

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Mediante las identidades externas en Azure AD, puede facilitar a personas ajenas a la organización el acceso a sus aplicaciones y recursos, además de permitirles iniciar sesión con la identidad que prefieran. Al compartir una aplicación con usuarios externos, es posible que no siempre sepa de antemano quién necesitará tener acceso a la aplicación. Con el [registro de autoservicio](#), puede facilitar a los usuarios invitados el registro y el acceso a una cuenta de invitado para sus aplicaciones de línea de negocio (LOB). El flujo de registro se puede crear y personalizar para admitir Azure AD e identidades sociales. También puede recopilar información adicional sobre el usuario durante el registro.

El libro Conditional Access Insights and Reporting (Información detallada e informes del acceso condicional) está disponible con carácter general

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

El [libro Conditional Access Insights and Reporting \(Información detallada e informes del acceso condicional\)](#) ofrece a los administradores un resumen del acceso condicional de Azure AD en su inquilino. Al poder seleccionar una directiva individual, los administradores pueden comprender mejor lo que hace cada directiva y supervisar los cambios en tiempo real. El libro transmite los datos almacenados en Azure Monitor, que puede configurar en unos minutos [según estas instrucciones](#). Para encontrar el panel con más facilidad, lo hemos trasladado a la nueva pestaña Conclusiones e informes del menú Acceso condicional de Azure AD.

La hoja Detalles de la directiva de Acceso condicional está en versión preliminar pública.

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

La nueva [hoja Detalles de la directiva](#) muestra las asignaciones, condiciones y controles que se han llevado a cabo durante la evaluación de la directiva de acceso condicional. Para acceder a la hoja, seleccione una fila en las pestañas Acceso condicional o Solo informe, en los detalles de inicio de sesión.

Nuevas funciones de consulta para objetos de directorio en Microsoft Graph ahora disponibles en versión preliminar pública

Tipo: Nueva característica

Categoría del servicio: MS Graph **Funcionalidad del producto:** Experiencia para el desarrollador

Se están incorporando nuevas funciones a las API de objetos de directorio de Microsoft Graph, que permiten realizar operaciones de recuento, búsqueda, filtrado y ordenación. Esto permitirá a los desarrolladores consultar rápidamente nuestros objetos de directorio sin necesidad de buscar alternativas como la ordenación y el filtrado en memoria. Puede obtener más información en esta [entrada de blog](#).

Actualmente nos encontramos en la fase de versión preliminar pública, a la espera de comentarios. Envíe sus comentarios por medio de esta [breve encuesta](#).

Configuración del inicio de sesión único basado en SAML mediante Microsoft Graph API (beta)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Ya se ofrece compatibilidad para crear y configurar una aplicación desde la galería de Azure AD mediante MS Graph API en la versión beta. Si necesita configurar el inicio de sesión único basado en SAML para varias instancias de una aplicación, ahorre tiempo y utilice Microsoft Graph API para [automatizar la configuración del inicio de sesión único basado en SAML](#).

Nuevos conectores de aprovisionamiento disponibles en la galería de aplicaciones de Azure AD, mayo de 2020

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Integración de terceros

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [8x8](#)
- [Juno Journey](#)
- [MediusFlow](#)
- [New Relic by Organization](#)
- [Oracle Cloud Infrastructure Console](#)

Para más información acerca de cómo proteger mejor una organización mediante el aprovisionamiento automatizado de cuentas de usuario, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

El cifrado de tokens SAML está disponible con carácter general

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

El [cifrado de tokens SAML](#) permite configurar las aplicaciones para que reciban aserciones de SAML cifradas. La característica ya está disponible con carácter general en todas las nubes.

Las notificaciones de nombre de grupo en tokens de aplicación están disponibles con carácter general

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Las notificaciones de grupo emitidas en un token ahora se pueden limitar a los grupos asignados a la aplicación. Esto es especialmente importante cuando los usuarios son miembros de un gran número de grupos y había riesgo de superar los límites de tamaño del token. Esta nueva funcionalidad permite [agregar nombres de grupo a los tokens](#) con carácter general.

La escritura diferida de Workday ahora admite el establecimiento de atributos relativos al número de teléfono del trabajo

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Hemos mejorado la aplicación de aprovisionamiento de escritura diferida de Workday para que admita la escritura diferida de los atributos relativos al número de teléfono del trabajo y al número de móvil. Además del correo electrónico y el nombre de usuario, ahora puede configurar la aplicación de aprovisionamiento de escritura diferida de Workday para transferir los valores de número de teléfono de Azure AD a Workday. Para más información sobre cómo configurar la escritura diferida de números de teléfono, consulte el tutorial de la aplicación de [escritura diferida de Workday](#).

Comprobación del publicador (versión preliminar)

Tipo: Nueva característica

Categoría del servicio: Otros

Funcionalidad del producto: Experiencia para el desarrollador

La comprobación del publicador (versión preliminar) ayuda a los administradores y usuarios finales a reconocer la autenticidad de los desarrolladores de aplicaciones que se integran en la plataforma de identidad de Microsoft.

Para más información, consulte [Comprobación del publicador \(versión preliminar\)](#).

Flujo de código de autorización para aplicaciones de una sola página

Tipo: Característica modificada **Categoría del servicio:** Autenticación **Funcionalidad del producto:**

Experiencia para el desarrollador

Debido a las [restricciones de cookies de terceros como Safari ITP](#) aplicadas en el explorador, las aplicaciones de página única (SPA) tendrán que usar el flujo de código de autorización en lugar del flujo implícito para mantener el SSO. MSAL.js v2.x admite ahora el flujo de código de autorización. Las actualizaciones correspondientes están disponibles en Azure Portal. De este modo, podrá actualizar sus aplicaciones de página única para que sean del tipo "spa" y utilicen el flujo de código de autenticación. Para más instrucciones, consulte [Inicio rápido: Inicio de sesión de los usuarios y obtención de un token de acceso en una SPA de JavaScript mediante el flujo de código de autorización](#).

El filtrado mejorado para dispositivos está en versión preliminar pública

Tipo: Característica modificada

Categoría del servicio: Administración de dispositivos **Funcionalidad del producto:** Administración del ciclo de vida de dispositivos

Antes, los únicos filtros que se podían usar eran "Habilitado" y "Fecha de actividad". Ahora, puede [filtrar la lista de dispositivos en función de más propiedades](#), como el tipo de sistema operativo, el tipo de combinación, el cumplimiento, etc. Estas incorporaciones permitirán encontrar fácilmente un dispositivo determinado.

La nueva experiencia Registros de aplicaciones para Azure AD B2C ya está disponible con carácter general

Tipo: Característica modificada

Categoría del servicio: B2C: administración de identidades de consumidor

Funcionalidad del producto: Administración del ciclo de vida de la identidad

La nueva experiencia Registros de aplicaciones para Azure AD B2C ya está disponible con carácter general.

Antes, había que administrar las aplicaciones Azure AD B2C orientadas al consumidor con independencia del resto de aplicaciones mediante la experiencia "Aplicaciones" heredada. Eso implicaba distintas experiencias de creación de aplicaciones en distintas ubicaciones de Azure.

La nueva experiencia muestra todos los registros de aplicaciones de Azure AD B2C y Azure AD en un solo lugar y proporciona una manera coherente de administrarlos. Si necesita administrar una aplicación orientada al cliente o una aplicación que tenga acceso a Microsoft Graph para administrar recursos de Azure AD B2C mediante

programación, solo tendrá que aprender una manera de hacer cosas.

Puede acceder a la nueva experiencia desde el servicio Azure AD B2C. Una vez ahí, seleccione la hoja Registros de aplicaciones. También puede acceder a la experiencia desde el servicio de Azure Active Directory.

La experiencia Registros de aplicaciones de Azure AD B2C se basa en la [experiencia de registro de aplicaciones](#) general para inquilinos de Azure AD, pero se ha adaptado para Azure AD B2C. La experiencia "Aplicaciones" heredada dejará de utilizarse en el futuro.

Para más información, visite [La nueva experiencia Registros de aplicaciones para Azure Active Directory B2C](#).

Abril de 2020

La experiencia combinada del registro de la información de seguridad ya está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Seguridad y protección de la identidad

La experiencia de registro combinada con autenticación multifactor (MFA) y autoservicio de restablecimiento de contraseña (SSPR) ahora están disponibles con carácter general. Esta nueva experiencia de registro permite a los usuarios registrarse en MFA y SSPR en un único proceso paso a paso. Al implementar la nueva experiencia para la organización, los usuarios pueden registrarse en menos tiempo y con menos complicaciones. Consulte la entrada de blog [aquí](#).

Evaluación continua de acceso

Tipo: Nueva característica

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Seguridad y protección de la identidad

Evaluación continua de acceso es una nueva característica de seguridad que permite el cumplimiento casi en tiempo real de las directivas en los usuarios de confianza que consumen tokens de acceso de Azure AD cuando se producen eventos en Azure AD (por ejemplo, la eliminación de cuentas de usuario). Esta característica la vamos a implementar en primer lugar para clientes de Teams y Outlook. Para más información, consulte el [blog](#) y la [documentación](#).

Inicio de sesión por SMS: Los trabajadores de primera línea pueden iniciar sesión en las aplicaciones respaldadas por Azure AD con su número de teléfono y sin contraseña.

Tipo: Nueva característica

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Office está lanzando una serie de aplicaciones empresariales orientadas a móviles dirigidas a organizaciones no tradicionales y a empleados de grandes organizaciones que no usan el correo electrónico como método de comunicación principal. Estas aplicaciones se dirigen a empleados de primera línea, trabajadores sin escritorio, agentes de campo o empleados de comercios minoristas que podrían no recibir una dirección de correo electrónico de su empleador, tener acceso a un equipo o a recursos de TI. Este proyecto permitirá a estos empleados iniciar sesión en las aplicaciones empresariales solo con un número de teléfono y la devolución de un código. Para más información, consulte la [documentación del administrador](#) y la [documentación del usuario final](#).

Invitar a usuarios internos a usar la colaboración B2B

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto:

Vamos a expandir la funcionalidad de invitación B2B para que se pueda invitar a las cuentas internas existentes a usar las credenciales de colaboración B2B en adelante. Esto se consigue pasando el objeto de usuario a la API de invitación, además de los parámetros típicos, como la dirección de correo electrónico invitada. El identificador de objeto del usuario, su UPN, la pertenencia a grupos, la asignación de aplicaciones, entre otros, permanecen intactos, pero en adelante usarán B2B para autenticarse con las credenciales de su inquilino particular en lugar de con las credenciales internas que usaban antes de la invitación. Para más información, consulte la [documentación](#).

El modo Solo informe para el Acceso condicional ya está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

El [modo Solo informe para el Acceso condicional de Azure AD](#) le permite evaluar el resultado de una directiva sin necesidad de aplicar controles de acceso. Puede probar las directivas del modo Solo informe en toda la organización y comprender su impacto antes de habilitarlas, lo que hará que la implementación sea más segura y fácil. Durante los últimos meses, hemos visto una importante adopción del modo Solo informe, con más de 26 millones de usuarios. Con este anuncio, se crearán nuevas directivas de acceso condicional de Azure AD en modo Solo informe de forma predeterminada. Esto significa que puede supervisar el impacto de las directivas desde el momento en el que se crean. Además, para aquellos usuarios que utilizan Microsoft Graph API, también puede [administrar directivas de Solo informe mediante programación](#).

El libro Conclusiones e informes de Acceso condicional está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

El [libro Conclusiones e informes](#) de Acceso condicional proporciona a los administradores una vista resumida del acceso condicional de Azure AD en el inquilino. Con la funcionalidad de seleccionar una directiva individual, los administradores pueden comprender mejor lo que hace cada directiva y supervisar los cambios en tiempo real. El libro transmite los datos almacenados en Azure Monitor, que puede configurar en unos minutos [según estas instrucciones](#). Para encontrar el panel con más facilidad, lo hemos trasladado a la nueva pestaña Conclusiones e informes del menú Acceso condicional de Azure AD.

La hoja Detalles de la directiva de Acceso condicional está en versión preliminar pública.

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

La nueva [hoja Detalles de la directiva](#) muestra qué asignaciones, condiciones y controles se cumplieron durante la evaluación de la directiva de acceso condicional. Para acceder a la hoja, seleccione una fila en las pestañas **Acceso condicional** o **Solo informe** de los detalles de inicio de sesión.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (abril de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En abril de 2020, hemos agregado a la galería de aplicaciones estas 31 nuevas aplicaciones que admiten federación:

SincroPool Apps, SmartDB, Float, LMS365, IWT Procurement Suite, Lunni, EasySSO for Jira, Virtual Training Academy, Meraki Dashboard, Office 365 Mover, Speaker Engage, Honestly, Ally, DutyFlow, AlertMedia, gr8 People, Pendo, HighGround, Harmony, Timetabling Solutions, SynchroNet CLICK, empower, Fortes Change Cloud, Litmus, GroupTalk, Frontify, MongoDB Cloud, TickitLMS Learn, COCO, Nitro Productivity Suite, Trend Micro Web Security(TMWS)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

La compatibilidad con las consultas delta de Microsoft Graph para oAuth2PermissionGrant está disponible para la versión preliminar pública.

Tipo: Nueva característica

Categoría del servicio: MS Graph

Funcionalidad del producto: Experiencia para el desarrollador

Las consultas delta para oAuth2PermissionGrant están disponibles en versión preliminar pública. Ahora puede realizar el seguimiento de los cambios sin necesidad de sondear Microsoft Graph continuamente. [Más información](#).

La compatibilidad con las consultas delta de Microsoft Graph para contactos de la organización está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: MS Graph

Funcionalidad del producto: Experiencia para el desarrollador

Las consultas delta para contactos de la organización están disponibles con carácter general. Ahora puede realizar el seguimiento de los cambios en las aplicaciones de producción sin necesidad de sondear Microsoft Graph continuamente. Reemplace el código existente que ahora sondea continuamente los datos de orgContact por una consulta delta para mejorar significativamente el rendimiento. [Más información](#).

La compatibilidad con las consultas delta de Microsoft Graph para aplicaciones está disponible con carácter general.

Tipo: Nueva característica

Categoría del servicio: MS Graph

Funcionalidad del producto: Experiencia para el desarrollador

Las consultas delta para aplicaciones están disponibles con carácter general. Ahora puede realizar el seguimiento de los cambios en las aplicaciones de producción sin necesidad de sondear Microsoft Graph continuamente. Reemplace el código existente que ahora sondea continuamente los datos de la aplicación por una consulta delta para mejorar significativamente el rendimiento. [Más información](#).

La compatibilidad con las consultas delta de Microsoft Graph para unidades administrativas está disponible en versión preliminar pública.

Tipo: Nueva característica

Categoría del servicio: MS Graph

Funcionalidad del producto: Las consultas delta de la experiencia del desarrollador para unidades administrativas están disponibles en versión preliminar pública. Ahora puede realizar el seguimiento de los cambios sin necesidad de sondear Microsoft Graph continuamente. [Más información.](#)

Administre los números de teléfono de autenticación y mucho más en las nuevas Microsoft Graph API en versión beta.

Tipo: Nueva característica

Categoría del servicio: MS Graph

Funcionalidad del producto: Experiencia para el desarrollador

Estas API son una herramienta fundamental para administrar los métodos de autenticación de los usuarios. Ahora puede realizar un registro previo y administrar mediante programación los autenticadores usados para MFA y el autoservicio de restablecimiento de contraseña (SSPR). Esta ha sido una de las características más solicitadas en las áreas de Azure MFA, SSPR y Microsoft Graph. Las nuevas API que hemos publicado en esta oleada le ofrecen la posibilidad de:

- Leer, agregar, actualizar y eliminar los teléfonos de autenticación de un usuario
- Restablecer la contraseña de un usuario
- Activar y desactivar el inicio de sesión por SMS

Para más información, consulte [Introducción a la API de métodos de autenticación de Azure AD.](#)

Versión preliminar de las unidades administrativas

Tipo: Nueva característica

Categoría del servicio: RBAC

Funcionalidad del producto: Control de acceso

Las unidades administrativas permiten conceder permisos de administrador que están restringidos a un departamento, a una región o a otro segmento de la organización que se defina. Puede usar las unidades administrativas para delegar permisos en los administradores regionales o establecer directivas de forma pormenorizada. Por ejemplo, un administrador de cuentas de usuario podría actualizar la información del perfil, restablecer las contraseñas y asignar las licencias para los usuarios solo en su unidad administrativa.

Mediante el uso de unidades administrativas, un administrador central podría:

- Crear una unidad administrativa para la administración descentralizada de los recursos.
- Asignar un rol con permisos administrativos solo sobre los usuarios de Azure AD de una unidad administrativa.
- Rellenar las unidades administrativas con usuarios y grupos según sea necesario.

Para más información, consulte [Administración de unidades administrativas en Azure Active Directory \(versión preliminar\).](#)

Roles integrados Administrador de impresoras y Técnico de impresoras

Tipo: Nueva característica

Categoría del servicio: RBAC

Funcionalidad del producto: Control de acceso

Administrador de impresoras: los usuarios con este rol pueden registrar impresoras y administrar todos los aspectos de todas las configuraciones de impresora en la solución de impresión universal de Microsoft, incluida la

configuración del conector de impresión universal. Pueden dar su consentimiento a todas las solicitudes de permiso de impresión delegada. Los administradores de impresoras también tienen acceso a los informes de impresión.

Técnico de impresoras: los usuarios con este rol pueden registrar impresoras y administrar el estado de la impresora en la solución de impresión universal de Microsoft. También pueden leer toda la información del conector. Una tarea clave que un Técnico de impresoras no puede realizar es establecer permisos de usuario en las impresoras ni compartir impresoras. [Más información](#).

Rol integrado Administrador de identidades híbridas

Tipo: Nueva característica

Categoría del servicio: RBAC

Funcionalidad del producto: Control de acceso

Los usuarios de este rol pueden habilitar, configurar y administrar servicios y configuraciones relacionados con la habilitación de la identidad híbrida en Azure AD. Este rol concede la capacidad de configurar Azure AD en uno de los tres métodos de autenticación admitidos: la sincronización de hash de contraseña (PHS), la autenticación de paso a través (PTA) o la federación (AD FS o proveedor de federación de terceros), así como implementar la infraestructura local relacionada para habilitarlos. La infraestructura local incluye agentes de aprovisionamiento y PTA. Este rol concede la capacidad de habilitar el inicio de sesión único de conexión directa (S-SSO) para habilitar la autenticación directa en dispositivos que no son de Windows 10 o equipos que no son de Windows Server 2016. Además, este rol concede la capacidad de ver los registros de inicio de sesión y el acceso a los datos de mantenimiento y análisis para la supervisión y la solución de problemas. [Más información](#).

Rol integrado Administrador de red

Tipo: Nueva característica

Categoría del servicio: RBAC

Funcionalidad del producto: Control de acceso

Los usuarios con este rol pueden revisar las recomendaciones de la arquitectura de perímetro de red de Microsoft que se basan en la telemetría de red desde sus ubicaciones de usuario. El rendimiento de red para Office 365 se basa en una arquitectura de perímetro de red de cliente empresarial rigurosa que suele ser específica de la ubicación del usuario. Este rol permite la edición de ubicaciones de usuario detectadas y la configuración de parámetros de red para esas ubicaciones con el fin de facilitar la mejora de las medidas de telemetría y las recomendaciones de diseño. [Más información](#).

Actividad y descargas masivas en la experiencia del portal de administración de Azure AD

Tipo: Nueva característica

Categoría del servicio: User Management

Funcionalidad del producto: Directorio

Ahora puede realizar actividades masivas con usuarios y grupos de Azure AD mediante la carga de un archivo CSV en la experiencia del portal de administración de Azure AD. Puede crear usuarios o eliminar usuarios, e invitar a usuarios. También puede agregar y quitar miembros de un grupo.

Además, puede descargar listas de recursos de Azure AD desde la experiencia del portal de administración de Azure AD. Puede descargar la lista de usuarios del directorio, la lista de grupos del directorio y los miembros de un grupo determinado.

Para más información, consulte lo siguiente:

- [Crear usuarios o invitar a usuarios](#) .
 - [Eliminar usuarios o restaurar usuarios eliminados](#).
 - [Descargar la lista de usuarios o descargar la lista de grupos](#)
 - [Aregar \(importar\) miembros, eliminar miembros o descargar la lista de miembros](#) de un grupo.
-

Administración delegada de usuarios Mi personal

Tipo: Nueva característica

Categoría del servicio: User Management

Funcionalidad del producto:

Mi personal permite a los administradores de primera línea, como el administrador de una tienda, garantizar que los miembros del personal puedan acceder a sus cuentas de Azure AD. En lugar de depender de un departamento de soporte técnico central, las organizaciones pueden delegar tareas comunes, como el restablecimiento de contraseñas o el cambio de números de teléfono, en un administrador de primera línea. Con Mi personal, un usuario que no puede acceder a su cuenta puede recuperar el acceso con tan solo un par de clics, sin necesidad de ayuda del personal de TI o el departamento de soporte técnico. Para más información, consulte [Administración de usuarios con Mi personal \(versión preliminar\)](#) y [Delegación de la administración de usuarios con Mi personal \(versión preliminar\)](#).

Una experiencia de usuario final actualizada en las revisiones de acceso

Tipo: Característica modificada

Categoría del servicio: Revisiones de acceso

Funcionalidad del producto: Identity Governance

Hemos actualizado la experiencia del revisor para las revisiones de acceso de Azure AD en el portal Aplicaciones. A finales de abril, los revisores que han iniciado sesión en la experiencia del revisor de las revisiones de acceso de Azure AD, verán un banner que les permitirá probar la experiencia actualizada en Mi acceso. Tenga en cuenta que la experiencia de revisiones de acceso actualizada ofrece la misma funcionalidad que la experiencia actual, pero con una interfaz de usuario mejorada sobre nuevas funcionalidades para permitir que los usuarios sean productivos. [Aquí encontrará más información sobre la experiencia actualizada](#). Esta versión preliminar pública durará hasta finales de julio de 2020. A finales de julio, los revisores que no hayan participado en la experiencia en versión preliminar serán redirigidos automáticamente a Mi acceso para realizar las revisiones de acceso. Si desea que los revisores cambien permanentemente a la experiencia en versión preliminar en Mi acceso ahora, [realice una solicitud aquí](#).

Las aplicaciones de aprovisionamiento y escritura diferida de usuarios de entrada de WorkDay ahora admiten las versiones más recientes de la API Workday Web Services

Tipo: Característica modificada

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto:

Hemos tenido en cuenta los comentarios de los clientes y hemos actualizado las aplicaciones de aprovisionamiento y escritura diferida de usuarios de entrada de WorkDay en la galería de aplicaciones empresariales para admitir las versiones más recientes de la API Workday Web Services (WWS). Con este cambio, los clientes pueden especificar la versión de la API WWS que desean usar en la cadena de conexión. Esto proporciona a los clientes la capacidad de recuperar más atributos de recursos humanos disponibles en las versiones de WorkDay. La aplicación de escritura diferida de WorkDay ahora usa el servicio web de WorkDay recomendado, Change_Work_Contact_Info, para superar las limitaciones de Maintain_Contact_Info.

De forma predeterminada, si no se especifica ninguna versión en la cadena de conexión, las aplicaciones de aprovisionamiento de entrada de WorkDay seguirán usando WWS v21.1. Para cambiar a las versiones más recientes de la API Workday Web Services para el aprovisionamiento de usuarios de entrada, los clientes deben actualizar la cadena de conexión tal y como se documenta [en el tutorial](#), y también actualizar los valores de XPATH utilizados para los atributos de WorkDay, tal y como se describe en [Guía de referencia de atributos de Workday](#).

Para usar la nueva API para la escritura diferida, no se requieren cambios en la aplicación de aprovisionamiento de escritura diferida de WorkDay. En WorkDay, asegúrese de que la cuenta de usuario del sistema de integración (ISU) de WorkDay tiene permisos para invocar el proceso empresarial Change_Work_Contact, tal y como se describe en la sección del tutorial [Configuración de los permisos de la directiva de seguridad de procesos empresariales](#).

Hemos actualizado la [guía de tutoriales](#) para reflejar la compatibilidad con la nueva versión de la API.

Los usuarios con el rol de acceso predeterminado ahora están dentro del ámbito del aprovisionamiento

Tipo: Característica modificada

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Históricamente, los usuarios con el rol de acceso predeterminado han estado fuera del ámbito del aprovisionamiento. Hemos recibido comentarios acerca de que los clientes quieren que los usuarios con este rol estén dentro del ámbito del aprovisionamiento. A partir del 16 de abril de 2020, todas las nuevas configuraciones de aprovisionamiento permiten aprovisionar a los usuarios con el rol de acceso predeterminado. Cambiaremos gradualmente el comportamiento de las configuraciones de aprovisionamiento existentes para admitir el aprovisionamiento de usuarios con este rol. [Más información](#).

Actualización de la interfaz de usuario de aprovisionamiento

Tipo: Característica modificada

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Hemos actualizado la experiencia de aprovisionamiento para crear una vista de administración más centrada. Cuando vaya a la hoja de aprovisionamiento de una aplicación empresarial que ya se ha configurado, podrá supervisar fácilmente el progreso del aprovisionamiento y administrar acciones como el inicio, la detención y el reinicio del aprovisionamiento. [Más información](#).

La validación de reglas de grupos dinámicos ahora está disponible en versión preliminar pública

Tipo: Característica modificada

Categoría del servicio: Administración de grupos

Funcionalidad del producto: Colaboración

Azure Active Directory (Azure AD) ahora ofrece los medios para validar las reglas de grupos dinámicos. En la pestaña **Validación de las reglas**, puede validar la regla dinámica con los miembros del grupo de ejemplo, para confirmar que la regla funciona según lo previsto. Al crear o actualizar reglas de grupos dinámicos, los administradores quieren saber si un usuario o un dispositivo será miembro del grupo. Esto ayuda a evaluar si el usuario o el dispositivo cumplen los criterios de la regla y ayuda a solucionar problemas cuando no se espera la pertenencia.

Para más información, consulte [Validación de una regla de pertenencia dinámica a grupos \(versión preliminar\)](#).

Puntuación de seguridad de la identidad: valores predeterminados de seguridad y actualizaciones de las

acciones de mejora de MFA

Tipo: Característica modificada

Categoría del servicio: N/D

Funcionalidad del producto: Seguridad y protección de la identidad

Compatibilidad con los valores predeterminados de seguridad para las acciones de mejora de Azure AD:

La Puntuación de seguridad de Microsoft se actualizará con acciones de mejora para admitir [valores predeterminados de seguridad en Azure AD](#), lo que facilita la protección de la organización con una configuración de seguridad preconfigurada para ataques comunes. Esto afectará a las siguientes acciones de mejora:

- Garantizar que todos los usuarios pueden completar la autenticación multifactor para el acceso seguro
- Requerir MFA para roles administrativos
- Habilitar la directiva para bloquear la autenticación heredada

Actualizaciones de las acciones de mejora de MFA: Para reflejar la necesidad de las empresas de garantizar la mayor seguridad al aplicar directivas que funcionen con su negocio, la Puntuación de seguridad de Microsoft ha eliminado tres acciones de mejora centradas en la autenticación multifactor y ha agregado otras dos.

Acciones de mejora eliminadas:

- Registrar a todos los usuarios para la autenticación multifactor
- Exigir autenticación multifactor para todos los usuarios
- Requerir MFA para roles con privilegios Azure AD

Acciones de mejora agregadas:

- Garantizar que todos los usuarios pueden completar la autenticación multifactor para el acceso seguro
- Requerir MFA para roles administrativos

Estas nuevas acciones de mejora requerirán el registro de usuarios o administradores para la autenticación multifactor (MFA) en todo el directorio y el establecimiento del conjunto adecuado de directivas que se adapten a las necesidades de la organización. El objetivo principal es tener flexibilidad, asegurando al mismo tiempo que todos los usuarios y administradores puedan autenticarse con varios factores o solicitudes de comprobación de identidad basadas en riesgos. Se puede hacer con varias directivas que apliquen decisiones de ámbito o estableciendo valores predeterminados de seguridad (a partir del 16 de marzo) que permitan a Microsoft decidir cuándo desafiar a los usuarios con MFA. [Más información sobre las novedades en la Puntuación de seguridad de Microsoft](#).

Marzo de 2020

Cuentas de Azure Active Directory no administradas en la actualización B2B de marzo de 2021

Tipo: Plan de cambio

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

A partir del 31 de marzo de 2021, Microsoft dejará de admitir el canje de invitaciones mediante la creación de cuentas de Azure Active Directory (Azure AD) no administradas e inquilinos para escenarios de colaboración B2B. Como preparación para esto, le recomendamos que opte por la [autenticación de código de acceso de un solo uso por correo electrónico](#).

Los usuarios con el rol de acceso predeterminado estarán dentro del ámbito del aprovisionamiento.

Tipo: Plan de cambio

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Históricamente, los usuarios con el rol de acceso predeterminado han estado fuera del ámbito del aprovisionamiento. Hemos recibido comentarios acerca de que los clientes quieren que los usuarios con este rol estén dentro del ámbito del aprovisionamiento. Estamos trabajando en la implementación de un cambio para que todas las nuevas configuraciones de aprovisionamiento permitan aprovisionar a los usuarios con el rol de acceso predeterminado. Gradualmente, cambiaremos el comportamiento de las configuraciones de aprovisionamiento existentes para admitir el aprovisionamiento de usuarios con este rol. No se requiere ninguna acción del cliente. Publicaremos una actualización en la [documentación](#) una vez que este cambio esté en vigor.

La colaboración B2B de Azure AD estará disponible en Microsoft Azure controlado por inquilinos de 21Vianet (Azure China 21Vianet).

Tipo: Plan de cambio

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Las funcionalidades de colaboración B2B de Azure AD estarán disponibles en Microsoft Azure controlado por los inquilinos de 21Vianet (Azure China 21Vianet), lo que permite a los usuarios de un inquilino de Azure China 21Vianet colaborar sin problemas con los usuarios de otros inquilinos de Azure China 21Vianet. [Más información sobre la colaboración B2B de Azure AD.](#)

Rediseño del correo electrónico de invitación de colaboración B2B de Azure AD

Tipo: Plan de cambio

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Los [correos electrónicos](#) enviados por el servicio de invitación de colaboración B2B de Azure AD para invitar a los usuarios al directorio se rediseñarán para que la información de la invitación y los siguientes pasos del usuario sean más claros.

Los cambios de la directiva HomeRealmDiscovery aparecerán en los registros de auditoría

Tipo: Corregido

Categoría del servicio: Auditoría

Funcionalidad del producto: Supervisión e informes

Se ha corregido un error por el que los cambios en la [directiva HomeRealmDiscovery](#) no se incluían en los registros de auditoría. Ahora podrá ver cuándo y cómo ha cambiado la directiva, y quién la cambió.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (marzo de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En marzo de 2020, hemos agregado estas 51 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Cisco AnyConnect](#), [Zoho One China](#), [PlusPlus](#), [Profit.co SAML App](#), [iPoint Service Provider](#), [contextt.ai SPHERE](#), [Wisdom By Invictus](#), [Flare Digital Signage](#), [Logz.io - Cloud Observability for Engineers](#), [SpectrumU](#), [BizzContact](#), [Elqano SSO](#), [MarketSignShare](#), [CrossKnowledge Learning Suite](#), [Netvision Compas](#), [FCM HUB](#), [RIB A/S Byggeweb Mobile](#), [GoLinks](#), [Datadog](#), [Zscaler B2B User Portal](#), [LIFT](#), [Planview Enterprise One](#), [WatchTeams](#), [Aster](#), [Skills Workflow](#), [Node Insight](#), [IP Platform](#), [InVision](#), [Pipedrive](#), [Showcase Workshop](#), [Greenlight Integration Platform](#), [Greenlight Compliant Access Management](#), [Grok Learning](#), [Miradore Online](#), [Khoros Care](#), [AskYourTeam](#), [TruNarrative](#), [Smartwaiver](#), [Bizagi Studio for Digital Process Automation](#), [insuiteX](#), [sybo](#), [Britive](#), [WhosOffice](#), [E-days](#),

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Está disponible la colaboración B2B de Azure AD en inquilinos de Azure Government

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: B2B/B2C

Las características de colaboración B2B de Azure AD ahora están disponibles entre algunos inquilinos de Azure Government. Para averiguar si su inquilino es capaz de usar estas funcionalidades, siga las instrucciones que se indican en [¿Cómo puedo saber si la colaboración B2B está disponible en mi inquilino de Azure US Government?](#)

La integración de Azure Monitor para los registros de Azure ahora está disponible en Azure Government

Tipo: Nueva característica

Categoría del servicio: Notificación

Funcionalidad del producto: Supervisión e informes

La integración de Azure Monitor en los registros de Azure AD ahora está disponible en Azure Government. Puede enrutar los registros de Azure AD (registros de auditoría e inicio de sesión) a una cuenta de almacenamiento, un centro de eventos y Log Analytics. Consulte la [documentación detallada](#), así como los [planes de implementación para la elaboración de informes y la supervisión](#) para escenarios de Azure AD.

Actualización de Identity Protection en Azure Government

Tipo: Nueva característica

Categoría del servicio: Protección de identidad

Funcionalidad del producto: Seguridad y protección de la identidad

Nos complace compartir que ahora hemos implementado la experiencia actualizada de [Azure AD Identity Protection](#) en el [portal de Microsoft Azure Government](#). Para obtener más información, consulte nuestra [entrada de blog de anuncio](#).

Recuperación ante desastres: Descarga y almacenamiento de la configuración de aprovisionamiento

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

El servicio de aprovisionamiento de Azure AD proporciona un amplio conjunto de funcionalidades de configuración. Los clientes deben poder guardar su configuración para poder consultarla más adelante o revertir a una versión válida conocida. Hemos agregado la capacidad de descargar la configuración de aprovisionamiento como archivo JSON y cargarlo cuando sea necesario. [Más información](#).

SSPR (autoservicio de restablecimiento de contraseña) ahora requiere dos puertas para los administradores en Microsoft Azure controlado por 21Vianet (Azure China 21Vianet)

Tipo: Característica modificada

Categoría del servicio: Restablecimiento de contraseña de autoservicio

Funcionalidad del producto: Seguridad y protección de la identidad

Anteriormente, en Microsoft Azure controlado por 21Vianet (Azure China 21Vianet), los administradores que usaban el autoservicio de restablecimiento de contraseña (SSPR) para restablecer sus propias contraseñas solo necesitaban una "puerta" (desafío) para demostrar su identidad. En las nubes públicas y en otras nubes nacionales,

los administradores generalmente deben usar dos puertas para demostrar su identidad al usar SSPR. No obstante, dado que no se admiten las llamadas telefónicas ni SMS en Azure China 21Vianet, hemos permitido que los administradores restablezcan la contraseña con una sola puerta.

Estamos creando la paridad de características de SSPR entre Azure China 21Vianet y la nube pública. En el futuro, los administradores deberán usar dos puertas al usar SSPR. Se admitirán SMS, llamadas telefónicas, y códigos y notificaciones de aplicación de autenticador. [Más información](#).

La longitud de las contraseñas está limitada a 256 caracteres

Tipo: Característica modificada

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Para garantizar la confiabilidad del servicio de Azure AD, las contraseñas de usuario ahora tienen una longitud máxima de 256 caracteres. A los usuarios con contraseñas más largas que esta se les pedirá que cambien su contraseña en el inicio de sesión subsiguiente, ya sea poniéndose en contacto con su administrador o mediante la característica de autoservicio de restablecimiento de contraseña.

Este cambio se habilitó el 13 de marzo de 2020, a las 10:00 PST (18:00 UTC), y el error es AADSTS 50052, InvalidPasswordExceedsMaxLength. Para obtener más información, consulte el [aviso de cambio importante](#).

Los registros de inicio de sesión de Azure AD ahora están disponibles para todos los inquilinos gratuitos a través de Azure Portal

Tipo: Característica modificada

Categoría del servicio: Notificación

Funcionalidad del producto: Supervisión e informes

A partir de ahora, los clientes que dispongan de inquilinos gratuitos pueden tener acceso a los [registros de inicio de sesión de Azure AD desde Azure Portal](#) para un máximo de 7 días. Anteriormente, los registros de inicio de sesión solo estaban disponibles para los clientes con licencias de Azure Active Directory Premium. Con este cambio, todos los inquilinos pueden tener acceso a estos registros a través del portal.

NOTE

Los clientes todavía necesitan una licencia Premium (Azure Active Directory Premium P1 o P2) para tener acceso a los registros de inicio de sesión a través de Microsoft Graph API y Azure Monitor.

Opción en desuso de grupos de todo el directorio de la configuración general de grupos en Azure Portal

Tipo: Obsoleto

Categoría del servicio: Administración de grupos

Funcionalidad del producto: Colaboración

Para ofrecer a los clientes una manera más flexible de crear grupos de todo el directorio que se adapte mejor a sus necesidades, hemos reemplazado la opción **Grupos de todo el directorio** de la opción **Grupos > General** en Azure Portal por un vínculo a la [documentación de grupos dinámicos](#). Hemos mejorado la documentación para incluir más instrucciones para que los administradores puedan crear grupos de todos los usuarios que incluyan o excluyan usuarios invitados.

Febrero de 2020

Próximos cambios en los controles personalizados

Tipo: Plan de cambio

Categoría del servicio: MFA

Funcionalidad del producto: Seguridad y protección de la identidad

Tenemos previsto reemplazar la versión preliminar actual de los controles personalizados por un enfoque que permita que las funcionalidades de autenticación proporcionadas por el partner funcionen sin problemas con las experiencias de administrador y usuario final de Azure Active Directory. Hoy en día, las soluciones de MFA de los partners enfrentan las siguientes limitaciones: solo funcionan después de haber escrito una contraseña; no sirven como MFA para la autenticación de nivel superior en otros escenarios clave; y no se integran con las funciones de administración de credenciales administrativas ni de usuario final. La nueva implementación permitirá que los factores de autenticación proporcionados por los partners funcionen junto con factores integrados para escenarios clave, como el registro, el uso, las notificaciones de MFA, la autenticación de nivel superior, la creación de informes y el registro.

Los controles personalizados se seguirán admitiendo en la versión preliminar junto con el nuevo diseño hasta que alcancen la disponibilidad general. En ese momento, daremos tiempo a los clientes para migrar al nuevo diseño. Debido a las limitaciones del enfoque actual, no se incorporarán nuevos proveedores hasta que el nuevo diseño esté disponible. Estamos trabajando en estrecha colaboración con los clientes y proveedores, y comunicaremos los plazos a medida que nos acerquemos. [Más información](#).

Puntuación de seguridad de la identidad: actualizaciones de acciones de mejora de MFA

Tipo: Plan de cambio

Categoría del servicio: MFA

Funcionalidad del producto: Seguridad y protección de la identidad

Para reflejar la necesidad de las empresas de garantizar la mayor seguridad al aplicar directivas que funcionen con su negocio, la puntuación segura de Microsoft va a quitar tres acciones de mejora centradas en la autenticación multifactor (MFA) y va a añadir otras dos.

Se quitarán las siguientes acciones de mejora:

- Registrar todos los usuarios de MFA
- Exigir autenticación multifactor para todos los usuarios
- Requerir MFA para roles con privilegios Azure AD

Se agregarán las siguientes acciones de mejora:

- Asegurarse de que todos los usuarios pueden completar MFA para el acceso seguro
- Requerir MFA para roles administrativos

Estas nuevas acciones de mejora requerirán el registro de usuarios o administradores para MFA en todo el directorio y el establecimiento del conjunto adecuado de directivas que se adapten a las necesidades de la organización. El objetivo principal es tener flexibilidad, asegurando al mismo tiempo que todos los usuarios y administradores puedan autenticarse con varios factores o solicitudes de comprobación de identidad basadas en riesgos. Esto puede traducirse en la configuración de valores predeterminados de seguridad que permitan a Microsoft decidir cuándo desafiar a los usuarios para MFA o el mantenimiento de varias directivas que apliquen decisiones de ámbito. Como parte de estas actualizaciones de acciones de mejora, las directivas de protección de línea de base ya no se incluirán en los cálculos de puntuación. [Obtenga más información sobre lo próximo de la puntuación segura de Microsoft](#).

Selección de SKU Azure AD Domain Services

Tipo: Nueva característica

Categoría del servicio: Azure AD Domain Services

Funcionalidad del producto: Azure AD Domain Services

Hemos escuchado los comentarios de los clientes de Azure AD Domain Services que desean más flexibilidad a la

hora de seleccionar los niveles de rendimiento de sus instancias. A partir del 1 de febrero de 2020, cambiamos de un modelo dinámico (donde Azure AD determina el rendimiento y el plan de tarifa en función del número de objetos) a un modelo de selección automática. Ahora los clientes pueden elegir un nivel de rendimiento que se adapte a su entorno. Este cambio también nos permite habilitar nuevos escenarios, como los bosques de recursos, y características Premium, como las copias de seguridad diarias. El número de objetos es ahora ilimitado para todas las SKU, pero seguiremos ofreciendo sugerencias de cantidades de objetos para cada nivel.

No se requiere ninguna acción inmediata del cliente. Para los clientes actuales, el nivel dinámico que estaba en uso el 1 de febrero de 2020 determina el nuevo nivel predeterminado. El resultado de este cambio no afecta al precio ni al rendimiento. A partir de entonces, los clientes de Azure AD DS deberán evaluar los requisitos de rendimiento a medida que cambien sus características de carga de trabajo y el tamaño del directorio. El cambio entre los niveles de servicio seguirá siendo una operación sin tiempo de inactividad, y ya no se moverá automáticamente a los clientes a nuevos niveles en función del crecimiento de su directorio. Además, no habrá ningún aumento del precio y los nuevos precios se alinearán con nuestro modelo de facturación actual. Para obtener más información, consulte la [documentación de las SKU de Azure AD DS](#) y la [página de precios de Azure AD Domain Services](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (febrero de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En febrero de 2020, hemos agregado estas 31 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[IamIP Patent Platform](#), [Experience Cloud](#), [NS1 SSO For Azure](#), [Barracuda Email Security Service](#), [ABa Reporting](#), [In Case of Crisis - Online Portal](#), [BIC Cloud Design](#), [Beekeeper Azure AD Data Connector](#), [Korn Ferry Assessments](#), [Verkada Command](#), [Splashtop](#), [Syxsense](#), [EAB Navigate](#), [New Relic \(Limited Release\)](#), [Thulium](#), [Ticket Manager](#), [Template Chooser for Teams](#), [Beesy](#), [Health Support System](#), [MURAL](#), [Hive](#), [LavaDo](#), [Wakelet](#), [Firmex VDR](#), [ThingLink for Teachers and Schools](#), [Coda](#), [NearpodApp](#), [WEDO](#), [InvitePeople](#), [Reprints Desk - Article Galaxy](#), [TeamViewer](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevos conectores de aprovisionamiento en la galería de aplicaciones de Azure AD (febrero de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [Mixpanel](#)
- [TeamViewer](#)
- [Azure Databricks](#)
- [PureCloud by Genesys](#)
- [Zapier](#)

Para más información acerca de cómo proteger mejor una organización mediante el aprovisionamiento automatizado de cuentas de usuario, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

Compatibilidad de Azure AD con las claves de seguridad de FIDO2 en entornos híbridos

Tipo: Nueva característica

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Anunciamos la versión preliminar pública de la compatibilidad de Azure AD con las claves de seguridad de FIDO2 en entornos híbridos. Los usuarios ahora pueden usar las claves de seguridad de FIDO2 para iniciar sesión en sus dispositivos de Windows 10 unidos a Azure AD híbrido y obtener un inicio de sesión fluido en sus recursos locales y en la nube. La compatibilidad con entornos híbridos ha sido la característica más solicitada de nuestros clientes sin contraseña, ya que inicialmente lanzamos la versión preliminar pública para la compatibilidad con FIDO2 en dispositivos unidos a Azure AD. La autenticación sin contraseña mediante tecnologías avanzadas como la biométrica y la criptografía de clave privada y pública es cómoda y fácil de usar a la vez que segura. Con esta versión preliminar pública, ahora puede usar la autenticación moderna como las claves de seguridad de FIDO2 para acceder a los recursos de Active Directory tradicionales. Para obtener más información, vaya a [Inicio de sesión único en recursos locales](#).

Para empezar, visite [Habilitación de las claves de seguridad FIDO2 para un inquilino](#) para obtener instrucciones paso a paso.

La nueva experiencia de Mi cuenta ya está disponible con carácter general.

Tipo: Característica modificada

Categoría del servicio: Mi perfil/cuenta

Funcionalidad del producto: Experiencias de usuario final

Mi cuenta, el punto en el que se atienden todas las necesidades de administración de las cuentas de usuario final, ya está disponible con carácter general. Los usuarios finales pueden tener acceso a este nuevo sitio a través de la dirección URL o en el encabezado de la nueva experiencia Mis aplicaciones. Obtenga más información sobre todas las funcionalidades de autoservicio que ofrece la nueva experiencia en [¿Qué es el portal Mi cuenta?](#)

Actualización de la dirección URL del sitio de Mi cuenta a myaccount.microsoft.com

Tipo: Característica modificada

Categoría del servicio: Mi perfil/cuenta

Funcionalidad del producto: Experiencias de usuario final

La nueva experiencia de usuario final de Mi cuenta actualizará su dirección URL a <https://myaccount.microsoft.com> el próximo mes. Obtenga más información sobre la experiencia y todas las funcionalidades de autoservicio de cuenta que ofrece a los usuarios finales en la [ayuda del portal Mi cuenta](#).

Enero de 2020

El nuevo portal Mis aplicaciones ya está disponible con carácter general

Tipo: Plan de cambio

Categoría del servicio: Mis aplicaciones

Funcionalidad del producto: Experiencias de usuario final

Actualice su organización al nuevo portal Mis aplicaciones que ya está disponible con carácter general. Puede encontrar más información sobre el nuevo portal y las colecciones en [Creación de colecciones en el portal Mis aplicaciones](#).

Las áreas de trabajo de Azure AD se han renombrado a colecciones

Tipo: Característica modificada

Categoría del servicio: Mis aplicaciones

Funcionalidad del producto: Experiencias de usuario final

Las áreas de trabajo, que son filtros que los administradores pueden configurar para organizar las aplicaciones de sus usuarios, ahora se llamarán colecciones. Obtenga más información sobre cómo configurarlas en [Creación de colecciones en el portal Mis aplicaciones](#).

Registro e inicio de sesión mediante teléfono en Azure AD B2C con una directiva personalizada (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: B2C: administración de identidades de consumidor

Funcionalidad del producto: B2B/B2C

Con el registro y el inicio de sesión mediante el número de teléfono, los desarrolladores y las empresas pueden permitir a sus clientes registrarse e iniciar sesión con una contraseña de un solo uso enviada al número de teléfono del usuario a través de un SMS. Esta característica también permite al cliente cambiar su número de teléfono si pierde el acceso a su dispositivo. Con la eficacia de las directivas personalizadas, el registro y el inicio de sesión mediante el teléfono permiten a los desarrolladores y a las empresas comunicar su marca a través de la personalización de la página. Aprenda cómo [configurar el registro y el inicio de sesión en el teléfono con directivas personalizadas en Azure AD B2C](#).

Nuevos conectores de aprovisionamiento en la galería de aplicaciones de Azure AD (enero de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [Promapp](#)
- [Zscaler Private Access](#)

Para más información acerca de cómo proteger mejor una organización mediante el aprovisionamiento automatizado de cuentas de usuario, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (enero de 2020)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En enero de 2020, hemos agregado estas 33 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[JOSA](#), [Fastly Edge Cloud](#), [Terraform Enterprise](#), [Spintr SSO](#), [Aabit Netlogistik](#), [SkyKick](#), [Upshotly](#), [LeaveBot](#), [DataCamp](#), [TripActions](#), [SmartWork](#), [Dotcom-Monitor](#), [SSOGEN - Azure AD SSO Gateway for Oracle E-Business Suite - EBS](#), [PeopleSoft y JDE](#), [Hosted MyCirqa SSO](#), [Yuhu Property Management Platform](#), [LumApps](#), [Upwork Enterprise](#), [Talentsoft](#), [SmartDB for Microsoft Teams](#), [PressPage](#), [ContractSafe Saml2 SSO](#), [Maxient Conduct Manager Software](#), [Helpshift](#), [PortalTalk 365](#), [CoreView](#), [Squelch Cloud Office365 Connector](#), [PingFlow Authentication](#), [PrinterLogic SaaS](#), [Taskize Connect](#), [Sandwai](#), [EZRentOut](#), [AssetSonar](#), [Akari Virtual Assistant](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Dos nuevas detecciones de Identity Protection

Tipo: Nueva característica

Categoría del servicio: Protección de identidad

Funcionalidad del producto: Seguridad y protección de la identidad

Hemos agregado a Identity Protection dos nuevos tipos de detección vinculados al inicio de sesión: Reglas de manipulación sospechosa de la bandeja de entrada y Viaje imposible. Microsoft Cloud App Security (MCAS) descubre estas detecciones sin conexión e influye en los riesgos de usuario y de inicio de sesión en Identity Protection. Para más información sobre estas detecciones, consulte nuestros [tipos de riesgo de inicio de sesión](#).

Cambio de última hora: los fragmentos de URI no se trasladarán a través de la redirección de inicio de sesión

Tipo: Característica modificada

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

A partir del 8 de febrero de 2020, cuando se envíe una solicitud a login.microsoftonline.com para que un usuario inicie sesión, el servicio anexará un fragmento vacío a la solicitud. Esto evita una clase de ataques de redireccionamiento, ya que se asegura de que el explorador borra todo fragmento existente en la solicitud. Ninguna aplicación debe tener una dependencia de este comportamiento. Para más información, consulte [Cambios importantes](#) en la documentación de la plataforma de identidad de Microsoft.

Novedades de Azure Active Directory en Microsoft 365 Government

22/07/2020 • 4 minutes to read • [Edit Online](#)

Hemos realizado algunos cambios en Azure Active Directory (Azure AD) en la instancia en la nube de Microsoft 365 Government, que es aplicable a los clientes que usan los siguientes servicios:

- Microsoft Azure Government
- Microsoft 365 Government – GCC High
- Microsoft 365 Government – DoD

Este artículo no se aplica a los clientes de Microsoft 365 Government – GCC.

Cambios realizados en el nombre de dominio inicial

Durante la suscripción inicial de su organización a un servicio en línea de Microsoft 365 Government, se le pidió que eligiera el nombre de dominio de su organización, <your-domain-name>.onmicrosoft.com. Si ya tiene un nombre de dominio con el sufijo .com, nada cambiará.

Sin embargo, si está registrándose para un nuevo servicio de Microsoft 365 Government, le pedirá que elija un nombre de dominio con el sufijo .us. Por lo tanto, será <your-domain-name>.onmicrosoft.us.

NOTE

Este cambio no se aplica a todos los clientes que están administrados por los proveedores de servicios en la nube (CSP).

Cambios realizados en el acceso al portal

Hemos actualizado los puntos de conexión del portal de Microsoft Azure Government, Microsoft 365 Government – GCC High y Microsoft 365 Government – DoD, como se muestra en la [tabla de asignación de puntos de conexión](#).

Antes, los clientes podían iniciar sesión en cualquier parte del mundo con el portal de Azure (portal.azure.com) y con el portal de Office 365 (portal.office.com). Con esta actualización, ahora los clientes deben iniciar sesión con los portales específicos de Microsoft Azure Government, Microsoft 365 Government - GCC High y Microsoft 365 Government - DoD.

Asignación de puntos de conexión

En la siguiente tabla se muestran los puntos de conexión para todos los clientes:

NOMBRE	DETALLES DEL PUNTO DE CONEXIÓN
Portales	Microsoft Azure Government: https://portal.azure.us Microsoft 365 Government – GCC High: https://portal.office365.us Microsoft 365 Government – DoD: https://portal.apps.mil

NOMBRE	DETALLES DEL PUNTO DE CONEXIÓN
Punto de conexión de Azure Active Directory Authority	https://login.microsoftonline.us
Microsoft Graph API para Microsoft 365 Government - GCC High	https://graph.microsoft.us
Microsoft Graph API para Microsoft 365 Government - DoD	https://dod-graph.microsoft.us
Puntos de conexión de servicio de Azure Government	Para obtener más información, vea Guía para desarrolladores de Azure Government
Puntos de conexión de Microsoft 365 Government - GCC High	Para obtener más información, consulte Office 365 U.S. Government GCC High endpoints (Puntos de conexión de Office 365 U.S. Government GCC High)
Microsoft 365 Government - DoD	Para obtener más información, consulte Office 365 U.S. Government DoD endpoints (Puntos de conexión de Office 365 U.S. Government DoD)

Pasos siguientes

Para obtener más información, consulte estos artículos:

- [¿Qué es Azure Government?](#)
- [Azure Government AAD Authority Endpoint Update](#) (Actualización del punto de conexión de la entidad de AAD de Azure Government)
- [Puntos de conexión de Microsoft Graph en la nube del US Gov](#)
- [Office 365 US Government GCC High y DoD](#)

Archivo de ¿Cuáles son las novedades de Azure Active Directory?

22/07/2020 • 329 minutes to read • [Edit Online](#)

El artículo principal de notas de la versión [¿Cuáles son las novedades de Azure Active Directory?](#) contiene las actualizaciones de los últimos seis meses, mientras que este artículo contiene toda la información más antigua.

Las notas de la versión [¿Cuáles son las novedades de Azure Active Directory?](#) proporcionan información sobre:

- Versiones más recientes
- Problemas conocidos
- Corrección de errores
- Funciones obsoletas
- Planes de cambios

Diciembre de 2019

Integración del aprovisionamiento de SAP SuccessFactors en Azure AD y AD local (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Aprovisionamiento de aplicaciones

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Ahora puede integrar SAP SuccessFactors como origen de identidad relevante en Azure AD. Esta integración le ayuda a automatizar el ciclo de vida de la identidad de un extremo a otro, incluido el uso de eventos basados en recursos humanos, como nuevas contrataciones o resoluciones de contrato, para controlar el aprovisionamiento de cuentas de Azure AD.

Para obtener más información sobre cómo configurar el aprovisionamiento de entrada de SAP SuccessFactors para Azure AD, consulte el tutorial sobre [configuración del aprovisionamiento automático de SAP SuccessFactors](#).

Compatibilidad con correos electrónicos personalizados en Azure AD B2C (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: B2C: administración de identidades de consumidor

Funcionalidad del producto: B2B/B2C

Ahora puede usar Azure AD B2C para crear correos electrónicos personalizados cuando los usuarios se suscriban para usar las aplicaciones. Mediante el uso de DisplayControls (actualmente en versión preliminar) y un proveedor de correo electrónico de terceros (por ejemplo, [SendGrid](#), [SparkPost](#) o una API REST personalizada), puede usar su propia plantilla de correo electrónico, dirección De y texto del asunto, además de admitir la localización y la configuración personalizada de contraseña de un solo uso (OTP).

Para obtener más información, consulte el artículo sobre [comprobación de correo electrónico personalizada en Azure Active Directory B2C](#).

Sustitución de directivas de base de referencia por valores predeterminados de seguridad

Tipo: Característica modificada

Categoría del servicio: Otros

Funcionalidad del producto: Seguridad y protección de la identidad

Como parte de un modelo predeterminado seguro para la autenticación, vamos a quitar las directivas de protección de base de referencia existentes de todos los inquilinos. Se prevé que esta retirada se complete a finales de febrero. El reemplazo de estas directivas de protección de base de referencia son los valores predeterminados de seguridad. Si ha usado directivas de protección de base de referencia, debe planear la migración a la nueva directiva de valores predeterminados de seguridad o al acceso condicional. Si no ha usado estas directivas, no tiene que realizar ninguna acción.

Para obtener más información sobre los nuevos valores predeterminados de seguridad, consulte [¿Qué son los valores predeterminados de seguridad?](#) Para obtener más información sobre las directivas de acceso condicional, consulte [Directivas de acceso condicional habituales](#).

Noviembre de 2019

Compatibilidad con el atributo SameSite y Chrome 80

Tipo: Plan de cambio

Categoría del servicio: Autenticaciones (inicios de sesión)

Funcionalidad del producto: Autenticación de usuarios

Como parte de un modelo predeterminado y seguro para las cookies, el explorador Chrome 80 cambia el modo en que trata las cookies sin el atributo `SameSite`. Cualquier cookie que no especifique el atributo `SameSite` se tratará como si se hubiera establecido en `SameSite=Lax`, lo que producirá un bloqueo de Chrome en ciertos escenarios de uso compartido de cookies entre dominios de los que puede depender su aplicación. Para mantener el comportamiento de Chrome anterior, puede utilizar el atributo `SameSite=None` y agregar un atributo `Secure` adicional, por lo que solo se puede tener acceso a las cookies entre sitios a través de conexiones HTTPS. Chrome está programado para completar este cambio el 4 de febrero de 2020.

Se recomienda que todos los desarrolladores prueben sus aplicaciones siguiendo esta guía:

- Establecer el valor predeterminado de la opción **Usar cookies seguras** en Sí.
- Establecer el valor predeterminado del atributo **SameSite** en Ninguno.
- Agregar un atributo `SameSite` adicional de Seguro.

Para obtener más información, consulte el artículo sobre [próximos cambios en la cookie de SameSite en ASP.NET y ASP.NET Core y Posible interrupción para los sitios web de los clientes y los servicios de Microsoft en la versión 79 de Chrome Beta y versiones posteriores](#).

Nueva revisión para Microsoft Identity Manager (MIM) 2016 Service Pack 2 (SP2)

Tipo: Corregido

Categoría del servicio: Microsoft Identity Manager

Funcionalidad del producto: Administración del ciclo de vida de la identidad

Un paquete acumulativo de revisiones (compilación 4.6.34.0) está disponible para Microsoft Identity Manager (MIM) 2016 Service Pack 2 (SP2). Este paquete acumulativo resuelve problemas y agrega mejoras que se describen en la sección sobre "problemas corregidos y mejoras agregadas en esta actualización".

Para obtener más información y descargar el paquete de revisiones, consulte el artículo [El paquete acumulativo de actualizaciones de Microsoft Identity Manager 2016 Service Pack 2 \(compilación 4.6.34.0\) está disponible](#).

Nuevo informe de actividad de aplicaciones de AD FS para ayudar a migrar las aplicaciones a Azure AD (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Use el nuevo informe de actividad de aplicaciones de Servicios de federación de Active Directory (AD FS) en Azure Portal para identificar las aplicaciones que se pueden migrar a Azure AD. El informe evalúa todas las aplicaciones de AD FS con respecto a la compatibilidad con Azure AD, comprueba si hay problemas y proporciona instrucciones sobre cómo preparar aplicaciones concretas para su migración.

Para obtener más información, consulte [Uso del informe de actividades de aplicaciones de AD FS para migrar aplicaciones a Azure AD](#).

Nuevo flujo de trabajo para que los usuarios soliciten el consentimiento del administrador (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Control de acceso

El flujo de trabajo de consentimiento del administrador proporciona a los administradores una manera de conceder acceso a las aplicaciones que requieren la aprobación del administrador. Si un usuario intenta acceder a una aplicación, pero no puede dar su consentimiento, puede enviar una solicitud de aprobación del administrador. La solicitud se envía por correo electrónico, y se coloca en una cola a la que se puede acceder desde Azure Portal, a todos los administradores que se han designado como revisores. Una vez que un revisor realiza una acción en una solicitud pendiente, se notifica la acción a los usuarios que realizan la solicitud.

Para obtener más información, consulte [Configuración del flujo de trabajo de consentimiento del administrador \(versión preliminar\)](#).

Nueva experiencia de configuración del token de registros de aplicación de Azure AD para administrar notificaciones opcionales (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Otros

Funcionalidad del producto: Experiencia para el desarrollador

La nueva hoja de configuración del token de registros de aplicación de Azure AD de Azure Portal muestra ahora a los desarrolladores de aplicaciones una lista dinámica de notificaciones opcionales para sus aplicaciones. Esta nueva experiencia ayuda a simplificar las migraciones de aplicaciones de Azure AD y a minimizar las configuraciones incorrectas de las notificaciones opcionales.

Para obtener más información, consulte [Proporcionar notificaciones opcionales a la aplicación de Azure AD](#).

Nuevo flujo de trabajo de aprobación en dos fases de administración de derechos de Azure AD (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Otros

Funcionalidad del producto: Administración de derechos

Hemos presentado un nuevo flujo de trabajo de aprobación en dos fases que le permite exigir dos aprobadores para aprobar la solicitud de un usuario a un paquete de acceso. Por ejemplo, puede establecerlo de manera que el administrador del usuario que realiza la solicitud deba dar su aprobación en primer lugar y, a continuación, también puede exigir que un propietario del recurso dé su aprobación. Si uno de los aprobadores no da su aprobación, no se concede el acceso.

Para obtener más información, consulte [Cambio de la configuración de la solicitud y aprobación para un paquete de acceso de administración de derechos de Azure AD](#).

Actualizaciones de la página Mis aplicaciones con nuevas áreas de trabajo (versión preliminar pública)

Tipo: Nueva característica

Categoría del servicio: Mis aplicaciones

Funcionalidad del producto: Integración de terceros

Ahora puede personalizar la forma en que los usuarios de la organización ven y acceden a la experiencia actualizada de Mis aplicaciones. Esta nueva experiencia también incluye la nueva característica de áreas de trabajo, que facilita a los usuarios la búsqueda y organización de aplicaciones.

Para obtener más información sobre la nueva experiencia de Mis aplicaciones y la creación de áreas de trabajo, consulte el artículo sobre [creación de áreas de trabajo en el portal Mis aplicaciones](#).

Compatibilidad con identificadores sociales de Google para la colaboración B2B de Azure AD (disponibilidad general)

Tipo: Nueva característica

Categoría del servicio: B2B

Funcionalidad del producto: Autenticación de usuarios

La nueva compatibilidad con el uso de identificadores sociales de Google (cuentas Gmail) en Azure AD ayuda a simplificar la colaboración entre sus usuarios y partners. Ya no hay necesidad de que los partners creen y administren una cuenta específica de Microsoft. Microsoft Teams ahora es totalmente compatible con los usuarios de Google en todos los clientes y en los puntos de conexión de autenticación comunes y relacionados con los inquilinos.

Para obtener más información, consulte [Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B](#).

Compatibilidad de Microsoft Edge para dispositivos móviles con el acceso condicional y el inicio de sesión único (disponibilidad general)

Tipo: Nueva característica

Categoría del servicio: Acceso condicional

Funcionalidad del producto: Seguridad y protección de la identidad

Azure AD para Microsoft Edge en iOS y Android ahora admite acceso condicional e inicio de sesión único de Azure AD:

- **Inicio de sesión único (SSO) de Microsoft Edge:** El inicio de sesión único ahora está disponible en los clientes nativos (como Microsoft Outlook y Microsoft Edge) para todas las aplicaciones conectadas a Azure AD.
- **Acceso condicional de Microsoft Edge:** A través de las directivas de acceso condicional basado en aplicaciones, los usuarios deben usar exploradores protegidos por Microsoft Intune, como Microsoft Edge.

Para obtener más información sobre el acceso condicional y el inicio de sesión único con Microsoft Edge, consulte la entrada de blog sobre [compatibilidad de Microsoft Edge para dispositivos móviles con el acceso condicional y el inicio de sesión único ahora disponible con carácter general](#). Para obtener más información sobre cómo configurar las aplicaciones cliente con acceso condicional basado en aplicaciones o acceso condicional basado en dispositivos, consulte [Administración del acceso web mediante un explorador protegido por directivas de Microsoft Intune](#).

Administración de derechos de Azure AD (disponibilidad general)

Tipo: Nueva característica

Categoría del servicio: Otros

Funcionalidad del producto: Administración de derechos

La administración de derechos de Azure AD es una nueva característica de gobernanza de identidades, que ayuda a las organizaciones a administrar el ciclo de vida de identidad y acceso a escala. Esta nueva característica ayuda

mediante la automatización de los flujos de trabajo de solicitud de acceso, las asignaciones de acceso, las revisiones y la expiración entre grupos, aplicaciones y sitios de SharePoint Online.

Con la administración de derechos de Azure AD, puede administrar el acceso de forma más eficaz tanto para los empleados como para los usuarios ajenos a la organización que han de acceder a esos recursos.

Para obtener más información, consulte [¿Qué es la administración de derechos de Azure AD?](#)

Automatización del aprovisionamiento de cuentas de usuario para estas aplicaciones SaaS recién admitidas

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

[SAP Cloud Platform Identity Authentication Service](#), [RingCentral](#), [SpaceIQ](#), [Miro](#), [Cloudgate](#), [Infor CloudSuite](#), [OfficeSpace Software](#), [Priority Matrix](#)

Para más información acerca de cómo proteger mejor una organización mediante el aprovisionamiento automatizado de cuentas de usuario, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: noviembre de 2019

Tipo: Nueva característica

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: Integración de terceros

En noviembre de 2019, hemos agregado estas 21 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Airtable](#), [Hootsuite](#), [Blue Access for Members \(BAM\)](#), [Bitly](#), [Riva](#), [ResLife Portal](#), [NegometrixPortal Single Sign On \(SSO\)](#), [TeamsChamp](#), [Motus](#), [MyAryaka](#), [BlueMail](#), [Beedle](#), [Visma](#), [OneDesk](#), [Foko Retail](#), [Qmarkets Idea & Innovation Management](#), [Netskope User Authentication](#), [uniFLOW Online](#), [Claromentis](#), [Jisc Student Voter Registration](#), [e4enable](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

La nueva y mejorada galería de aplicaciones de Azure AD

Tipo: Característica modificada

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Hemos actualizado la galería de aplicaciones de Azure AD para que le resulte más fácil encontrar aplicaciones integradas previamente que admitan el aprovisionamiento, OpenID Connect y SAML en su inquilino de Azure Active Directory.

Para obtener más información, consulte [Incorporación de una aplicación a un inquilino de Azure Active Directory](#).

Límite de longitud de definición de roles de aplicación aumentado de 120 a 240 caracteres

Tipo: Característica modificada

Categoría del servicio: Aplicaciones empresariales

Funcionalidad del producto: SSO

Hemos escuchado de los clientes que el límite de longitud del valor de definición de rol de aplicación en algunas aplicaciones y servicios es demasiado corto en 120 caracteres. En respuesta, hemos aumentado la longitud máxima de la definición de valor de rol a 240 caracteres.

Para obtener más información sobre el uso de definiciones de roles específicas de la aplicación, consulte [Para ver más ejemplos e información, consulte Procedimiento para agregar roles de aplicación en la aplicación y recibirlas en el token.](#)

Octubre de 2019

Desuso de la API de identityRiskEvent para las detecciones de riesgo de Azure AD Identity Protection

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

En respuesta a los comentarios de los desarrolladores, los suscriptores de Azure AD Premium P2 ahora pueden realizar consultas complejas sobre los datos de detección de riesgos de Azure AD Identity Protection mediante la nueva API de riskDetection para Microsoft Graph. La versión beta existente de la API de [identityRiskEvent](#) dejará de devolver datos en torno al **10 de enero de 2020**. Si su organización usa la API de identityRiskEvent, debe realizar la transición a la nueva API de riskDetection.

Para obtener más información sobre la nueva API de riskDetection, consulte la [documentación de referencia de la API de detección de riesgos](#).

Compatibilidad del proxy de aplicación con el atributo SameSite y Chrome 80

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Un par de semanas antes del lanzamiento del explorador Chrome 80, tenemos previsto actualizar el modo en que las cookies del proxy de aplicación tratan el atributo **SameSite**. Con el lanzamiento de Chrome 80, cualquier cookie que no especifique el atributo **SameSite** se tratará como si se hubiera establecido en `SameSite=Lax`.

Para ayudar a evitar posibles impactos negativos debido a este cambio, vamos a actualizar las cookies de sesión y el acceso del proxy de aplicación de la siguiente manera:

- Estableciendo el valor predeterminado de la opción **Usar cookies seguras** en **Sí**.
- Estableciendo el valor predeterminado del atributo **SameSite** en **Ninguno**.

NOTE

Las cookies de acceso del proxy de aplicación siempre se han transmitido exclusivamente a través de canales seguros. Estos cambios solo se aplican a las cookies de sesión.

Para obtener más información sobre la configuración de las cookies del proxy de aplicación, consulte [Configuración de las cookies para el acceso a aplicaciones locales en Azure Active Directory](#).

La característica Registros de aplicaciones (heredada) y la funcionalidad de administración de aplicaciones en el Portal de registro de aplicaciones (apps.dev.microsoft.com) ya no están disponibles

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** N/D Experiencia para el desarrollador

Los usuarios con cuentas de Azure AD ya no pueden registrar o administrar aplicaciones mediante el Portal de registro de aplicaciones (apps.dev.microsoft.com), ni registrar ni administrar aplicaciones en la experiencia Registros de aplicaciones (característica heredada) de Azure Portal.

Para obtener más información sobre la nueva experiencia Registros de aplicaciones, consulte la sección sobre [Registros de aplicaciones en la guía de aprendizaje de Azure Portal](#).

Ya no es necesario que los usuarios vuelvan a registrarse durante la migración de MFA por usuario a MFA basada en el acceso condicional

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** MFA Seguridad y protección de la identidad

Hemos corregido un problema conocido por el que se requería que los usuarios se volvieran a registrar si estaban deshabilitados para la autenticación multifactor (MFA) por usuario y luego se habilitaban para la MFA a través de una directiva de acceso condicional.

Para requerir que los usuarios vuelvan a registrarse, puede seleccionar la opción **Requerir volver a registrar MFA** en los métodos de autenticación del usuario en el portal de Azure AD. Para obtener más información sobre la migración de usuarios de MFA por usuario a MFA basada en el acceso condicional, consulte [Conversión de los usuarios de MFA por usuario a MFA basado en acceso condicional](#).

Nuevas funcionalidades para transformar y enviar notificaciones en el token SAML

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Hemos agregado funcionalidades adicionales que lo ayudarán a personalizar y enviar notificaciones en el token SAML. Estas son algunas de ellas:

- Funciones de transformación de notificaciones adicionales, lo que lo ayudará a modificar el valor que envía en la notificación.
- Capacidad de aplicar varias transformaciones a una única notificación.
- Capacidad de especificar el origen de la notificación, en función del tipo de usuario y el grupo al que pertenece el usuario.

Para obtener información detallada sobre estas nuevas funcionalidades, incluido cómo usarlas, consulte [Personalización de las notificaciones emitidas en el token SAML para aplicaciones empresariales](#).

Nueva página Mis inicios de sesión para los usuarios finales en Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Supervisión e informes

Hemos agregado una nueva página **Mis inicios de sesión** (<https://mysignins.microsoft.com>) para que los usuarios de la organización puedan ver su historial de inicio de sesión reciente con el fin de comprobar si hay alguna actividad inusual. Esta nueva página permite a los usuarios comprobar lo siguiente:

- Si alguien intenta adivinar la contraseña.
- Si un atacante inició sesión correctamente en su cuenta y desde qué ubicación.
- Las aplicaciones a las que el atacante ha intentado acceder.

Para obtener más información, consulte la entrada de blog sobre cómo [los usuarios pueden comprobar ahora su historial de inicio de sesión para actividades inusuales](#).

Migración de Azure AD Domain Services (Azure AD DS) de las redes virtuales clásicas a las de Azure Resource Manager

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Domain Services Azure AD Domain Services

Tenemos excelentes noticias para los clientes que siguen usando las redes virtuales clásicas. Ahora puede realizar una migración puntual desde una red virtual clásica a una de Resource Manager. Después de migrar a la red virtual de Resource Manager, podrá aprovechar las ventajas de las características adicionales y actualizadas, como las directivas de contraseñas específicas, las notificaciones por correo electrónico y los registros de auditoría.

Para obtener más información, consulte [Versión preliminar: Migración de Azure AD Domain Services desde el modelo de red virtual clásica a Resource Manager](#).

Actualizaciones del diseño del contrato de página de Azure AD B2C

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Hemos introducido algunos cambios nuevos en la versión 1.2.0 del contrato de página de Azure AD B2C. En esta versión actualizada, ahora puede controlar el orden de carga de los elementos, lo que también puede ayudar a detener el parpadeo que se produce cuando se carga la hoja de estilos (CSS).

Para ver una lista completa de los cambios realizados en el contrato de página, vea el [registro de cambios de versión](#).

Actualización de la página Mis aplicaciones con nuevas áreas de trabajo (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones Control de acceso

Ahora puede personalizar la forma en que los usuarios de su organización ven y acceden a la nueva experiencia de Mis aplicaciones, incluido el uso de la nueva característica de áreas de trabajo para que sea más fácil buscar aplicaciones. La nueva funcionalidad de áreas de trabajo actúa como un filtro para las aplicaciones a las que los usuarios de su organización ya tienen acceso.

Para obtener más información sobre cómo implementar la nueva experiencia de Mis aplicaciones y crear áreas de trabajo, consulte el artículo sobre [creación de áreas de trabajo en el portal Mis aplicaciones \(versión preliminar\)](#).

Compatibilidad con el modelo de facturación basado en usuarios activos mensuales (disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Azure AD B2C admite ahora la facturación de usuarios activos mensuales (MAU). La facturación de MAU se basa en el número de usuarios únicos con actividad de autenticación durante un mes natural. Los clientes existentes pueden pasarse a este nuevo método de facturación en cualquier momento.

A partir del 1 de noviembre de 2019, a todos los clientes nuevos se les facturará automáticamente con este método. Este método de facturación beneficia a los clientes gracias a las ventajas que ofrece en cuanto a costos y a la posibilidad de planear con anterioridad.

Para obtener más información, consulte [Actualización al modelo de facturación de usuarios activos mensuales](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: octubre de 2019

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En octubre de 2019, hemos agregado estas 35 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[In Case of Crisis – Mobile](#), [Juno Journey](#), [ExponentHR](#), [Tact](#), [OpusCapita Cash Management](#), [Salestim](#), [Learnster](#), [Dynatrace](#), [HunchBuzz](#), [Freshworks](#), [eCornell](#), [ShipHazmat](#), [Netskope Cloud Security](#), [Contentful](#), [Bindtuning](#), [HireVue Coordinate – Europe](#), [HireVue Coordinate - USOnly](#), [HireVue Coordinate - US](#), [WittyParrot Knowledge Box](#),

Cloudmore, Visit.org, Cambium Xirrus EasyPass Portal, Paylocity, Mail Luck!, Teamie, Velocity for Teams, SIGNL4, EAB Navigate IMPL, ScreenMeet, Omega Point, Speaking Email for Intune (iPhone), Speaking Email for Office 365 Direct (iPhone/Android), ExactCare SSO, iHealthHome Care Navigation System, Qubie

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Elemento de menú consolidado Seguridad en el portal de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

Ahora puede acceder a todas las características de seguridad de Azure AD disponibles en el nuevo elemento de menú **Seguridad** y en la barra **Buscar** de Azure Portal. Además, la nueva página de aterrizaje **Seguridad** denominada **Seguridad - Introducción** proporcionará vínculos a nuestra documentación pública, así como guías de seguridad y de implementación.

El nuevo menú **Seguridad** incluye lo siguiente:

- Acceso condicional
- Protección de identidad
- Security Center
- Puntuación segura de identidad
- Métodos de autenticación
- MFA
- Informes de riesgo: usuarios de riesgo, inicios de sesión peligrosos, detecciones de riesgo, etc.
- Y mucho más.

Para obtener más información, visite [Seguridad - Introducción](#).

Directiva de expiración de grupos de Office 365 mejorada con renovación automática

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración de grupos Administración del ciclo de vida de la identidad

La directiva de expiración de grupos de Office 365 se ha mejorado para renovar automáticamente los grupos que los miembros estén usando activamente. Los grupos se renuevan en función de la actividad del usuario en todas las aplicaciones de Office 365, como Outlook, SharePoint y Teams.

Esta mejora ayuda a reducir las notificaciones de expiración de los grupos, así como a garantizar que los grupos activos sigan estando disponibles. Si ya tiene una directiva de expiración activa para grupos de Office 365, no es necesario hacer nada para activar esta nueva funcionalidad.

Para obtener más información, vea [Configuración de la directiva de expiración de grupos de Office 365](#).

Experiencia de creación de Azure AD Domain Services (Azure AD DS) actualizada

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Azure AD Domain Services Azure AD Domain Services

Hemos actualizado Azure AD Domain Services (Azure AD DS) para incluir una experiencia de creación nueva y mejorada, que lo ayudará a crear un dominio administrado en tan solo tres clics. Además, ahora puede cargar e implementar instancias de Azure AD DS desde una plantilla.

Para más información, consulte el [Tutorial: Creación y configuración de una instancia de Azure Active Directory Domain Services](#).

Septiembre de 2019

Planeado su cambio: Desuso de los paquetes de contenido de Power BI

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Informes Supervisión e informes

A partir del 1 de octubre de 2019, Power BI comenzará a dejar de usar todos los paquetes de contenido, incluido el paquete de contenido de Azure AD Power BI. Como alternativa a este paquete de contenido, puede usar libros de Azure AD para obtener información sobre los servicios relacionados con Azure AD. Próximos libros de trabajo adicionales, incluidos los libros sobre las directivas de acceso condicional en modo de solo informes, información basada en el consentimiento de la aplicación, etc.

Para obtener más información acerca de los libros, consulte [Cómo usar los libros de Azure Monitor en informes de Azure Active Directory](#). Para obtener más información sobre el desuso de los paquetes de contenido, consulte la publicación de blog [Anuncio de disponibilidad general de aplicaciones de plantilla de Power BI](#).

Mi perfil cambia de nombre y se integra con la página de la cuenta de Microsoft Office

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Mi perfil/cuenta Colaboración

A partir de octubre, la experiencia Mi perfil se convertirá en Mi cuenta. Como parte de ese cambio, en todas partes en las que aparezca **Mi perfil**, este pasará a llamarse **Mi cuenta**. Además del cambio de nomenclatura y algunas mejoras de diseño, la experiencia actualizada ofrecerá una integración adicional con la página de la cuenta de Microsoft Office. En concreto, podrá obtener acceso a las instalaciones y suscripciones de Office desde la página **Overview Account** (Descripción general de la cuenta), junto con las preferencias de contacto relacionadas con Office desde la página **Privacy** (Privacidad).

Para obtener más información sobre la experiencia Mi perfil (versión preliminar), consulte la [descripción general del portal Mi perfil \(versión preliminar\)](#).

Administración masiva de grupos y miembros mediante archivos CSV en el portal de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Nos complace anunciar la disponibilidad de la versión preliminar pública de las experiencias de administración masiva de grupos en el portal de Azure AD. Ahora puede usar un archivo CSV y el portal de Azure AD para administrar grupos y listas de miembros, entre los que se incluyen:

- Incorporación o eliminación de miembros de un grupo.
- Descarga de la lista de grupos del directorio.
- Descarga de la lista de miembros del grupo para un grupo específico.

Para obtener más información, consulte [Aregar miembros de forma masiva](#), [Eliminar miembros de forma masiva](#), [Descarga masiva de los miembros de la lista](#) y [Descarga masiva de los grupos de la lista](#).

Además se admite el consentimiento dinámico a través de un nuevo punto de conexión de consentimiento del administrador.

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Hemos creado un nuevo punto de conexión de consentimiento del administrador para admitir la opción de consentimiento dinámico, lo que le resultará útil para las aplicaciones que vayan a usar el modelo de consentimiento dinámico en la plataforma de Microsoft Identity.

Para obtener más información sobre cómo usar este nuevo punto de conexión, consulte [Usar el punto de conexión](#)

del consentimiento de administrador.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: septiembre de 2019

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En septiembre de 2019, hemos agregado estas 29 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

ScheduleLook, MS Azure SSO Access for Ethidex Compliance Office™ - Single sign-on, iServer Portal, SKYSITE, Concur Travel and Expense, WorkBoard, <https://apps.yeeflow.com/>, ARC Facilities, Luware Stratus Team, Wide Ideas, Prisma Cloud, JDLT Client Hub, RENRAKU, SealPath Secure Browser, Prisma Cloud, <https://app.penneo.com/>, <https://app.testhtm.com/settings/email-integration>, Cintoo Cloud, Whitesource, Hosted Heritage Online SSO, IDC, CakeHR, BIS, Coo Kai Team Build, Sonarqube, Adobe Identity Management, Discovery Benefits SSO, Amelio, <https://itask.yipinapp.com/>

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevo rol de lector global de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** RBAC Control de acceso

A partir del 24 de septiembre de 2019, empezaremos a implementar un nuevo rol de Azure Active Directory (AD) denominado Lector global. Este lanzamiento comenzará con los clientes de producción y de la nube global (GCC), y finalizará en octubre a nivel global.

El rol del Lector global es la contrapartida de la opción de solo lectura del administrador global. Los usuarios de este rol pueden leer la configuración y la información administrativa en los servicios de Microsoft 365, pero no pueden llevar a cabo acciones de administración. Por ello, hemos creado el rol del Lector global para que pueda reducir la cantidad de administradores globales en su organización. Debido a que las cuentas de administrador global son a la vez eficaces y vulnerables a los ataques, le recomendamos que tenga menos de cinco administradores globales. Igualmente, le recomendamos usar el rol de Lector global para la planificación, las auditorías o las investigaciones. También le recomendamos usar el rol de Lector global en combinación con otros roles de administrador limitados, como el de administrador de Exchange, para que pueda realizar el trabajo necesario sin tener que usar el rol de administrador global.

El rol del Lector global funciona con el nuevo Centro de administración de Microsoft 365, el Centro de administración de Exchange, el Centro de administración de Teams, el Centro de seguridad, el Centro de cumplimiento, el Centro de administración de Azure AD y el Centro de administración de la administración de dispositivos.

NOTE

Al comienzo de la versión preliminar pública, el rol de Lector global no funcionará con: SharePoint, Privileged Access Management, Caja de seguridad del cliente, etiquetas de confidencialidad, Ciclo de vida de Teams, Creación de informes y análisis de llamadas de Teams, Administración de dispositivos de teléfono IP de Teams y Catálogo de aplicaciones de Teams.

Para obtener más información, consulte los [permisos del rol de administrador en Azure Active Directory](#).

Acceder a un servidor de informes local desde la aplicación Power BI Mobile con Azure Active Directory Application Proxy

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

La nueva integración entre la aplicación Power BI Mobile y Azure AD Application Proxy le permite iniciar sesión de forma segura en la aplicación Power BI Mobile y ver cualquiera de los informes de la organización hospedados en la instancia local de Power BI Report Server.

Para obtener más información acerca de la aplicación de Power BI Mobile, incluyendo el lugar desde dónde descargar la aplicación, consulte el [sitio de Power BI](#). Para obtener más información sobre cómo configurar la aplicación de Power BI Mobile con Azure AD Application Proxy, consulte [Habilitar el acceso remoto a Power BI Mobile con Azure AD Application Proxy](#).

Hay una nueva versión del módulo de PowerShell de AzureADPreview disponible

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Directorio

Se agregaron nuevos cmdlets al módulo AzureADPreview, para ayudar a definir y asignar roles personalizados en Azure AD, que incluyen:

- `Add-AzureADMSFeatureRolloutPolicyDirectoryObject`
 - `Get-AzureADMSFeatureRolloutPolicy`
 - `New-AzureADMSFeatureRolloutPolicy`
 - `Remove-AzureADMSFeatureRolloutPolicy`
 - `Remove-AzureADMSFeatureRolloutPolicyDirectoryObject`
 - `Set-AzureADMSFeatureRolloutPolicy`
-

Nueva versión de Azure AD Connect

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Directorio

Hemos publicado una versión actualizada de Azure AD Connect para clientes que usen la actualización automática. Esta nueva versión incluye varias características nuevas, mejoras y correcciones de errores. Para obtener más información sobre esta versión nueva, consulte [Azure AD Connect: historial de versiones](#).

Ya está disponible la versión 8.0.2 del servidor de Multi-Factor Authentication de Azure (MFA)

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** MFA Seguridad y protección de la identidad

Si es un cliente ya existente que activó el servidor MFA antes del 1 de julio de 2019, ya puede descargar la versión más reciente del servidor MFA (versión 8.0.2). En esta nueva versión, hemos realizado lo siguiente:

- Se corrigió un problema por el que, cuando Azure AD Sync cambia el estado de un usuario de "deshabilitado" a "habilitado", se envía un correo electrónico al mismo.
- Se corrigió un problema para que los clientes puedan realizar sus actualizaciones correctamente, al tiempo que se sigue usando la funcionalidad de etiquetas.
- Se agregó el código de país de Kosovo (+ 383).
- Se agregó un registro de auditoría de omisión por única vez a MultiFactorAuthSvc.log.
- Se mejoró el rendimiento del SDK del servicio web.
- Se corrigieron otros errores menores.

A partir del 1 de julio de 2019, Microsoft dejó de ofrecer el servidor de MFA en las nuevas implementaciones. Los clientes nuevos que quieran exigir la autenticación multifactor a sus usuarios deberán usar Azure Multi-Factor Authentication basado en la nube. Para obtener más información, consulte [Planificación de una implementación de Azure Multi-Factor Authentication basada en la nube](#).

Agosto de 2019

Funciones de búsqueda, filtrado y ordenación mejorados para los grupos están disponibles en el portal de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Nos complace anunciar la disponibilidad de la versión preliminar pública de las experiencias mejoradas relacionadas con grupos en el portal de Azure AD. Estas mejoras ayudan a administrar mejor los grupos y las listas de miembros, ya que proporcionan:

- Funcionalidades de búsqueda avanzada, como la búsqueda de subcadenas en listas de grupos.
- Opciones avanzadas de filtrado y ordenación en las listas de miembros y propietarios.
- Nuevas funcionalidades de búsqueda para listas de miembros y propietarios.
- Recuentos de grupos más precisos para grupos grandes.

Para obtener más información, consulte [Administración de grupos en Azure Portal](#).

Nuevos roles personalizados están disponibles para la administración de registro de aplicaciones (Versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** RBAC Control de acceso

Los roles personalizados (disponibles con una suscripción Azure AD P1 o P2) ahora pueden ayudarle a proporcionar acceso específico, permitiéndole crear definiciones de roles con permisos específicos y, a continuación, asignar esos roles a recursos específicos. Actualmente, se crean roles personalizados mediante el uso de permisos para administrar los registros de aplicaciones y, a continuación, se asigna el rol a una aplicación específica. Para obtener más información sobre los roles personalizados, consulte [Roles de administrador personalizados en Azure Active Directory \(versión preliminar\)](#).

Si necesita más permisos o recursos admitidos que no vea actualmente, puede enviar comentarios a nuestro [sitio de comentarios de Azure](#) e incorporaremos su solicitud a nuestra guía de ruta de actualización.

Los nuevos registros de aprovisionamiento pueden ayudarle a supervisar y solucionar problemas de la implementación de aprovisionamiento de aplicaciones (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Administración del ciclo de vida de la identidad

Nuevos registros de aprovisionamiento disponibles para ayudarle a supervisar y solucionar problemas de la implementación de aprovisionamiento de usuarios y grupos. Estos nuevos archivos de registro incluyen información sobre:

- Qué grupos se han creado correctamente en ServiceNow
- Cómo se han importado los roles de [Amazon Web Services\(AWS\)](#)
- Qué empleados no se importaron desde [WorkDay](#)

Para obtener más información, consulte [Informes de aprovisionamiento en el portal de Azure Active Directory \(versión preliminar\)](#).

Nuevos informes de seguridad para todos los administradores de Azure AD (Disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

De forma predeterminada, todos los administradores de Azure AD podrán acceder pronto a informes de seguridad modernos dentro de Azure AD. Hasta el final de septiembre, podrá usar el banner de la parte superior de los informes de seguridad modernos para volver a los informes antiguos.

Los informes de seguridad modernos proporcionarán funciones adicionales de las versiones anteriores, entre las que se incluyen:

- Filtrado y ordenación avanzados
- Acciones en masa, como descartar el riesgo del usuario
- Confirmación de entidades en peligro o seguras
- Estado de riesgo, que abarca: En riesgo, Descartado, Corregido y Confirmado (en peligro)
- Nuevas detecciones relacionadas con riesgos (disponibles para suscriptores de Azure AD Premium)

Para obtener más información, consulte [Usuarios riesgosos](#), [Inicios de sesión riesgosos](#) y [Detecciones de riesgos](#).

La identidad administrada asignada por el usuario está disponible para máquinas virtuales y conjuntos de escalado de máquinas virtuales (Disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identidades administradas para recursos de Azure Experiencia para el desarrollador

Las identidades administradas asignadas por el usuario ahora están generalmente disponibles para máquinas virtuales y conjuntos de escalado de máquinas virtuales. Como parte de esto, Azure puede crear una identidad en el inquilino de Azure AD que sea de confianza para la suscripción en uso y se puede asignar a una o varias instancias de servicio de Azure. Para obtener más información sobre las identidades administradas asignadas por el usuario, consulte [¿Qué son las identidades administradas para los recursos de Azure?](#).

Los usuarios pueden restablecer sus contraseñas mediante una aplicación móvil o un token de hardware (Disponibilidad general)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Autenticación de usuarios

Los usuarios que han registrado una aplicación móvil en su organización ahora pueden restablecer su propia contraseña mediante la aprobación de una notificación de la aplicación de Microsoft Authenticator o mediante la introducción de un código de su aplicación móvil o token de hardware.

Para obtener más información, [Consulte cómo funciona: Autoservicio de restablecimiento de contraseña de Azure AD](#). Para obtener más información sobre la experiencia del usuario, consulte [Información general sobre cómo restablecer su propia contraseña profesional o educativa](#).

ADAL.NET ignora la memoria caché compartida de MSAL.NET para escenarios en representación

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

A partir de la versión 5.0.0-preview de la biblioteca de autenticación de Azure AD (ADAL.NET), los desarrolladores de aplicaciones deben [serializar una caché por cuenta para las aplicaciones web y API web](#). En caso contrario, algunos escenarios que usan el [flujo en representación de](#), junto con algunos casos de uso específicos de [UserAssertion](#), pueden dar como resultado una elevación de privilegios. Para evitar esta vulnerabilidad, ADAL.NET ignora ahora la caché compartida de la biblioteca de autenticación de Microsoft para dotnet (MSAL.NET) para escenarios en representación.

Para más información acerca de este problema, consulte [Vulnerabilidad de elevación de privilegios de la Biblioteca de autenticación de Active Directory](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: agosto de 2019

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En agosto de 2019, hemos agregado estas 26 nuevas aplicaciones con compatibilidad con la federación para la galería de aplicaciones:

Civic Platform, Amazon Business, ProNovos Ops Manager, Cognidox, Viareport's Inativ Portal (Europe), Azure Databricks, Robin, Academy Attendance, Priority Matrix, Cousto MySpace, Uploadcare, Carbonite Endpoint Backup, CPQSync by Cincom, Chargebee, deliver.media™ Portal, Frontline Education, F5, stashcat AD connect, Blink, Vocoli, ProNovos Analytics, Sigstr, Darwinbox, Watch by Colors, Harness, EAB Navigate Strategic Care

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Están disponibles nuevas versiones de los módulos AzureAD PowerShell y AzureADPreview PowerShell.

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Directorio

Están disponibles nuevas versiones de los módulos AzureAD PowerShell y AzureADPreview PowerShell.

- Se agregó un nuevo parámetro `-Filter` al parámetro `Get-AzureADDirectoryRole` en el módulo AzureAD. Este parámetro le ayuda a filtrar por los roles de directorio devueltos por el cmdlet.
- Se agregaron nuevos cmdlets al módulo AzureADPreview, para ayudar a definir y asignar roles personalizados en Azure AD, que incluyen:
 - `Get-AzureADMSRoleAssignment`
 - `Get-AzureADMSRoleDefinition`
 - `New-AzureADMSRoleAssignment`
 - `New-AzureADMSRoleDefinition`
 - `Remove-AzureADMSRoleAssignment`
 - `Remove-AzureADMSRoleDefinition`
 - `Set-AzureADMSRoleDefinition`

Mejoras en la interfaz de usuario del generador de reglas de grupos dinámicos en Azure Portal

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración de grupos Colaboración

Hemos realizado algunas mejoras de la interfaz de usuario en el generador de reglas de grupo dinámico, disponible en el Azure Portal, para ayudarle a configurar más fácilmente una nueva regla o cambiar las reglas existentes. Esta mejora del diseño le permite crear reglas con hasta cinco expresiones, en lugar de solo una. También hemos actualizado la lista de propiedades del dispositivo para quitar las propiedades del dispositivo en desuso.

Para obtener más información, consulte [Administrar reglas de pertenencia dinámica](#).

Nuevo permiso de aplicación Microsoft Graph disponible para su uso con las revisiones de acceso

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Revisiones de acceso Identity Governance

Hemos introducido un nuevo permiso de aplicación Microsoft Graph, `AccessReview.ReadWrite.Membership`, que permite a las aplicaciones crear y recuperar automáticamente revisiones de acceso para pertenencias a grupos y asignaciones de aplicaciones. Este permiso se puede usar en los trabajos programados o como parte de la automatización, sin necesidad de un contexto de usuario que haya iniciado sesión.

Para obtener más información, consulte el [Ejemplo de cómo crear revisiones de acceso de Azure AD mediante los permisos de la aplicación Microsoft Graph con el blog de PowerShell](#).

Los registros de actividad de Azure AD ahora están disponibles para las instancias de la nube de administración pública en Azure Monitor

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Nos complace anunciar que los registros de actividad de Azure AD ahora están disponibles para las instancias de la nube de administración pública en Azure Monitor. Ahora puede enviar registros de Azure AD a su cuenta de almacenamiento o a un centro de eventos para integrarlos con las herramientas SIEM, como [Sumologic](#), [Splunk](#) y [Arcsight](#).

Para obtener más información sobre la configuración de Azure Monitor, consulte [Registros de actividad de Azure AD en Azure Monitor](#).

Actualice a sus usuarios a la nueva experiencia de información de seguridad mejorada

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

El 25 de septiembre de 2019, desactivaremos la antigua experiencia de información de seguridad no mejorada para registrar y administrar la información de seguridad del usuario y solo activaremos la nueva [versión mejorada](#). Esto significa que los usuarios ya no podrán usar la experiencia antigua.

Para más información sobre la experiencia de información de seguridad mejorada, consulte nuestra [documentación de administración](#) y nuestra [documentación de usuario](#).

Para activar esta nueva experiencia, debe:

1. Inicie sesión en Azure Portal como administrador global o administrador de usuarios.
2. Vaya a **Azure Active Directory > Configuración de usuario > Administrar la configuración de las características en versión preliminar del panel de acceso**.
3. En el área **Mejoras para los usuarios a la hora de utilizar las características en versión preliminar para registrar y administrar la información de seguridad**, seleccione **Seleccionado** y luego elija un grupo de usuarios o elija **Todos** a fin de activar esta función para todos los usuarios del inquilino.
4. En el **Los usuarios pueden usar las características de vista previa para registrar y administrar el área de información de seguridad**, seleccione **Ninguno**.
5. Guarde la configuración.

Después de guardar la configuración, ya no tendrá acceso a la antigua experiencia de información de seguridad.

IMPORTANT

Si no completa estos pasos antes del 25 de septiembre de 2019, el inquilino de Azure Active Directory se habilitará automáticamente para mejorar la experiencia. Si le queda alguna duda, póngase en contacto con nosotros registrationpreview@microsoft.com.

Las solicitudes de autenticación que utilizan inicios de sesión POST serán validadas de forma más rigurosa

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Estándares

A partir del 2 de septiembre de 2019, las solicitudes de autenticación que usan el método POST se validarán de forma más rigurosa con los estándares HTTP. Concretamente, los espacios y las comillas dobles ("") ya no se

quitarán de los valores del formulario de solicitud. No se espera que estos cambios interrumpan ningún cliente existente y ayudarán a garantizar que las solicitudes enviadas a Azure AD se controlan de forma confiable en todo momento.

Para obtener más información, consulte [Notificaciones de cambios de última hora de Azure AD](#).

Julio de 2019

Planeado su cambio: actualización del servicio Proxy de la aplicación para que admita solo TLS 1.2

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Como ayuda para que le proporcionemos nuestro cifrado más seguro, vamos a empezar a limitar el acceso del servicio Proxy de la aplicación para solo a los protocolos TLS 1.2. Esta limitación se distribuirá inicialmente a los clientes que ya usen protocolos TLS 1,2, por lo que no verá el impacto. Los protocolos TLS 1.0 y TLS 1.1 quedarán totalmente en desuso el 31 de agosto de 2019. Los clientes que aún usen TLS 1.0 y TLS 1.1 recibirán un aviso con tiempo suficiente para prepararse para este cambio.

Para mantener la conexión con el servicio Proxy de la aplicación durante todo este cambio, es aconsejable asegurarse de que las combinaciones de cliente-servidor y explorador web-servidor se actualizan para que usen TLS 1.2. También es aconsejable asegurarse de incluir los sistemas cliente que usan los empleados para acceder a las aplicaciones publicadas mediante el servicio Proxy de la aplicación.

Para obtener más información, vea [Adición de una aplicación local para el acceso remoto mediante el proxy de aplicación en Azure Active Directory](#).

Planeado su cambio: hay actualizaciones de diseño disponibles para la Galería de aplicaciones

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Aplicaciones empresariales SSO

Se van a realizar nuevos cambios en la interfaz de usuario en el diseño del área **Agregar desde la galería** de la hoja **Agregar una aplicación**. Estos cambios le ayudarán a encontrar más fácilmente las aplicaciones que admiten el aprovisionamiento automático, OpenID Connect, Lenguaje de marcado de aserción de seguridad (SAML) y el inicio de sesión único (SSO) con contraseña.

Planeado su cambio: Eliminación de la dirección IP del servidor MFA de la dirección IP de Office 365

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** MFA Seguridad y protección de la identidad

Vamos a quitar la dirección IP del servidor MFA del [servicio web de URL y dirección IP de Office 365](#). Si actualmente utiliza estas páginas para actualizar la configuración del firewall, debe asegurarse de incluir también la lista de direcciones IP documentadas en la sección **requisitos del firewall del servidor Azure Multi-Factor Authentication** del artículo [Introducción a Servidor Azure Multi-Factor Authentication](#).

Los tokens que solo sean de aplicación ahora requieren que la aplicación cliente exista en el inquilino de recursos

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

El 26 de julio de 2019 cambiamos la forma en que proporcionamos tokens solo de aplicaciones a través [de la concesión de credenciales de cliente](#). Anteriormente, las aplicaciones podían obtener tokens para llamar a otras aplicaciones, independientemente de si la aplicación cliente se encontraba en el inquilino. Hemos actualizado este comportamiento para que a los recursos de inquilino único, a veces denominados API Web, solo puedan llamarlos las aplicaciones cliente que existen en el inquilino de recursos.

Si la aplicación no se encuentra en el inquilino de recursos, recibirá el siguiente mensaje de error:

The service principal named <app_name> was not found in the tenant named <tenant_name>. This can happen if the application has not been installed by the administrator of the tenant.

Para solucionar este problema, debe crear la entidad de servicio de la aplicación cliente en el inquilino, para lo que debe usar el [punto de conexión de consentimiento del administrador](#) o [mediante PowerShell](#), lo que garantiza que el inquilino ha dado a la aplicación permiso para operar dentro del inquilino.

Para más información, consulte [Novedades en la autenticación](#).

NOTE

El consentimiento existente entre el cliente y la API sigue sin ser necesario. Las aplicaciones aún deben realizar sus propias comprobaciones para saber si tienen autorización.

Nuevo inicio de sesión sin contraseña para Azure AD mediante claves de seguridad FIDO2

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Los clientes de Azure AD ahora pueden establecer directivas para administrar las claves de seguridad FIDO2 para los usuarios y grupos de su organización. Los usuarios finales también pueden registrar automáticamente sus claves de seguridad, usar las claves para iniciar sesión con sus cuentas Microsoft en sitios web mientras estén en dispositivos compatibles con FIDO, así como iniciar sesión en sus dispositivos de Windows 10 unidos a Azure AD.

Para más información, consulte [Habilitación del inicio de sesión sin contraseña para Azure AD \(versión preliminar\)](#) para obtener información relacionada con el administrador y [Configuración de la información de seguridad para usar una clave de seguridad \(versión preliminar\)](#) para la información relacionada con el usuario final.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (julio de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En julio de 2019, hemos agregado estas 18 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Ungerboeck Software](#), [Bright Pattern Omnichannel Contact Center](#), [Clever Nelly](#), [AcquireIO](#), [Loop](#), [productboard](#), [MS Azure SSO Access for Ethidex Compliance Office™](#), [Hype](#), [Abstract](#), [Ascentis](#), [Flipsnack](#), [Wandera](#), [TwineSocial](#), [Kallidus](#), [HyperAnna](#), [PharmID WasteWitness](#), [i2B Connect](#), [JFrog Artifactory](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Automatización del aprovisionamiento de cuentas de usuario para estas aplicaciones SaaS recién admitidas

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Supervisión e informes

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [Dialpad](#)
- [Federated Directory](#)
- [Figma](#)
- [Leapsome](#)

- [Peakon](#)
- [Smartsheet](#)

Para obtener más información sobre cómo proteger mejor la organización mediante el aprovisionamiento de cuentas de usuario de forma automatizada, vea [Automatización del aprovisionamiento de usuarios para aplicaciones SaaS con Azure AD](#).

Nueva etiqueta de servicio de Azure AD Domain Services para el grupo de seguridad de red

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Domain Services
Azure AD Domain Services

Si está cansado de administrar largas listas de rangos y direcciones IP, puede usar la nueva etiqueta de servicio de red **AzureActiveDirectoryDomainServices** en el grupo de seguridad de red de Azure para ayudar a proteger el tráfico que entra en la subred de la red virtual de Azure AD Domain Services.

Para más información acerca de esta nueva etiqueta de servicio, consulte [Grupos de seguridad de red para Azure AD Domain Services](#).

Nuevas auditorías de seguridad para Azure AD Domain Services (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Domain Services
Azure AD Domain Services

Nos complace anunciar el lanzamiento de la auditoría de seguridad de Azure AD Domain Services en versión preliminar pública. La auditoría de seguridad le ayuda a proporcionar información crítica acerca de los servicios de autenticación mediante la transmisión en secuencias de eventos de auditoría de seguridad a recursos de destino, entre los que se incluyen Azure Storage, áreas de trabajo de Azure Log Analytics y Azure Event Hubs, mediante el portal de Azure AD Domain Services.

Para más información, consulte [Habilitación de auditorías de seguridad para Azure AD Domain Services \(versión preliminar\)](#).

Conclusiones y uso de los nuevos métodos de autenticación (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Supervisión e informes

Los informes de las conclusiones y uso de los nuevos métodos de autenticación pueden ayudarle a entender cómo se registran y usan características como Azure Multi-Factor Authentication y el restablecimiento de contraseña de autoservicio en su organización, lo que incluye el número de usuarios registrados para cada característica, la frecuencia con que se usa el restablecimiento de contraseña de autoservicio para restablecer contraseñas y el método de restablecimiento.

Para más información, consulte [Conclusiones y uso de los métodos de autenticación \(versión preliminar\)](#).

Hay nuevos informes de seguridad disponibles para todos los administradores de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

Ahora, todos los administradores de Azure ad pueden seleccionar el banner de la parte superior de los informes de seguridad existentes, como el informe **Usuarios marcados en riesgo**, para empezar a usar la nueva experiencia de seguridad, como se muestra en los informes **Usuarios de riesgo e Inicios de sesión de riesgo**. Con el tiempo, todos los informes de seguridad pasarán de las versiones anteriores a las nuevas y los informes nuevos le proporcionarán las siguientes funcionalidades adicionales:

- Filtrado y ordenación avanzados
- Acciones en masa, como descartar el riesgo del usuario
- Confirmación de entidades en peligro o seguras
- Estado de riesgo, que abarca: En riesgo, Descartado, Corregido y Confirmado (en peligro)

Para más información, consulte [Informe de usuarios de riesgo](#) e [Informe de inicios de sesión peligrosos](#).

Nuevas auditorías de seguridad para Azure AD Domain Services (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Domain Services
Azure AD Domain Services

Nos complace anunciar el lanzamiento de la auditoría de seguridad de Azure AD Domain Services en versión preliminar pública. La auditoría de seguridad le ayuda a proporcionar información crítica acerca de los servicios de autenticación mediante la transmisión en secuencias de eventos de auditoría de seguridad a recursos de destino, entre los que se incluyen Azure Storage, áreas de trabajo de Azure Log Analytics y Azure Event Hubs, mediante el portal de Azure AD Domain Services.

Para más información, consulte [Habilitación de auditorías de seguridad para Azure AD Domain Services \(versión preliminar\)](#).

Nueva federación directa B2B mediante SAML/WS-FED (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

La federación directa facilita el trabajo con aquellos con asociados cuya solución de identidad administrada de tecnologías de la información no es Azure AD, ya que se trabaja con sistemas de identidad que admiten los estándares SAML o WS-Fed. Después de configurar una relación de federación directa con un asociado, todos los usuarios a los que invite desde dicho dominio pueden colaborar con usted mediante su cuenta de organización existente, lo que hace que la experiencia de sus invitados sea más fluida.

Para más información, consulte [Federación directa con AD FS y proveedores de terceros para usuarios invitados \(versión preliminar\)](#).

Automatización del aprovisionamiento de cuentas de usuario para estas aplicaciones SaaS recién admitidas

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Supervisión e informes

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [Dialpad](#)
- [Federated Directory](#)
- [Figma](#)
- [Leapsome](#)
- [Peakon](#)
- [Smartsheet](#)

Para más información acerca de cómo proteger mejor una organización mediante el aprovisionamiento automatizado de cuentas de usuario, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

Nueva comprobación de nombres de grupos duplicados en el portal de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Ahora, al crear o actualizar un nombre de grupo desde el portal de Azure AD, realizaremos una comprobación para ver si está duplicando un nombre de grupo existente en el recurso. Si determinamos que el nombre ya lo está usando otro grupo, se le pedirá que lo modifique.

Para más información, consulte [Administración de grupos en el portal de Azure AD](#).

Azure AD ahora admite parámetros de consulta estáticos en las direcciones URI de respuesta (redireccionamiento)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Las aplicaciones de Azure AD ahora pueden registrar y usar identificadores URI (redireccionamiento) con parámetros de consulta estáticos (por ejemplo, `https://contoso.com/oauth2?idp=microsoft`) para las solicitudes de OAuth 2.0. El parámetro de consulta estático está sujeto a la coincidencia de cadenas en los identificadores URI de respuesta, al igual que las restantes partes del identificador URI. Si no hay ninguna cadena registrada que coincida con el identificador URI de redireccionamiento con la URL descodificada, se rechazará la solicitud. Si se encuentra el identificador URI, se usa toda la cadena para redirigir al usuario, incluido el parámetro de consulta estático.

Los identificadores URI de redireccionamiento dinámico siguen estando prohibidos, ya que representan un riesgo para la seguridad y no se pueden usar para conservar la información de estado a través de una solicitud de autenticación. Para este propósito, use el parámetro `state`.

Actualmente, las pantallas de registro de aplicaciones del Azure Portal aún bloquean los parámetros de consulta. Sin embargo, puede editar manualmente el manifiesto de la aplicación para agregar y probar los parámetros de consulta en su aplicación. Para más información, consulte [Novedades en la autenticación](#).

Los registros de actividad (MS Graph API) para Azure AD ahora están disponibles a través de los cmdlets de PowerShell

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Nos complace anunciar que los registros de actividad de Azure AD (informes de auditoría e inicio de sesión) ahora están disponibles a través del módulo de Azure AD PowerShell. Antes podía crear sus propios scripts mediante los de MS Graph API y ahora hemos ampliado esa funcionalidad a los cmdlets de PowerShell.

Para más información acerca de cómo usar estos cmdlets, consulte [Cmdlets de PowerShell de Azure AD para informes](#).

Controles de filtro actualizados para los registros de auditoría e inicio de sesión en Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Hemos actualizado los informes de auditoría e inicio de sesión, por lo que ahora puede aplicar varios filtros sin tener que agregarlos como columnas en las pantallas de informes. Además, ahora puede decidir el número de filtros que desea mostrar en la pantalla. Estas actualizaciones funcionan conjuntamente para que los informes sean más fáciles de leer y se ajusten más a sus necesidades.

Para más información acerca de estas actualizaciones, consulte [Filtrado de registros de auditoría](#) y [Filtrado de las actividades de inicio de sesión](#) de actividades de inicio de sesión.

Junio de 2019

Nueva API riskDetections de Microsoft Graph (versión preliminar)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

Nos complace anunciar que la nueva API riskDetections de Microsoft Graph ya se encuentra en fase de versión preliminar pública. Puede usar esta nueva API para ver una lista de detecciones de riesgos de inicio de sesión y usuario relativos a Identity Protection de su organización. También puede utilizarla para consultar más eficazmente las detecciones de riesgos, incluidos detalles sobre el tipo de detección, el estado, el nivel y mucho más.

Para obtener más información, vea la [documentación de referencia de la API de detección de riesgos](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (junio de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En junio de 2019, hemos agregado estas 22 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Azure AD SAML Toolkit](#), [Otsuka Shokai \(大塚商会\)](#), [ANAQUA](#), [Azure VPN Client](#), [Expenseln](#), [Helper Helper](#), [Costpoint](#), [GlobalOne](#), [Mercedes-Benz In-Car Office](#), [Skore](#), [Oracle Cloud Infrastructure Console](#), [CyberArk SAML Authentication](#), [Scrible Edu](#), [PandaDoc](#), [Perceptyx](#), [Proptimise OS](#), [Vtiger CRM \(SAML\)](#), Oracle Access Manager for Oracle Retail Merchandising, Oracle Access Manager for Oracle E-Business Suite, Oracle IDCS for E-Business Suite, Oracle IDCS for PeopleSoft y Oracle IDCS for JD Edwards

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Automatización del aprovisionamiento de cuentas de usuario para estas aplicaciones SaaS recién admitidas

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Supervisión e informes

Ahora, puede automatizar la creación, actualización y eliminación de cuentas de usuario para estas aplicaciones recién integradas:

- [Zoom](#)
- [Envoy](#)
- [Proxyclick](#)
- [4me](#)

Para obtener más información sobre cómo proteger mejor la organización mediante el aprovisionamiento de cuentas de usuario de forma automatizada, vea [Automatización del aprovisionamiento de usuarios para aplicaciones SaaS con Azure AD](#).

Consulta del progreso en tiempo real del servicio de aprovisionamiento de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Administración del ciclo de vida de la identidad

Hemos actualizado la experiencia de aprovisionamiento de Azure AD para incluir una nueva barra de progreso que muestra a qué altura está el proceso de aprovisionamiento de usuario. Esta experiencia mejorada también proporciona información sobre el número de usuarios aprovisionados durante el ciclo actual, así como los

usuarios aprovisionados hasta la fecha.

Para obtener más información, vea [Comprobación del estado de aprovisionamiento](#).

Ahora, la personalización de marca aparece en las pantallas de cierre de sesión y de error

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Hemos actualizado Azure AD para que, ahora, la personalización de marca de su empresa aparezca en las pantallas de cierre de sesión y de error, así como en la página de inicio de sesión. Para activar esta característica no es preciso hacer nada, Azure AD usa los recursos que ya están configurados en el área **Personalización de marca de empresa** de Azure Portal.

Para obtener más información sobre cómo configurar la personalización de marca de su empresa, vea [Incorporación de la personalización de marca en las páginas de Azure Active Directory de la organización](#).

El Servidor Azure Multi-Factor Authentication (MFA) ya no está disponible para nuevas implementaciones

Tipo: Categoría del servicio: En desuso **Funcionalidad del producto:** MFA Seguridad y protección de la identidad

A partir del 1 de julio de 2019, Microsoft ya no ofrecerá el Servidor MFA para nuevas implementaciones. Ahora, los clientes nuevos que quieran exigir la autenticación multifactor en su organización deberán usar Azure Multi-factor Authentication en la nube. Los clientes que tengan activado el Servidor MFA desde antes del 1 de julio no apreciarán ningún cambio. Podrán seguir descargando las versiones más recientes, obteniendo actualizaciones futuras y generando credenciales de activación.

Para obtener más información, vea [Introducción al Servidor Azure Multi-Factor Authentication](#). Para obtener más información sobre Azure Multi-Factor Authentication en la nube, vea [Planeación de una implementación de Azure Multi-Factor Authentication en la nube](#).

Mayo de 2019

Cambio de servicio: próxima compatibilidad únicamente con protocolos TLS 1.2 en el servicio Application Proxy

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

A fin de proporcionar el mejor cifrado a nuestros clientes, estamos limitando el acceso a únicamente protocolos TLS 1.2 en el servicio Application Proxy. Este cambio se está implantando gradualmente en clientes que ya usan protocolos TLS 1.2 exclusivamente, por lo que no deberían apreciar cambio alguno.

La obsolescencia de TLS 1.0 y TLS 1.1 tendrá lugar el 31 de agosto de 2019, pero avisaremos con antelación para que tenga tiempo para prepararse para este cambio. Para prepararse para este cambio, asegúrese de que sus combinaciones de servidor cliente y servidor de examinador (incluidos los clientes que los usuarios usan para tener acceso a aplicaciones publicadas a través de Application Proxy) se actualizan para usar el protocolo TLS 1.2 y, así, mantengan la conexión con el servicio Application Proxy. Para obtener más información, vea [Adición de una aplicación local para el acceso remoto mediante el proxy de aplicación en Azure Active Directory](#).

Utilización del informe de uso y conclusiones para ver datos de inicio de sesión relativos a las aplicaciones

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Supervisión e informes

Ahora, puede usar el informe de uso y conclusiones, ubicado en el área **Aplicaciones empresariales** de Azure Portal, para obtener una vista de los datos de inicio de sesión relativos a las aplicaciones, con información sobre lo

siguiente:

- Aplicaciones más usadas en la organización
- Aplicaciones con los inicios de sesión con más errores
- Principales errores de inicio de sesión de cada aplicación

Para obtener más información sobre esta característica, vea [Informe de uso y conclusiones en el portal de Azure Active Directory](#).

Automatización del aprovisionamiento de usuarios a aplicaciones en la nube mediante Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Supervisión e informes

Siga estos nuevos tutoriales para utilizar el servicio de aprovisionamiento de Azure AD para automatizar la creación, eliminación y actualización de cuentas de usuario de las siguientes aplicaciones en la nube:

- [Comeet](#)
- [DynamicSignal](#)
- [KeeperSecurity](#)

También puede seguir este nuevo [tutorial de Dropbox](#), que proporciona información sobre cómo aprovisionar objetos de grupo.

Para obtener más información sobre cómo proteger mejor la organización a través del aprovisionamiento automatizado de cuentas de usuario, vea [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

La puntuación segura de identidad ya está disponible en Azure AD (disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** N/D Seguridad y protección de la identidad

Ahora, puede supervisar y mejorar su posición de seguridad de identidad gracias a la característica de puntuación segura de identidad de Azure AD. La característica de puntuación segura de identidad utiliza un mismo panel para ayudarle a:

- Medir de forma objetiva su nivel de seguridad de la identidad, según una puntuación de entre 1 y 223.
- Planear la realización de mejoras en la seguridad de la identidad.
- Ver si las mejoras han logrado sus objetivos de seguridad.

Para obtener más información sobre la característica de puntuación segura de identidad, vea [¿Qué es la puntuación segura de identidad en Azure Active Directory?](#)

Nueva experiencia Registros de aplicaciones ya disponible (disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Experiencia para el desarrollador

La nueva experiencia [Registros de aplicaciones](#) ya está disponible en versión de disponibilidad general. Esta nueva experiencia incluye todas las características clave a las que está acostumbrado de Azure Portal y del portal de Registros de aplicaciones, y las mejora a través de lo siguiente:

- **Una mejor administración de las aplicaciones.** En lugar de ver las aplicaciones en diversos portales, ahora puede verlas todas en una misma ubicación.

- **Un registro de aplicaciones simplificado.** Desde la experiencia de navegación mejorada a la experiencia de selección de permisos renovada, ahora es más fácil registrar y administrar sus aplicaciones.
- **Una información más pormenorizada.** Encontrará más detalles sobre la aplicación, incluidas guías de inicio rápido y otras muchas cosas.

Para obtener más información, vea [Plataforma de identidad de Microsoft](#) y la entrada de blog que anuncia que la [experiencia Registros de aplicación ya está disponible de forma general](#).

Nuevas capacidades disponibles en la API correspondiente a los usuarios de riesgo de Identity Protection

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

Nos complace anunciar que, ahora, puede usar la API correspondiente a los usuarios de riesgo para recuperar el historial de riesgos de los usuarios, descartar usuarios de riesgo y confirmar usuarios como usuarios de riesgo. Este cambio ayuda a actualizar el estado de riesgo de los usuarios de forma más eficaz y a entender sus historiales de riesgos.

Para obtener más información, vea la [documentación de referencia de la API correspondiente a los usuarios de riesgo](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (mayo de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En mayo de 2019, hemos agregado estas 21 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Freedcamp](#), [Real Links](#), [Kianda](#), [Simple Sign](#), [Braze](#), [Displayr](#), [Templafy](#), [Marketo Sales Engage](#), [ACLP](#), [OutSystems](#), [Meta4 Global HR](#), [Quantum Workplace](#), [Cobalt](#), [webMethods API Cloud](#), [RedFlag](#), [Whatfix](#), [Control](#), [JOBHUB](#), [NEOGOV](#), [Foodee](#) y [MyVR](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Experiencias mejoradas de administración y creación de grupos en el portal de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Hemos realizado mejoras en las experiencias relativas a grupos del portal de Azure AD. Estas mejoras permiten a los administradores administrar de mejor forma las listas de grupos y las listas de miembros, así como proporcionar más opciones de creación.

Estas mejoras incluyen:

- Filtrado básico por tipo de pertenencia y tipo de grupo.
- Incorporación de columnas nuevas, como Origen y Dirección de correo electrónico.
- Posibilidad de seleccionar varios grupos, miembros y listas de propietarios para eliminarlos con facilidad.
- Posibilidad de elegir una dirección de correo electrónico y de agregar propietarios durante la creación del grupo.

Para obtener más información vea [Creación de un grupo básico e incorporación de miembros con Azure Active Directory](#).

Configuración de una directiva de nomenclatura para grupos de Office 365 en el portal de Azure AD (disponibilidad general)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración de grupos Colaboración

Ahora, los administradores pueden configurar una directiva de nomenclatura de grupos de Office 365 mediante el portal de Azure AD. Este cambio ayuda a aplicar las convenciones de nomenclatura coherentes para los grupos de Office 365 creados o editados por los usuarios de su organización.

La directiva de nomenclatura de grupos de Office 365 se puede configurar de dos maneras diferentes:

- Definir prefijos o sufijos, que se agregan automáticamente al nombre de un grupo.
- Cargar un conjunto personalizado de palabras bloqueadas de la organización que no se permiten en los nombres de grupo (por ejemplo, "CEO, nómina, RR. HH.").

Para obtener más información, vea [Aplicación de una directiva de nomenclatura en los grupos de Office 365](#).

Ahora, los puntos de conexión de la API de Microsoft Graph están disponibles para los registros de actividad de Azure AD (disponibilidad general)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Nos complace anunciar la disponibilidad general de compatibilidad de puntos de conexión de la API de Microsoft Graph en los registros de actividad de Azure AD. Con este lanzamiento, ahora puede usar la versión 1.0 tanto de los registros de auditoría de Azure AD como de las API de registros de inicio de sesión.

Para obtener más información, vea [Información general sobre la API de registros de auditoría de Azure AD](#).

Ahora, los administradores pueden usar el acceso condicional en el proceso de registro combinado (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Acceso condicional Seguridad y protección de la identidad

Ahora, los administradores pueden crear directivas de acceso condicional para su uso en la página de registro combinado. Esto incluye la puesta en marcha de directivas que permiten el registro bajo estos supuestos:

- Los usuarios están en una red de confianza.
- Los usuarios presentan un bajo riesgo de inicio de sesión.
- Los usuarios están en un dispositivo administrado.
- Los usuarios han aceptado las condiciones de uso de la organización.

Para obtener más información sobre el acceso condicional y el restablecimiento de contraseña, puede ver la entrada de blog sobre el [acceso condicional en la experiencia de registro combinado de restablecimiento de contraseña y MFA de Azure AD](#). Para obtener más información sobre las directivas de acceso condicional en el proceso de registro combinado, vea [Directivas de acceso condicional para el registro combinado](#). Para obtener más información sobre la característica Condiciones de uso de Azure AD, vea [Característica Condiciones de uso de Azure Active Directory](#).

Abril de 2019

Nueva detección de la inteligencia sobre amenazas de Azure AD ya disponible como parte de Azure AD Identity Protection

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Identity Protection Seguridad y protección de la identidad

La detección de la inteligencia sobre amenazas de Azure AD ya está disponible como parte de la característica actualizada Azure AD Identity Protection. Esta nueva funcionalidad ayuda a identificar una actividad de usuario poco común para el usuario en cuestión o una actividad que encaja con patrones de ataque conocidos según los orígenes de la inteligencia sobre amenazas internas y externas de Microsoft.

Para obtener más información sobre la versión actualizada de Azure AD Identity Protection, vea la entrada de blog sobre las [cuatro grandes mejoras de Azure AD Identity Protection que ya están en fase de versión preliminar pública](#) y el artículo [¿Qué es Azure Active Directory Identity Protection \(actualizado\)?](#). Para obtener más información sobre la detección de inteligencia sobre amenazas de Azure AD, vea el artículo [Referencia sobre eventos de riesgo de Azure Active Directory Identity Protection](#).

La administración de derechos de Azure AD ya está disponible (versión preliminar)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Governance Identity Governance

La administración de derechos de Azure AD, ahora en versión preliminar pública, permite a los clientes delegar la administración de paquetes de acceso, que define cómo los empleados y los asociados comerciales pueden solicitar acceso, quién debe aprobar ese acceso y cuánto va a durar ese acceso. Los paquetes de acceso pueden administrar la pertenencia a grupos de Azure AD y Office 365, las asignaciones de roles en aplicaciones empresariales y las asignaciones de roles para sitios de SharePoint Online. Encontrará más información sobre la administración de derechos en el artículo de [información general sobre la administración de derechos de Azure AD](#). Para obtener más información sobre el amplio abanico de características de Azure AD Identity Governance, incluidos Privileged Identity Management, revisiones del acceso y las condiciones de uso, vea [¿Qué es Azure AD Identity Governance?](#)

Configuración de una directiva de nomenclatura para grupos de Office 365 en el portal de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Ahora, los administradores pueden configurar una directiva de nomenclatura de grupos de Office 365 mediante el portal de Azure AD. Este cambio ayuda a aplicar las convenciones de nomenclatura coherentes para los grupos de Office 365 creados o editados por los usuarios de su organización.

La directiva de nomenclatura de grupos de Office 365 se puede configurar de dos maneras diferentes:

- Definir prefijos o sufijos, que se agregan automáticamente al nombre de un grupo.
- Cargar un conjunto personalizado de palabras bloqueadas de la organización que no se permiten en los nombres de grupo (por ejemplo, "CEO, nómina, RR. HH.").

Para obtener más información, vea [Aplicación de una directiva de nomenclatura en los grupos de Office 365](#).

Los registros de actividad de Azure AD ya están disponibles en Azure Monitor (disponibilidad general)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Para que sea más fácil atender sus comentarios sobre las visualizaciones de los registros de actividad de Azure AD, hemos incluido una nueva característica Información en Log Analytics. Esta característica sirve para obtener información sobre los recursos de Azure AD mediante nuestras plantillas interactivas, llamadas libros. Estos libros pregenerados proporcionan detalles sobre las aplicaciones o los usuarios, como lo siguiente:

- **Inicios de sesión** Proporciona detalles sobre las aplicaciones y los usuarios, incluida la ubicación de inicio de sesión, el sistema operativo o el cliente y versión del explorador que se usa y el número de inicios de sesión correctos o con errores.
- **Autenticación heredada y acceso condicional** Proporciona detalles sobre las aplicaciones y los usuarios que usan la autenticación heredada, incluido el uso de Multi-Factor Authentication desencadenado por las directivas de acceso condicional, las aplicaciones que usan directivas de acceso condicional, etc.
- **Análisis de errores de inicio de sesión** Ayuda a averiguar si los errores de inicio de sesión se deben a una acción del usuario, a problemas de directiva o a la infraestructura existente.
- **Informes personalizados** Puede crear libros o editar los ya existentes para ayudar a personalizar la característica Información de su organización.

Para obtener más información, vea [Cómo usar los libros de Azure Monitor en informes de Azure Active Directory](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (abril de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En abril de 2019, hemos agregado estas 21 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

SAP Fiori, HRworks Single Sign-On, Percolate, MobiControl, Citrix NetScaler, Shibumi, Benchling, MileIQ, PageDNA, EduBrite LMS, RStudio Connect, AMMS, Mitel Connect, Alibaba Cloud (Role-based SSO), Certent Equity Management, Sectigo Certificate Manager, GreenOrbit, Workgrid, monday.com, SurveyMonkey Enterprise e Indigo

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nueva opción de frecuencia de revisiones de acceso y selección de varios roles

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Revisiones de acceso Identity Governance

Las nuevas actualizaciones de las revisiones de acceso de Azure AD permiten lo siguiente:

- Cambiar la frecuencia de las revisiones de acceso a **Semestral**, además de las opciones ya existentes (Semanal, Mensual, Trimestral y Anual).
- Seleccionar varios roles de recursos de Azure y de Azure AD al crear una revisión de acceso único. En esta situación, todos los roles se configuran igual y se notifica a todos los revisores al mismo tiempo.

Para obtener más información sobre cómo crear una revisión de acceso, vea [Creación de una revisión de acceso de los grupos o las aplicaciones en las revisiones de acceso de Azure AD](#).

Transición de los sistemas de alertas por correo electrónico de Azure AD Connect en curso; se está enviando información de nuevo remitente de correo electrónico a algunos clientes

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Sincronización de AD Plataforma

Azure AD Connect está en fase de transición de nuestros sistemas de alertas de correo electrónico, lo que puede hacer que algunos clientes vean un nuevo remitente de correo electrónico. Para solucionar este problema, hay que agregar `azure-noreply@microsoft.com` a la lista de permitidos de la organización, o no podrá seguir recibiendo alertas importantes de los servicios de Office 365, Azure o Sync.

Los cambios en los sufijos UPN ya se realizan correctamente entre dominios federados en Azure AD Connect

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Sincronización de AD Plataforma

Ahora puede cambiar correctamente el sufijo UPN de un usuario de un dominio federado a otro en Azure AD Connect. Esta corrección implica que ya no debería aparecer el mensaje de error FederatedDomainChangeError durante el ciclo de sincronización, ni recibir una notificación por correo electrónico que informa de que el objeto no se puede actualizar en Azure Active Directory porque el atributo [FederatedUser.UserPrincipalName] no es válido y pide actualizar el valor en los servicios de directorio local.

Para obtener más información, vea [Solución de errores durante la sincronización](#).

Mayor seguridad con la directiva de acceso condicional basada en la protección de aplicaciones en Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Acceso condicional

Seguridad y protección de la identidad

Ahora, el acceso condicional basado en la protección de aplicaciones está disponible a través de la directiva **Requerir protección de aplicaciones**. Esta nueva directiva ayuda a aumentar la seguridad de la organización al tratar de impedir que:

- Los usuarios obtengan acceso a las aplicaciones sin contar con una licencia de Microsoft Intune.
- Los usuarios no puedan obtener una directiva de protección de aplicaciones de Microsoft Intune.
- Los usuarios obtengan acceso a las aplicaciones sin una directiva de protección de aplicaciones configurada de Microsoft Intune.

Para obtener más información, vea [Cómo usar la aplicación Requerir protección de aplicaciones para el acceso a aplicaciones en la nube mediante el acceso condicional](#).

Nueva compatibilidad con el acceso condicional y el inicio de sesión único de Azure AD en Microsoft Edge (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Acceso condicional

Seguridad y protección de la identidad

Hemos mejorado la compatibilidad de Azure AD para Microsoft Edge, incluido proporcionar nueva compatibilidad con el inicio de sesión único en Azure AD y el acceso condicional. Si ya usó previamente Microsoft Intune Managed Browser, ahora puede usar Microsoft Edge en su lugar.

Para obtener más información sobre cómo configurar y administrar los dispositivos y aplicaciones mediante el acceso condicional, vea [Requerir dispositivos administrados para el acceso a aplicaciones en la nube con el acceso condicional](#) y [Requerir aplicaciones de cliente aprobadas para el acceso a aplicaciones en la nube con el acceso condicional](#). Para obtener más información sobre cómo administrar el acceso mediante Microsoft Edge con directivas de Microsoft Intune, vea [Administración del acceso web con un explorador protegido por directiva de Microsoft Intune](#).

Marzo de 2019

Identity Experience Framework y las directivas personalizadas ya están disponibles en Azure Active Directory B2C (GA)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Ahora es posible crear directivas personalizadas en Azure AD B2C, incluidas las siguientes tareas, que se admiten a escala y bajo nuestro SLA de Azure:

- Crear y cargar trayectos de autenticación personalizada de los usuarios mediante directivas personalizadas.
- Describir los recorridos del usuario paso a paso como intercambios entre proveedores de notificaciones.
- Definir la creación de ramas condicional en recorridos del usuario.
- Transformar y asignar notificaciones para su uso en las comunicaciones y las decisiones en tiempo real.
- Usar servicios habilitados por la API de REST en los trayectos de autenticación personalizada de los usuarios. Por ejemplo, con proveedores de correo electrónico, CRM y sistemas de autorización propietarios.
- Federarse con proveedores de identidades que cumplen con el protocolo OpenIDConnect. Por ejemplo, con Azure AD multiinquilino, proveedores de cuentas de redes sociales o proveedores de verificación de dos factores.

Para más información sobre la creación de directivas personalizadas, vea [Notas para desarrolladores de directivas personalizadas en Azure Active Directory B2C](#) y lea la [entrada de blog de Alex Simon](#), que incluye casos prácticos.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (marzo de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En marzo de 2019, hemos agregado estas 14 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[ISEC7 Mobile Exchange Delegate](#), [MediusFlow](#), [ePlatform](#), [Fulcrum](#), [ExcelityGlobal](#), [Explanation-Based Auditing System](#), [Lean](#), [Powerschool Performance Matters](#), [Cinode](#), [Iris Intranet](#), [Empactis](#), [SmartDraw](#), [Confirmit Horizons](#) y [TAS](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevos conectores de aprovisionamiento de Zscaler y Atlassian en la galería Azure AD (marzo de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Integración de terceros

Automatice la creación, la actualización y la eliminación de cuentas de usuario para las siguientes aplicaciones:

[Zscaler](#), [Zscaler Beta](#), [Zscaler One](#), [Zscaler Two](#), [Zscaler Three](#), [Zscaler ZSCloud](#) y [Atlassian Cloud](#)

Para obtener más información sobre cómo proteger mejor la organización a través del aprovisionamiento automatizado de cuentas de usuario, vea [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#).

Restaurar y administrar los grupos de Office 365 eliminados en el portal de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Ahora es posible ver y administrar los grupos de Office 365 eliminados desde el portal de Azure AD. Este cambio ayuda a ver qué grupos se pueden restaurar, además de permitir eliminar de forma permanente los grupos que la organización no necesite.

Para obtener más información, vea [Restauración de grupos expirados o eliminados](#).

El inicio de sesión único está ahora disponible para aplicaciones locales protegidas por SAML de Azure AD a través del proxy de la aplicación (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Ahora se puede proporcionar una experiencia de inicio de sesión único (SSO) en aplicaciones locales con autenticación SAML, junto con acceso remoto a estas aplicaciones a través del proxy de la aplicación. Para obtener más información sobre cómo configurar el SSO de SAML con las aplicaciones locales, vea [Inicio de sesión único de SAML para aplicaciones locales con proxy de aplicación \(versión preliminar\)](#).

Se interrumpirán las aplicaciones cliente en bucles de solicitud para mejorar la confiabilidad y la experiencia del usuario

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Las aplicaciones cliente pueden emitir incorrectamente cientos de solicitudes del mismo inicio de sesión durante un breve período de tiempo. Todas estas solicitudes, aprobadas o no, contribuyen a una experiencia de usuario deficiente y a mayores cargas de trabajo para el IDP, lo que aumenta la latencia de todos los usuarios y reduce la disponibilidad del IDP.

Esta actualización envía el error `invalid_grant`:

`AADSTS50196: The server terminated an operation because it encountered a loop while processing a request` a las aplicaciones cliente que emiten solicitudes duplicadas varias veces en un breve período de tiempo, más allá del ámbito de operación normal. Las aplicaciones cliente que experimentan este problema deben mostrar un mensaje interactivo que requiera que el usuario vuelva a iniciar sesión. Para obtener más información sobre este cambio y sobre cómo corregir la aplicación si se encuentra con este error, vea [Novedades en la autenticación](#).

Ya disponible la nueva experiencia de usuario de los registros de auditoría

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Hemos creado una nueva página **Registros de auditoría** de Azure AD para mejorar la legibilidad y la búsqueda de información. Para ver la página **Registros de auditoría**, seleccione **Registros de auditoría** en la sección **Actividad** de Azure AD.

The screenshot shows the 'Audit logs' section of the Azure AD portal. The left sidebar has 'Audit logs' selected under 'Contoso - Audit logs'. The main area displays a table of audit log entries with columns: DATE, SERVICE, CATEGORY, ACTIVITY, and STATUS. The table lists various events such as policy updates, role management, and access reviews, all marked as 'Success'. At the top, there are filters for Service (All), Category (All), Activity (All), and Status (All), along with date range and time zone options (Local or UTC). A search bar and buttons for 'Columns', 'Refresh', 'Download', and 'Export Data Settings' are also present.

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
3/25/2019, 2:52:29 PM	Core Directory	Policy	Update policy	Success
3/25/2019, 12:56:09 PM	Core Directory	RoleManagement	Add member to role	Failure
3/25/2019, 12:56:03 PM	Access Reviews	UserManagement	Create access review	Success
3/24/2019, 2:52:28 PM	Core Directory	Policy	Update policy	Success
3/24/2019, 10:49:15 AM	Access Reviews	UserManagement	Access review ended	Success
3/23/2019, 2:52:32 PM	Core Directory	Policy	Update policy	Success
3/22/2019, 2:52:32 PM	Core Directory	Policy	Update policy	Success
3/22/2019, 2:52:31 PM	Core Directory	Policy	Update policy	Success
3/21/2019, 2:52:31 PM	Core Directory	Policy	Update policy	Success
3/21/2019, 12:56:38 PM	Access Reviews	UserManagement	Apply access review	Success
3/21/2019, 12:56:35 PM	Access Reviews	UserManagement	Apply access review	Success

Para obtener más información sobre la página **Registros de auditoría**, vea [Informes de actividad de auditoría en el portal de Azure Active Directory](#).

Nuevas advertencias e instrucciones para ayudar a evitar el bloqueo accidental del administrador por una mala configuración de las directivas de acceso condicional

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Acceso condicional Seguridad y protección de la identidad

Para evitar que los administradores se bloquen accidentalmente a sí mismos en sus propios inquilinos a causa de una mala configuración de las directivas de acceso, hemos creado nuevas advertencias y hemos actualizado las instrucciones en Azure Portal. Para obtener más información sobre las nuevas instrucciones, vea [¿Cuáles son las dependencias del servicio de acceso condicional de Azure Active Directory?](#).

Experiencia mejorada de las condiciones de uso en dispositivos móviles

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Términos de uso Gobernanza

Hemos actualizado y mejorado el modo en el que los usuarios leen y aceptan las condiciones de uso en un dispositivo móvil. Ahora es posible ampliar y reducir el texto, volver atrás, descargar la información y seleccionar hipervínculos. Para obtener más información sobre las nuevas condiciones de uso, vea [Característica Condiciones de uso de Azure Active Directory](#).

Disponible la nueva experiencia de descarga de los registros de actividad de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Ahora se pueden descargar grandes cantidades de registros de actividad directamente desde Azure Portal. Este cambio le permite:

- Descargar hasta 250 000 filas.
- Recibir una notificación cuando se complete la descarga.
- Personalizar el nombre del archivo.
- Determinar el formato de salida como JSON o CSV.

Para más información acerca de esta característica, consulte [Inicio rápido: Descarga de un informe de auditoría mediante Azure Portal](#).

Cambio importante: modificaciones en la evaluación de estado de Exchange ActiveSync (EAS)

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Acceso condicional Control de acceso

Estamos actualizando el modo en que Exchange ActiveSync (EAS) evalúa las condiciones siguientes:

- Ubicación del usuario, basada en el país, la región o la dirección IP.
- Riesgo de inicio de sesión
- Plataforma de dispositivo

Si ha usado estas condiciones anteriormente en las directivas de acceso condicional, tenga en cuenta que el comportamiento de la condición puede cambiar. Por ejemplo, si ha usado la condición de ubicación de usuario en una directiva, es posible que la directiva se omita ahora en función de la ubicación del usuario.

Febrero de 2019

Cifrado de tokens SAML de Azure AD configurable (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Ahora se puede configurar cualquier aplicación SAML compatible para que reciba tokens SAML cifrados. Cuando se configura y se usa con una aplicación, Azure AD cifra las aserciones SAML emitidas mediante una clave pública que se obtiene de un certificado almacenado en Azure AD.

Para obtener más información sobre cómo configurar el cifrado de tokens SAML, vea [Configuración del cifrado de tokens SAML de Azure AD](#).

Creación de una revisión de acceso para grupos o aplicaciones con las revisiones de acceso de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Revisiones de acceso Gobernanza

Ahora se pueden incluir varios grupos o aplicaciones en una única revisión de acceso de Azure AD para comprobar la pertenencia a grupos o la asignación de aplicaciones. Las revisiones de acceso con varios grupos o aplicaciones se configuran usando los mismos valores y todos los revisores incluidos son notificados al mismo tiempo.

Para obtener más información sobre cómo crear una revisión de acceso con las revisiones acceso de Azure AD, vea [Creación de una revisión de acceso de grupos o aplicaciones con las revisiones de acceso de Azure AD](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (febrero de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En febrero de 2019, hemos agregado estas 27 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[Euromonitor Passport](#), [MindTickle](#), [FAT FINGER](#), [AirStack](#), [Oracle Fusion ERP](#), [IDrive](#), [Skyward Qmlativ](#), [Brightidea](#), [AlertOps](#), [Soloinsight-CloudGate SSO](#), [Permission Click](#), [Brandfolder](#), [StoregateSmartFile](#), [Pexip](#), [Stormboard](#), [Seismic](#), [Share A Dream](#), [Bugsnag](#), [webMethods Integration Cloud](#), [Knowledge Anywhere LMS](#), [OU Campus](#), [Periscope Data](#), [Netop Portal](#), [smartvid.io](#), [PureCloud by Genesys](#) y [ClickUp Productivity Platform](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Mejora del registro MFA/SSPR combinado

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Autenticación de usuarios

En respuesta a los comentarios de los clientes, se ha mejorado la experiencia en versión preliminar del registro combinado de MFA/SSPR para que los usuarios puedan registrar de forma más rápida su información de seguridad para MFA y SSPR.

Si quiere activar ahora la experiencia mejorada para los usuarios, siga estos pasos:

1. Inicie sesión como administrador global o administrador de usuarios en Azure Portal y vaya a [Azure Active Directory > Configuración de usuario > Administrar la configuración de las características en versión preliminar del panel de acceso](#).
2. En la opción **Usuarios que pueden utilizar las características en versión preliminar para registrar y administrar la información de seguridad – actualizar**, elija activar las características para un **Grupo**

seleccionado de usuarios o para Todos los usuarios.

A lo largo de las próximas semanas se retirará la capacidad de activar la antigua experiencia combinada de vista previa de registro MFA/SSPR para los inquilinos que todavía no la hayan activado.

Para ver si el control se retirará en su inquilino, siga estos pasos:

1. Inicie sesión como administrador global o administrador de usuarios en Azure Portal y vaya a [Azure Active Directory > Configuración de usuario > Administrar la configuración de las características en versión preliminar del panel de acceso](#).
2. Si la opción **Usuarios que pueden utilizar las características en versión preliminar para registrar y administrar la información de seguridad** está establecida en **Ninguno**, la opción se retirará del inquilino.

Independientemente de si con anterioridad se ha activado la antigua experiencia combinada de vista previa de registro MFA/SSPR, la antigua experiencia se desactivará en una fecha futura. Por ello, es muy recomendable que cambie a la nueva experiencia lo antes posible.

Para obtener más información sobre la experiencia de registro mejorada, vea la entrada de blog sobre las [interesantes mejoras en la experiencia de registro combinado MFA y restablecimiento de contraseña de Azure AD](#).

Experiencia actualizada de la administración de directivas para flujos de usuario

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Se ha actualizado el proceso de creación y administración de directivas para facilitar los flujos del usuario (anteriormente conocidos como directivas integradas). Esta experiencia nueva es ahora la predeterminada para todos los inquilinos de Azure AD.

Si quiere hacer algún otro comentario o sugerencia, use los iconos de sonrisa o desaprobación del área **Envíenos comentarios** en la parte superior de la pantalla del portal.

Para obtener más información sobre la nueva experiencia de administración de directivas, vea la entrada de blog [Azure AD B2C tiene ahora la personalización de JavaScript y muchas más características nuevas](#).

Elección de versiones específicas de elementos de página proporcionadas por Azure AD B2C

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Ahora puede elegir una versión específica de los elementos de página proporcionados por Azure AD B2C. Si selecciona una versión específica, puede probar las actualizaciones antes de que aparezcan en la página y predecir el comportamiento. Además, ahora puede decidir aplicar versiones específicas de la página para permitir las personalizaciones de JavaScript. Para activar esta característica, vaya a la página **Propiedades** en los flujos de usuario.

Para obtener más información sobre cómo elegir versiones específicas de los elementos de la página, vea la entrada de blog [Azure AD B2C tiene ahora la personalización de JavaScript y muchas más características nuevas](#).

Requisitos de contraseña del usuario final configurables para B2C (GA)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Ya es posible configurar la complejidad de las contraseñas que usan los usuarios finales de la organización, en lugar de tener que utilizar la directiva nativa de contraseñas de Azure AD. En la hoja **Propiedades** de los flujos de usuario (antes conocidos como directivas integradas), puede elegir una complejidad de contraseña **Simple** o

Segura, o bien puede crear un conjunto de requisitos **Personalizado**.

Para obtener más información sobre la configuración de los requisitos de complejidad de contraseñas, vea [Configuración de los requisitos de complejidad de contraseñas de Azure Active Directory B2C](#).

Nuevas plantillas predeterminadas para experiencias de autenticación con marca personalizada

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Puede usar nuestras nuevas plantillas predeterminadas, ubicadas en la hoja **Diseños de página** de los flujos de usuario (anteriormente conocidos como directivas integradas), para que los usuarios disfruten de una experiencia de autenticación adaptada a su marca.

Para obtener más información sobre el uso de las plantillas, vea [Azure AD B2C tiene ahora la personalización de JavaScript y muchas más características nuevas](#).

Enero de 2019

Colaboración B2B de Active Directory mediante la autenticación con código de acceso de un solo uso (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

Se ha introducido la autenticación con código de acceso de un solo uso (OTP) para los usuarios invitados de B2B que no pueden autenticarse por otros medios, como Azure AD, una cuenta Microsoft (MSA) o la federación de Google. Este nuevo método de autenticación significa que los usuarios invitados no tienen que crear una nueva cuenta Microsoft. En cambio, al canjear una invitación o acceder a un recurso compartido, un usuario invitado puede solicitar el envío de un código temporal a una dirección de correo electrónico. Con este código temporal, el usuario invitado puede seguir iniciando sesión.

Para más información, consulte [Autenticación con código de acceso de un solo uso de correo electrónico \(versión preliminar\)](#) y el blog [Azure AD makes sharing and collaboration seamless for any user with any account](#) (Azure AD simplifica el uso compartido y la colaboración para cualquier usuario con una cuenta).

Nueva configuración de cookies de Azure AD Application Proxy

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Hemos incluido tres nuevas configuraciones de cookies, disponibles para las aplicaciones que se publican a través de Application Proxy:

- **Usar cookie solo HTTP.** Establece la marca **HTTPOnly** en las cookies de sesión y acceso de Application Proxy. La activación de esta configuración ofrece ventajas de seguridad adicionales, como ayuda para evitar la copia o modificación de cookies por medio de scripting del lado cliente. Se recomienda activar esta marca (elija Sí) para disfrutar de estas ventajas.
- **Usar cookies seguras.** Establece la marca **Segura** en las cookies de sesión y acceso de Application Proxy. La activación de esta configuración ofrece ventajas de seguridad adicionales, como la garantía de que las cookies se transmiten solo a través de canales seguros de TLS, como HTTPS. Se recomienda activar esta marca (elija Sí) para disfrutar de estas ventajas.
- **Usar cookies persistentes.** Impide que las cookies de acceso expiren cuando se cierra el explorador web. Estas cookies se mantienen vigentes durante toda la duración del token de acceso. Sin embargo, las cookies se restablecen si se alcanza la hora de expiración o si el usuario elimina manualmente la cookie. Se recomienda que mantenga la configuración predeterminada **No**, activando el ajuste solo para las aplicaciones anteriores que no comparten cookies entre procesos.

Para obtener más información acerca de las nuevas cookies, consulte [Configuración de las cookies para el acceso a aplicaciones locales en Azure Active Directory](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD (enero de 2019)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En enero de 2019, hemos agregado estas 35 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

Firstbird, Folloze, Talent Palette, Infor CloudSuite, Cisco Umbrella, Zscaler Internet Access Administrator, Expiration Reminder, InstaVR Viewer, CorpTax, Verb, OpenLattice, TheOrgWiki, Pavaso Digital Close, GoodPractice Toolkit, Cloud Service PICCO, AuditBoard, iProva, Workable, CallPlease, GTNexus SSO System, CBRE ServiceInsight, Deskradar, Coralogixv, Signagelive, ARES for Enterprise, K2 for Office 365, Xledger, iDiD Manager, HighGear, Visitly, Korn Ferry ALP, Acadia y Adoddle cSaas Platform

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevas mejoras de Azure AD Identity Protection (versión preliminar pública)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

Nos complace anunciar que hemos agregado las siguientes mejoras a la oferta de versión preliminar pública de Azure AD Identity Protection:

- Una interfaz de usuario actualizada y más integrada
- API adicionales
- Evaluación de riesgos mejorada a través de aprendizaje automático
- Alineación de todo el producto entre usuarios e inicios de sesión no seguros

Para obtener más información sobre las mejoras, consulte [What is Azure Active Directory Identity Protection \(refreshed\)?](#) (¿Qué es Azure Active Directory Identity Protection [actualizado]?) a fin de conocer los detalles y compartir sus ideas a través de los mensajes en el producto.

Nueva característica Bloqueo de aplicación para la aplicación Microsoft Authenticator en dispositivos iOS y Android

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicación Microsoft Authenticator Seguridad y protección de la identidad

Para proteger sus códigos de acceso de un solo uso, la información de aplicación y la configuración de la aplicación, puede activar la característica Bloqueo de aplicación en la aplicación Microsoft Authenticator. Al activar el Bloqueo de aplicación se le pedirá que se autentique con su PIN o características biométricas cada vez que abra la aplicación Microsoft Authenticator.

Para obtener más información, vea las [Preguntas más frecuentes de la aplicación Microsoft Authenticator](#).

Mejora de las capacidades de exportación de Azure AD Privileged Identity Management (PIM)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

Los administradores de Privileged Identity Management (PIM) ahora pueden exportar todas las asignaciones de

roles activas y válidas para un recurso específico, lo cual incluye las asignaciones de roles para todos los recursos secundarios. Anteriormente, a los administradores les resultaba difícil obtener una lista completa de asignaciones de roles para una suscripción y tenían que exportar dichas asignaciones para cada recurso específico.

Para obtener más información, consulte [Visualización de la actividad y del historial de auditoría para los roles de recursos de Azure en PIM](#).

Noviembre/diciembre de 2018

Los usuarios que se quitaron del ámbito de sincronización ya no podrán cambiarse a cuentas solo en la nube

Tipo: Categoría del servicio: Corregida Funcionalidad del producto: Administración de usuarios Directorio

IMPORTANT

Hemos escuchado y comprendido la frustración que les genera esta corrección. Por lo tanto, hemos revertido este cambio hasta el momento en que podamos ofrecerle una implementación más sencilla para su organización.

Se ha corregido un error en el que la marca DirSyncEnabled de un usuario se cambiaba erróneamente a **False** cuando el objeto de Active Directory Domain Services se excluía del ámbito de sincronización y, después, se movía a la Papelera de reciclaje de Azure AD en el siguiente ciclo de sincronización. Como resultado de esta corrección, si el usuario se excluye del ámbito de sincronización y posteriormente se restaura desde la Papelera de reciclaje de Azure AD, la cuenta de dicho usuario permanece sincronizada desde la instancia local de AD, según lo previsto, y no se puede administrar en la nube, ya que su origen de autoridad (SoA) permanece como AD local.

Antes de esta corrección, había un problema cuando se cambiaba la marca DirSyncEnabled a False. Daba la impresión errónea de que estas cuentas se convertían en objetos solo en la nube y de que las cuentas se podían administrar en la nube. Sin embargo, las cuentas siguen conservando su SoA como propiedades locales y sincronizadas (atributos paralelos) procedentes de la instancia local de AD. Esta situación provocó varios problemas en Azure AD y en otras cargas de trabajo en la nube (como Exchange Online), ya que esperaban tratar estas cuentas como sincronizadas desde AD y, sin embargo, se comportaban como cuentas solo en la nube.

En este momento, la única manera de convertir realmente una cuenta sincronizada de AD en una cuenta de solo nube, es deshabilitando DirSync en el nivel del inquilino, lo que desencadena una operación de back-end para transferir el SoA. Este tipo de cambio de SoA requiere (pero no se limita a) la limpieza de todos los atributos locales relacionados (como los atributos paralelos y de LastDirSyncTime) y el envío de una señal a otras cargas de trabajo en la nube para convertir también su objeto respectivo en una cuenta solo en la nube.

Por lo tanto, esta corrección evita las actualizaciones directas sobre el atributo ImmutableID de un usuario sincronizado desde AD, lo que era necesario en algunos escenarios en el pasado. Por diseño, el atributo ImmutableID de un objeto en Azure AD, como su nombre indica, es inmutable. Existen nuevas características implementadas en los clientes de sincronización de Azure AD Connect y Azure AD Connect Health para abordar estos escenarios:

- **Actualizaciones del atributo ImmutableID a gran escala para muchos usuarios por etapas**

Por ejemplo, debe realizar una migración entre bosques de AD DS larga. Solución: Use Azure AD Connect para la **Configuración del delimitador de origen** y, mientras el usuario migra, copie los valores del atributo ImmutableID existentes de Azure AD al atributo DS-Consistency-Guid del usuario de AD DS local del nuevo bosque. Para obtener más información, consulte [Uso de msDS-ConsistencyGuid como sourceAnchor](#).

- **Actualizaciones del atributo ImmutableID a gran escala para muchos usuarios de una sola vez**

Por ejemplo, al implementar Azure AD Connect se cometió un error, y ahora es necesario cambiar el atributo SourceAnchor. Solución: Deshabilite DirSync en el nivel del inquilino y borre todos los valores de

ImmutableID no válidos. Para obtener más información, vea [Desactivar la sincronización de directorios para Office 365](#).

- **Hacer coincidir un usuario local con un usuario existente de Azure AD** Por ejemplo, un usuario que se haya vuelto a crear en AD DS genera un duplicado en la cuenta de Azure AD en lugar de reasignarlo a una cuenta de Azure AD existente (objeto huérfano). Solución: Use Azure AD Connect Health en Azure Portal para reasignar el delimitador de origen o el atributo ImmutableID. Para obtener más información, consulte [Escenario del objeto huérfano](#).

Cambio de última hora: Actualizaciones de los esquemas de registros de auditoría y de inicio de sesión mediante Azure Monitor

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Informes Supervisión e informes

Actualmente, estamos publicando los flujos de registro de auditorías e inicios de sesión mediante Azure Monitor, por lo que puede integrar fácilmente los archivos de registro con sus herramientas SIEM o con Log Analytics. Basándonos en sus comentarios, y en preparación para el anuncio de disponibilidad general para esta característica, vamos a realizar los siguientes cambios en el esquema. Estos cambios en los esquemas y las actualizaciones de documentación relacionadas se producirán en la primera semana de enero.

Nuevos campos en el esquema de auditoría

Vamos a agregar un nuevo campo **Tipo de operación**, para proporcionar el tipo de operación que se realiza en el recurso. Por ejemplo, **Agregar**, **Actualizar** o **Eliminar**.

Campos modificados en el esquema de auditoría

Los siguientes campos han cambiado en el esquema de auditoría:

NOMBRE DEL CAMPO	QUÉ CAMBIA	VALORES ANTERIORES	NUEVOS VALORES
Category	Este era el campo Nombre de servicio . Ahora es el campo Categorías de auditoría . A Nombre de servicio se le ha cambiado el nombre por el de campo loggedByService .	<ul style="list-style-type: none">• Account Provisioning (Aprovisionamiento de cuentas)• Core Directory (Directorio principal)• Autoservicio de restablecimiento de contraseña	<ul style="list-style-type: none">• User Management• Administración de grupos• Administración de la aplicación
targetResources	Incluye TargetResourceType en el nivel superior.		<ul style="list-style-type: none">• Directiva• Aplicación• Usuario• Grupo
loggedByService	Proporciona el nombre del servicio que generó el registro de auditoría.	Null	<ul style="list-style-type: none">• Account Provisioning (Aprovisionamiento de cuentas)• Core Directory (Directorio principal)• Restablecimiento de la contraseña de autoservicio

NOMBRE DEL CAMPO	QUÉ CAMBIA	VALORES ANTERIORES	NUEVOS VALORES
Resultado	Proporciona el resultado de los registros de auditoría. Anteriormente, este aparecía en una lista, pero ahora se muestra el valor real.	<ul style="list-style-type: none"> • 0 • 1 	<ul style="list-style-type: none"> • Correcto • Error

Campos modificados en el esquema de inicio de sesión

Los siguientes campos han cambiado en el esquema de inicio de sesión:

NOMBRE DEL CAMPO	QUÉ CAMBIA	VALORES ANTERIORES	NUEVOS VALORES
appliedConditionalAccessPolicies	Este era el campo conditionalaccessPolicies . Ahora es el campo appliedConditionalAccessPolicies .	Sin cambios	Sin cambios
conditionalAccessStatus	Proporciona el resultado del estado de la directiva de acceso condicional en el inicio de sesión. Anteriormente, este aparecía en una lista, pero ahora se muestra el valor real.	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3 	<ul style="list-style-type: none"> • Correcto • Error • No aplicado • Disabled
appliedConditionalAccessPolicies: result	Proporciona el resultado del estado individual de la directiva de acceso condicional en el inicio de sesión. Anteriormente, este aparecía en una lista, pero ahora se muestra el valor real.	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3 	<ul style="list-style-type: none"> • Correcto • Error • No aplicado • Disabled

Para más información acerca del esquema, consulte [Interpretación del esquema de registros de auditoría de Azure AD en Azure Monitor \(versión preliminar\)](#).

Mejoras de la protección de identidades en el modelo de Machine Learning supervisado y en el motor de puntuaciones de riesgo

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Identity Protection Puntuaciones de riesgo

Las mejoras en el usuario relacionadas con la protección de identidades y en el motor de evaluación de riesgos de inicio de sesión pueden ayudar a mejorar la precisión y cobertura de los riesgos del usuario. Puede que los administradores hayan observado que el nivel de riesgo del usuario ya no está vinculado directamente al nivel de riesgo de detecciones específicas y que hay un aumento en el número y en el nivel de los eventos de inicio de sesión de riesgo.

El modelo de Machine Learning supervisado es el encargado ahora de evaluar las detecciones de riesgo. Este calcula el riesgo del usuario usando características adicionales de los inicios de sesión del usuario y un patrón de detecciones. Según este modelo, el administrador puede detectar usuarios con puntuaciones de riesgo altas, incluso aunque las detecciones asociadas con ese usuario sean de nivel bajo o medio.

Los administradores pueden restablecer sus propias contraseñas mediante la aplicación Microsoft Authenticator (versión preliminar pública)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Autenticación de usuarios

Los administradores de Azure AD ya pueden restablecer sus propias contraseñas mediante las notificaciones de la aplicación Microsoft Authenticator o mediante un código de cualquier aplicación de autenticación móvil, o token de hardware. Para restablecer sus propias contraseñas, los administradores ahora pueden usar dos de los métodos siguientes:

- Notificación de la aplicación Microsoft Authenticator
- Un código de otra aplicación de autenticación móvil o un token de hardware
- Email
- Llamada de teléfono
- mensaje de texto

Para más información sobre el uso de la aplicación Microsoft Authenticator para restablecer contraseñas, consulte [Autoservicio de restablecimiento de contraseña de Azure AD: Aplicación móvil y SSPR \(versión preliminar\)](#)

Nuevo rol de administrador de dispositivos en la nube de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración y registro de dispositivos Control de acceso

Los administradores pueden asignar usuarios al nuevo rol de administrador de dispositivos en la nube para realizar las tareas propias de este rol. Los usuarios asignados a este rol pueden habilitar, deshabilitar y eliminar dispositivos en Azure AD y leer las claves de BitLocker de Windows 10 (si las hay) en Azure Portal.

Para más información acerca de los roles y permisos, consulte [Asignación de roles de administrador en Azure Active Directory](#).

Administración de dispositivos con la nueva marca de tiempo de actividad de Azure AD (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración y registro de dispositivos Administración del ciclo de vida de dispositivos

Somos conscientes de que, con el paso del tiempo, debe actualizar y retirar los dispositivos de su organización en Azure AD para evitar tener dispositivos obsoletos en su entorno. Para ayudarle con este proceso, Azure AD ya actualiza los dispositivos con una nueva marca de tiempo de actividad que le ayuda a administrar el ciclo de vida del dispositivo.

Para más información acerca de cómo obtener y usar esta marca de tiempo, consulte [Procedimiento: Administración de dispositivos obsoletos en Azure AD](#).

Los administradores pueden requerir que los usuarios acepten los términos de uso en cada dispositivo

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Gobernanza

Los administradores ahora pueden activar la opción **Requerir que los usuarios concedan su consentimiento en todos los dispositivos** para requerir que los usuarios acepten los términos de uso en todos los dispositivos que estén usando en su inquilino.

Para obtener más información, consulte [la sección de términos de uso por dispositivo del artículo Característica Términos de uso de Azure Active Directory](#).

Los administradores pueden configurar la expiración de los términos de uso mediante una programación periódica

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Gobernanza

Los administradores pueden ahora activar la opción **Expirar autorizaciones** para hacer que los términos de uso expiren para todos los usuarios según la programación periódica especificada. La programación puede ser anual, semestral, trimestral o mensual. Una vez que los términos de uso expiran, los usuarios deben volver a aceptarlos.

Para obtener más información, consulte [la sección Agregar términos de uso del artículo Característica Términos de uso de Azure Active Directory](#).

Los administradores pueden configurar la expiración de los términos de uso según la programación de cada usuario

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Gobernanza

Los administradores ahora pueden especificar una duración tras la cual el usuario debe volver a aceptar los términos de uso. Por ejemplo, los administradores pueden especificar que los usuarios deben volver a aceptar los términos de uso cada 90 días.

Para obtener más información, consulte [la sección Agregar términos de uso del artículo Característica Términos de uso de Azure Active Directory](#).

Nuevos correos electrónicos de Azure Active Directory Privileged Identity Management (PIM) para los roles de Azure Active Directory

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

Los clientes que usan Azure AD Privileged Identity Management (PIM) ahora pueden recibir un correo electrónico de resumen semanal que incluye la información siguiente de los últimos siete días:

- Introducción a las asignaciones de roles principales y permanentes
- Número de usuarios que activan roles
- Número de usuarios asignados a roles en PIM
- Número de usuarios asignados a roles fuera de PIM
- Número de usuarios a los que se ha "convertido en permanentes" en PIM

Para más información sobre PIM y las notificaciones de correo electrónico disponibles, consulte [Notificaciones por correo electrónico en PIM](#).

Las licencias basadas en grupos tienen ahora disponibilidad general

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Directorio

Las licencias basadas en grupos ya no están en la fase de versión preliminar pública sino en la de disponibilidad general. Como parte de esta versión general, se ha logrado que esta característica sea más escalable y se ha agregado la posibilidad de volver a procesar las asignaciones de licencias basadas en grupos para un solo usuario y la posibilidad de usar licencias basadas en grupos con licencias E3/A3 de Office 365.

Para más información acerca de las licencias basadas en grupos, consulte [¿En qué consisten las licencias basadas en grupos de Azure Active Directory?](#)

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: noviembre de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En noviembre de 2018, hemos agregado 26 nuevas aplicaciones con compatibilidad con la federación a la galería

de aplicaciones:

[CoreStack](#), [HubSpot](#), [GetThere](#), [Gra-Pe](#), [eHour](#), [Consent2Go](#), [Appinux](#), [DriveDollar](#), [Useall](#), [Infinite Campus](#), [Alaya](#), [HeyBuddy](#), [Wrike SAML](#), [Drift](#), [Zenegy for Business Central 365](#), [Everbridge Member Portal](#), [IDEO](#), [Ivanti Service Manager \(ISM\)](#), [Peakon](#), [Allbound SSO](#), [Plex Apps - Classic Test](#), [Plex Apps – Classic](#), [Plex Apps - UX Test](#), [Plex Apps – UX](#), [Plex Apps – IAM](#), [CRAFTS - Childcare Records, Attendance, & Financial Tracking System](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Octubre de 2018

Los registros de Azure AD ahora funcionan con Azure Log Analytics (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Nos complace anunciar que ahora puede reenviar los registros de Azure AD a Azure Log Analytics. Esta característica tan solicitada le ayuda a obtener un acceso aún mejor al análisis para su negocio, las operaciones y la seguridad, además de contribuir a supervisar la infraestructura. Para más información, consulte el blog sobre [los registros de actividad de Azure Active Directory en Azure Log Analytics que ya está disponible](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: octubre de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En octubre de 2018, hemos agregado 14 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[My Award Points](#), [Vibe HCM](#), [ambyint](#), [MyWorkDrive](#), [BorrowBox](#), [Dialpad](#), [ON24 Virtual Environment](#), [RingCentral](#), [Zscaler Three](#), [Phraseanet](#), [Appraisd](#), [Workspot Control](#), [Shuccho Navi](#), [Glassfrog](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Notificaciones por correo electrónico de Azure AD Domain Services

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Domain Services Azure AD Domain Services

Azure AD Domain Services proporciona alertas en Azure Portal sobre configuraciones incorrectas o problemas con el dominio administrado. Estas alertas incluyen guías paso a paso para que pueda intentar corregir los problemas sin tener que ponerse en contacto con el servicio de soporte técnico.

A partir de octubre, podrá personalizar la configuración de notificaciones para el dominio administrado por lo que, cuando se produzcan nuevas alertas, se enviará un correo electrónico a un grupo de personas designado, sin necesidad de tener que comprobar constantemente si en el portal hay actualizaciones.

Para más información, consulte [Configuración de notificaciones de Azure AD Domain Services](#).

El portal de Azure AD admite el uso de la API de dominio ForceDelete para eliminar los dominios personalizados

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración de directorios Directorio

Nos complace anunciar que ahora puede usar la API de dominio ForceDelete para eliminar los nombres de dominio personalizados cambiando las referencias de forma asíncrona, como los usuarios, los grupos y las aplicaciones del nombre de dominio personalizado (contoso.com) al nombre de dominio predeterminado inicial (contoso.onmicrosoft.com).

Este cambio ayuda a eliminar más rápidamente los nombres de dominio personalizados si la organización ya no utiliza el nombre o si necesita utilizar ese nombre de dominio con otra instancia de Azure AD.

Para más información, consulte [Eliminación de un nombre de dominio personalizado](#).

Septiembre de 2018

Permisos de rol de administrador actualizados para grupos dinámicos

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Administración de grupos Colaboración

Se ha corregido un problema, por lo que determinados roles de administrador ya pueden crear y actualizar reglas de pertenencia dinámicas, sin necesidad de ser el propietario del grupo.

Los roles son:

- Administrador global
- Administrador de Intune
- Administrador de usuarios

Para más información, consulte [Creación de un grupo dinámico y comprobación de su estado](#)

Valores de configuración simplificada de inicio de sesión único (SSO) para algunas aplicaciones de terceros

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Somos conscientes de que la configuración del inicio de sesión único (SSO) para aplicaciones de SaaS (software como servicio) puede ser un desafío debido a la naturaleza única de la configuración de cada aplicación. Hemos creado una configuración simplificada para llenar de forma automática los valores de configuración de SSO para las siguientes aplicaciones de SaaS de terceros:

- Zendesk
- ArcGIS Online
- Jamf Pro

Para empezar a usar esta experiencia de un solo clic, vaya a la página [Azure Portal > Configuración de SSO](#) de la aplicación. Para más información, consulte [Integración de aplicación SaaS con Azure Active Directory](#)

Página Azure Active Directory - Where is your data located? (Azure Active Directory: dónde se encuentran los datos)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Otros GoLocal

Seleccione la región de su empresa en la página [Azure Active Directory - Where is your data located?](#) (Azure Active Directory: dónde se encuentran los datos) para ver qué centro de datos de Azure alberga los datos en reposo de Azure AD para todos los servicios de Azure AD. Puede filtrar la información por los servicios específicos de Azure AD para la región de su empresa.

Para acceder a esta característica y para más información, consulte [Azure Active Directory - Where is your data located? \(Azure Active Directory: dónde se encuentran los datos\)](#).

Nuevo plan de implementación disponible para el panel de acceso a Mis aplicaciones

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones SSO

Consulte el nuevo plan de implementación disponible para el panel de acceso a Mis aplicaciones (<https://aka.ms/deploymentplans>). El panel de acceso a Mis aplicaciones proporciona a los usuarios un único lugar en el que pueden buscar y acceder a sus aplicaciones. Este portal también proporciona a los usuarios oportunidades de autoservicio, como por ejemplo solicitar acceso a aplicaciones y grupos, o administrar el acceso a estos recursos en nombre de otros.

Para más información, consulte [¿Qué es el portal Mis aplicaciones?](#)

Pestaña nueva solución de problemas y soporte técnico de la página de registros de inicios de sesión de Azure Portal

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

El fin de la nueva pestaña **Solución de problemas y soporte técnico** de la página **Inicios de sesión** de Azure Portal es ayudar a los administradores e ingenieros de soporte técnico a solucionar problemas relacionados con los inicios de sesión de Azure AD. Esta nueva pestaña proporciona el código de error, mensaje de error y las recomendaciones de corrección (si existen) para ayudar a solucionar el problema. Si no puede resolver el problema, también le ofrecemos una nueva forma de crear una incidencia de soporte técnico mediante **Copiar al Portapapeles**, que rellena los campos **Id. de solicitud** y **Fecha (UTC)** del archivo de registro en su incidencia de soporte técnico.

The screenshot shows the Azure Active Directory Sign-ins blade for the 'Wingtip Toys - Sign-ins' application. On the left, there's a navigation menu with options like Company branding, User settings, Properties, Notifications settings, Security (Identity Secure Score, Conditional access, MFA Server, Users flagged for risk, Risky sign-ins, Authentication methods), Activity (Sign-ins, Audit logs), and Troubleshooting + Support. The main area displays sign-in details for a user named 'johndoe'. The 'Details' section has tabs for Sign-In info, Device info, MFA, Conditional Access, and Troubleshooting and support (which is highlighted with a red box). Under 'Sign-In info', it shows 'Sign-in status: Failure' and 'Sign-in error code: 65005'. The 'Failure reason' section contains a detailed message about a missing resource access list. To the right, there's a 'Create a new support request' section with steps 1-4 and fields for Request ID and Timestamp.

Wingtip Toys - Sign-ins
Azure Active Directory

Search (Ctrl+ /) Columns Refresh Download Script Power BI Export Data Settings Troubleshoot

Company branding User settings Properties Notifications settings Security Activity Troubleshooting + Support

Sign-In info Device info MFA Conditional Access Troubleshooting and support

Sign-in status: Failure
Sign-in error code: 65005

Failure reason: The application required resource access list does not contain applications discoverable by the resource or The client application has requested access to resource, which was not specified in its required resource access list or Graph service returned bad request or resource not found. If the application supports SAML, you may have configured the application with the wrong identifier (Entity). Try out the resolution listed for SAML using the link below: https://docs.microsoft.com/azure/active-directory/application-sign-in-problem-federated-sso-gallery/?WT.mc_id=DMC_AAD_Manage_Apps_Troubleshooting_Nav#no-resource-in-requiredresourceaccess-list.

If you need assistance from Microsoft Customer Support

1. Create a new support request
2. On the 'Basics' tab, set Issue type to 'Technical', and Service to 'Azure Active Directory'
3. On the 'Problem' tab, set Problem type to 'Issue signing in to applications' and Category to 'Gallery + "bring your own" applications'
4. In the 'Problem details' section, paste the request ID and timestamp:

Request ID: d8ca2572-ec81-4a3b-b3fa-14d4568f0600
Timestamp: 2018-09-19T04:19:04.734Z

Compatibilidad mejorada con las propiedades de extensión personalizadas utilizadas para crear reglas de pertenencia dinámica

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración de grupos Colaboración

Con esta actualización, ahora puede hacer clic en el vínculo **Get custom extension properties** (Obtener propiedades de extensión personalizadas) desde el generador de reglas de grupo de usuarios dinámico, escriba el identificador de aplicación único y recibir la lista completa de las propiedades de extensión personalizadas para usarla al crear una regla de pertenencia dinámica para los usuarios. Esta lista también se puede actualizar esta lista para obtener nuevas propiedades de extensión personalizada para la aplicación.

Para más información acerca del uso de propiedades de extensión personalizadas para las reglas de pertenencia dinámica, consulte [Propiedades de extensión y propiedades de extensión personalizadas](#)

Nuevas aplicaciones cliente aprobadas para el acceso condicional basado en aplicaciones de Azure AD

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

Las siguientes aplicaciones se incluyen en la lista de [aplicaciones cliente aprobadas](#):

- Microsoft To-Do
- Microsoft Stream

Para más información, consulte:

- [Acceso condicional basado en aplicaciones de Azure AD](#)

Nueva compatibilidad con Autoservicio de restablecimiento de contraseña desde la pantalla de bloqueo de Windows 7/8.1

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** SSPR Autenticación de usuarios

Después de configurar esta nueva característica los usuarios verán un vínculo para restablecer su contraseña desde la pantalla de **bloqueo** de un dispositivo que ejecuta Windows 7, Windows 8 o Windows 8.1. Al hacer clic en ese vínculo, se guía al usuario por el mismo flujo de restablecimiento de contraseña que por el explorador web.

Para más información, consulte [How to: Enable password reset from Windows 7, 8, and 8.1](#) (Procedimiento para habilitar el restablecimiento de contraseña desde Windows 7, 8, and 8.1)

Aviso de cambio: Los códigos de autorización ya no estarán disponibles para su reutilización

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

A partir del 15 de noviembre de 2018, Azure AD dejará de aceptar los códigos de autenticación que se usaban anteriormente para las aplicaciones. Este cambio de seguridad ayuda a poner Azure AD en consonancia con la especificación de OAuth y se aplicará en los puntos de conexión v1 y v2.

Si la aplicación reutiliza códigos de autorización para obtener tokens para varios recursos, es recomendable que use el código para obtener un token de actualización y, a continuación, utilice este para adquirir tokens adicionales para otros recursos. Los códigos de autorización solo se pueden usar una vez, pero los tokens de actualización se pueden usar varias veces en varios recursos. Una aplicación que intente reutilizar un código de autenticación durante el flujo de código de OAuth obtendrá el error `invalid_grant`.

Para este y otros cambios relacionados con los protocolos, consulte [la lista completa de las novedades de la autenticación](#).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: septiembre de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En septiembre de 2018, hemos agregado 16 nuevas aplicaciones con compatibilidad con la federación a la galería de aplicaciones:

[Uberflip](#), [Comeet Recruiting Software](#), [Workteam](#), [ArcGIS Enterprise](#), [Nuclino](#), [JDA Cloud](#), [Snowflake](#), [NavigoCloud](#), [Figma](#), [join.me](#), [ZephyrSSO](#), [Silverback](#), [Riverbed Xirrus EasyPass](#), [Rackspace SSO](#), [Enlyft SSO for Azure](#), [SurveyMonkey](#), [Convene](#) y [dmarcian](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure

AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Compatibilidad con métodos de transformación de notificaciones adicionales

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Hemos introducido nuevos métodos de transformación de notificaciones, ToLower() y ToUpper(), que se pueden aplicar a los tokens SAML desde la página **Configuración del inicio de sesión único basada en SAML**.

Para más información, consulte [Procedimientos para personalizar las notificaciones emitidas en el token SAML para aplicaciones empresariales en Azure AD](#)

Interfaz de usuario de la configuración de aplicaciones basadas en SAML actualizada (versión preliminar)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Aplicaciones empresariales SSO

Como parte de nuestra interfaz de usuario de la configuración de aplicaciones basadas en SAML actualizada, obtendrá:

- Una experiencia actualizada del tutorial para configurar aplicaciones basadas en SAML.
- Mayor visibilidad de lo que falta o es incorrecto en la configuración.
- La capacidad para agregar varias direcciones de correo electrónico para la notificación de expiración de certificados.
- Nuevos métodos de transformación de notificaciones, ToLower() ToUpper(), y más.
- Una forma de cargar su propio certificado de firma de tokens para las aplicaciones empresariales.
- Una forma de establecer el formato de NameID para aplicaciones SAML y una forma de establecer el valor de NameID como extensiones de directorio.

Para activar esta vista actualizada, haga clic en el vínculo **Try out our new experience** (Probar nuestra nueva experiencia) en la parte superior de la página **Inicio de sesión único**. Para más información, consulte el [Tutorial: Configuración del inicio de sesión único basado en SAML para una aplicación con Azure Active Directory](#).

Agosto de 2018

Cambios realizados en los intervalos de direcciones IP de Azure Active Directory

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Otros Plataforma

Estamos introduciendo intervalos IP mayores en Azure AD, lo que significa que si ha configurado los intervalos IP de Azure AD para los firewalls, enruteadores o grupos de seguridad de red, deberá actualizarlos. Realizamos esta actualización para que no tenga que volver a cambiar su firewall, enruteador ni las configuraciones de intervalo IP de los grupos de seguridad de red cuando Azure AD agregue nuevos puntos de conexión.

El tráfico se moverá a estos nuevos intervalos durante los próximos dos meses. Para continuar con un servicio ininterrumpido, debe agregar estos valores actualizados a las direcciones IP antes del 10 de septiembre de 2018:

- 20.190.128.0/18
- 40.126.0.0/18

Se recomienda encarecidamente no quitar los intervalos IP antiguos hasta que todo el tráfico se haya movido a los nuevos intervalos. Para actualizaciones sobre el movimiento y saber cuándo quitar los intervalos antiguos, consulte [Office 365 URLs and IP address ranges](#) (Direcciones URL e intervalos IP de Office 365).

Aviso de cambio: Los códigos de autorización ya no estarán disponibles para su reutilización

Tipo: Categoría del servicio: Plan de cambio Funcionalidad del producto: Autenticaciones (inicios de sesión)
Autenticación de usuarios

A partir del 15 de noviembre de 2018, Azure AD dejará de aceptar los códigos de autenticación que se usaban anteriormente para las aplicaciones. Este cambio de seguridad ayuda a poner Azure AD en consonancia con la especificación de OAuth y se aplicará en los puntos de conexión v1 y v2.

Si la aplicación reutiliza códigos de autorización para obtener tokens para varios recursos, es recomendable que use el código para obtener un token de actualización y, a continuación, utilice este para adquirir tokens adicionales para otros recursos. Los códigos de autorización solo se pueden usar una vez, pero los tokens de actualización se pueden usar varias veces en varios recursos. Una aplicación que intente reutilizar un código de autenticación durante el flujo de código de OAuth obtendrá el error invalid_grant.

Para este y otros cambios relacionados con los protocolos, consulte [la lista completa de las novedades de la autenticación](#).

Administración de información de seguridad convergida para restablecimiento de contraseña de autoservicio (SSPR) y Multi-Factor Authentication (MFA)

Tipo: Categoría del servicio: Nueva característica Funcionalidad del producto: SSPR Autenticación de usuarios

Esta nueva característica ayuda a los usuarios a administrar su información de seguridad (por ejemplo, número de teléfono, aplicación móvil, etc.) para SSPR y MFA en una sola ubicación y una misma experiencia, al contrario que sucedía anteriormente cuando se realizaba en dos ubicaciones diferentes.

Esta experiencia convergente también funciona para los usuarios que utilizan MFA o SSPR. Además, aunque la organización no aplique el registro de MFA o de SSPR, los usuarios pueden registrar todos los métodos de información de seguridad que permita la organización desde el portal Mis aplicaciones.

Se trata de una versión preliminar pública opcional. Los administradores pueden activar la nueva experiencia (si lo desean) para un grupo de usuarios seleccionado o para todos los usuarios de un inquilino. Para más información sobre la experiencia convergente, consulte el [blog de experiencia convergente](#)

Nueva configuración de las cookies solo HTTP en las aplicaciones de Azure AD Application Proxy

Tipo: Categoría del servicio: Nueva característica Funcionalidad del producto: Proxy de aplicaciones Control de acceso

Hay un nuevo valor llamado, **HTTP-Only Cookies** (Cookies solo HTTP) en las aplicaciones de Application Proxy. Este valor ayuda a proporcionar un nivel extra de seguridad incluyendo la marca HTTPOnly en el encabezado de la respuesta HTTP para las cookies de acceso a Application Proxy y las de la sesión, impidiendo el acceso a cookies procedentes de un script en el lado del cliente e impidiendo acciones como la copia o modificación de la cookie. Aunque esta marca no se ha usado anteriormente, las cookies se han cifrado y transmitido siempre a través de una conexión TLS para proteger frente a modificaciones no adecuadas.

Este valor no es compatible con aplicaciones que usan controles ActiveX, como Escritorio remoto. Si este es su caso, es aconsejable que desactive este valor.

Para más información acerca del valor de cookies solo HTTP, consulte [Publicación de aplicaciones mediante Azure AD Application Proxy](#).

Privileged Identity Management (PIM) para recursos de Azure es compatible con los tipos de recursos del grupo de administración

Tipo: Categoría del servicio: Nueva característica Funcionalidad del producto: Privileged Identity

Management Privileged Identity Management

La configuración de la activación y asignación Just-In-Time se puede aplicar ahora a los tipos de recursos del grupo de administración, al igual que ya lo hace con las suscripciones, grupos de recursos y recursos (como máquinas virtuales, App Services, etc). Además, cualquier usuario con un rol que proporcione acceso de administrador para un grupo de administración puede detectar y administrar ese recurso en PIM.

Para más información acerca de PIM y los recursos de Azure, consulte [Detectar y administrar recursos de Azure mediante Privileged Identity Management](#)

La característica de acceso a la aplicación (versión preliminar) proporciona un acceso más rápido al portal de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

En la actualidad, al activar un rol con PIM, puede que los permisos tarden más de 10 minutos en surtir efecto. Si opta por usar la característica de acceso a la aplicación, que se encuentra actualmente en versión preliminar pública, los administradores podrán acceder al portal de Azure AD tan pronto como se complete la solicitud de activación.

Actualmente, esta característica solo admite la experiencia del portal de Azure AD y los recursos de Azure. Para más información acerca de PIM y la característica de acceso a la aplicación, consulte [¿Qué es Azure AD Privileged Identity Management?](#)

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: agosto de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En agosto de 2018, hemos agregado estas 16 nuevas aplicaciones con compatibilidad con la federación para la galería de aplicaciones:

[Hornbill](#), [Bridgeline Unbound](#), [Sauce Labs - Mobile and Web Testing](#), [Meta Networks Connector](#), [Way We Do](#), [Spotinst](#), [ProMaster \(by Inlogik\)](#), [SchoolBooking](#), [4me](#), [Dossier](#), [N2F - Expense reports](#), [Comm100 Live Chat](#), [SafeConnect](#), [ZenQMS](#), [eLuminate](#), [Dovetale](#).

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Ahora ya está disponible la compatibilidad nativa con Tableau en Azure AD Application Proxy

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Gracias a la actualización del protocolo de concesión de código de OpenID Connect a OAuth 2.0 para nuestro protocolo de autenticación previa, ya no es necesario realizar ninguna configuración adicional para usar Tableau con Application Proxy. Este cambio de protocolo también ayuda a Application Proxy a mejorar su compatibilidad con aplicaciones más modernas mediante el uso exclusivo de redirecciones HTTP, que normalmente son compatibles con las etiquetas de JavaScript y HTML.

Nueva compatibilidad para agregar Google como proveedor de identidades de usuarios invitados de B2B en Azure Active Directory (versión preliminar)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

Mediante la configuración de la federación con Google en su organización, puede permitir que usuarios invitados de Gmail inicien sesión en sus aplicaciones y recursos compartidos con su cuenta de Google existente sin tener

que crear una cuenta Microsoft (MSA) personal o una cuenta de Azure AD.

Se trata de una versión preliminar pública opcional. Para más información sobre la federación con Google, consulte [Incorporación de Google como proveedor de identidades para los usuarios invitados de B2B](#).

Julio de 2018

Mejoras en las notificaciones de Azure Active Directory por correo electrónico

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Administración del ciclo de vida de la identidad

Los correos electrónicos de Azure Active Directory (Azure AD) ahora tienen un diseño actualizado, además de cambios en el nombre para mostrar del remitente y la dirección de correo electrónico del destinatario cuando los mensajes se envían desde los servicios siguientes:

- Revisiones de acceso de Azure AD
- Azure AD Connect Health
- Azure AD Identity Protection
- Administración de identidades con privilegios de Azure AD
- Aplicación empresarial: expiración de las notificaciones de certificado
- Aplicación empresarial: aprovisionamiento de las notificaciones de servicio

Las notificaciones de correo electrónico se enviarán desde la siguiente dirección de correo electrónico y nombre para mostrar:

- Dirección de correo electrónico: azure-noreply@microsoft.com
- Nombre para mostrar: Microsoft Azure

Para un ejemplo de algunos de los nuevos diseños de correo electrónico y más información, consulte [Email notifications in Azure AD PIM](#) (Notificaciones por correo electrónico en Azure AD PIM).

Los registros de actividad de Azure AD ahora están disponibles a través de Azure Monitor

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Los registros de actividad de Azure AD ahora están disponibles en la versión preliminar pública de Azure Monitor (servicio supervisión en toda la plataforma de Azure). Azure Monitor ofrece una retención a largo plazo e integración sin problemas, además de estas mejoras:

- Retención a largo plazo mediante el enrutamiento de los archivos de registro en su propia cuenta de almacenamiento de Azure.
- Integración SIEM perfecta, sin necesidad de escribir o mantener scripts personalizados.
- Integración sin problemas con sus propias soluciones personalizadas, herramientas de análisis o soluciones de administración de incidentes.

Para más información sobre estas nuevas funcionalidades, consulte nuestro blog [Azure AD activity logs in Azure Monitor diagnostics is now in public preview](#) (Los registros de actividad de Azure AD en diagnósticos de Azure Monitor están ahora en versión preliminar pública) y nuestra documentación, [Registros de actividad de Azure AD en Azure Monitor \(versión preliminar\)](#).

Información de acceso condicional agregada al informe de inicio de sesión de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Seguridad y

protección de la identidad

Esta actualización le permite ver qué directivas se evalúan cuando un usuario inicia sesión, junto con el resultado de la directiva. Además, el informe ahora incluye el tipo de aplicación cliente que el usuario utiliza, de manera que usted puede identificar el tráfico de protocolo heredado. Ahora también se pueden buscar entradas de informe para un identificador de correlación, que puede encontrarse en el mensaje de error de cara al usuario y puede usarse para identificar la solicitud de inicio de sesión coincidente y solucionar problemas en dicha solicitud.

Visualización de autenticaciones heredadas a través de los registros de actividad de inicios de sesión

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Con la introducción del campo **Aplicación cliente** en los registros de actividad de inicio de sesión, los clientes ya pueden ver los usuarios que utilizan autenticaciones heredadas. Los clientes podrán acceder a esta información mediante Microsoft Graph API de los registros de inicio de sesión o mediante los registros de actividad de inicio de sesión del portal Azure AD, donde se puede usar el control **Aplicación cliente** para filtrar por autenticaciones heredadas. Para más información, consulte la documentación.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: julio de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En julio de 2018, hemos agregado estas 16 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[Innovation Hub](#), [Leapsome](#), [Certain Admin SSO](#), [PSUC Staging](#), [iPass SmartConnect](#), [Screencast-O-Matic](#), [PowerSchool Unified Classroom](#), [Eli Onboarding](#), [Bomgar Remote Support](#), [Nimblex](#), [Imagineer WebVision](#), [Insight4GRC](#), [SecureW2 JoinNow Connector](#), [Kanbanize](#), [SmartLPA](#) y [Skills Base](#).

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevas integraciones de aplicaciones de SaaS de aprovisionamiento de usuarios: julio de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Integración de terceros

Azure AD permite automatizar la creación, el mantenimiento y la eliminación de identidades de usuario en aplicaciones de SaaS, como Dropbox, Salesforce, ServiceNow, etc. En julio de 2018, hemos agregado compatibilidad con el aprovisionamiento de usuarios a las siguientes aplicaciones de la Galería de aplicaciones de Azure AD:

- [Cisco WebEx](#)
- [Bonusly](#)

Para una lista de todas las aplicaciones que admiten el aprovisionamiento de usuarios en la Galería de Azure AD, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Connect Health para sincronización: una manera más sencilla de corregir errores de sincronización de atributos duplicados o huérfanos

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Supervisión e informes

Azure AD Connect Health presenta la corrección de autoservicio para ayudarle a resaltar y corregir errores de sincronización. Esta característica soluciona los errores de sincronización de atributos duplicados y repara los

objetos huérfanos desde Azure AD. Este diagnóstico tiene las siguientes ventajas:

- Reduce los errores de sincronización de atributos duplicado, proporcionando correcciones específicas
- Aplica una corrección para escenarios de Azure AD dedicados, resolviendo los errores en un solo paso dedicado
- No es necesaria ninguna actualización o configuración para activar y usar esta característica

Para más información, consulte [Diagnóstico y solución de errores de sincronización de atributos duplicados](#).

Actualizaciones de objetos visuales en Azure AD y experiencias de inicio de sesión de MSA

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Azure AD Autenticación de usuarios

Hemos actualizado la interfaz de usuario de la experiencia de inicio de sesión de los servicios en línea de Microsoft, como Office 365 y Azure. Este cambio hace que las pantallas estén menos saturadas y sean más sencillas. Para más información sobre este cambio, consulte el blog [Upcoming improvements to the Azure AD sign-in experience](#) (Próximas mejoras en la experiencia de inicio de sesión de Azure AD).

Nueva versión de Azure AD Connect: julio de 2018

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Administración del ciclo de vida de la identidad

La versión más reciente de Azure AD Connect incluye:

- Correcciones de errores y actualizaciones de compatibilidad
- Disponibilidad general de la integración PingFederate
- Actualizaciones en el cliente más reciente de SQL 2012

Para más información sobre esta actualización, consulte [Azure AD Connect: historial de versiones](#)

Actualizaciones en la interfaz de usuario del usuario final correspondiente a los términos de uso

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Términos de uso Gobernanza

Estamos actualizando la cadena de aceptación en la interfaz de usuario del usuario final correspondiente a las condiciones de uso.

Texto actual. Para acceder a los recursos de [nombrelInquilino], debe aceptar las condiciones de uso.

Nuevo texto. Para acceder al recurso de [nombrelInquilino], debe leer las condiciones de uso.

Texto actual: Si elige Aceptar, significa que acepta todas las condiciones de uso anteriores.

Nuevo texto: Haga clic en Aceptar para confirmar que ha leído y comprendido las condiciones de uso.

La autenticación de paso a través es compatible con las aplicaciones y protocolos heredados

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

La autenticación de paso a través es compatible con las aplicaciones y los protocolos heredados. Ahora se admiten completamente las siguientes limitaciones:

- Inicios de sesión de usuario en las aplicaciones cliente de Office heredadas, Office 2010 y Office 2013, sin necesidad de autenticación moderna.

- Acceso a uso compartido del calendario e información de disponibilidad en entornos híbridos de Exchange solo en Office 2010.
- Inicios de sesión de usuarios en aplicaciones cliente de Skype Empresarial sin necesidad de autenticación moderna.
- Inicios de sesión de usuario en PowerShell 1.0.
- El Programa de inscripción de dispositivos de Apple (DEP de Apple), mediante el Asistente para configuración de iOS.

Administración de información de seguridad convergida para restablecimiento de contraseña de autoservicio y Multi-Factor Authentication

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** SSPR Autenticación de usuarios

Esta nueva característica permite a los usuarios administrar su información de seguridad (por ejemplo, número de teléfono, dirección de correo electrónico, aplicación móvil, etc.) para el restablecimiento de contraseña de autoservicio (SSPR) y Multi-Factor Authentication (MFA) en una sola experiencia. Los usuarios ya no tendrán que registrar la misma información de seguridad para SSPR y MFA en dos experiencias diferentes. Esta nueva experiencia también se aplica a los usuarios que tienen SSPR o MFA.

Si una organización no aplica el registro MFA o SSPR, los usuarios pueden registrar su información de seguridad a través del portal **Mis aplicaciones**. Desde allí, los usuarios pueden registrar los métodos habilitados para MFA o SSPR.

Se trata de una versión preliminar pública opcional. Los administradores pueden activar la nueva experiencia (si lo desean) para un grupo de usuarios seleccionado o para todos los usuarios en un inquilino.

Uso de la aplicación Microsoft Authenticator para verificar su identidad cuando restablezca la contraseña

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** SSPR Autenticación de usuarios

Esta característica permite a los no administradores verificar su identidad al restablecer una contraseña mediante una notificación o un código de Microsoft Authenticator (o cualquier otra aplicación de autenticador). Una vez que los administradores activan este método de restablecimiento de contraseña de autoservicio, los usuarios que hayan registrado una aplicación móvil a través de aka.ms/mfasetup o aka.ms/setupsecurityinfo pueden usar su aplicación móvil como método de verificación al restablecer su contraseña.

La notificación de la aplicación móvil solo se puede activar como parte de una directiva que requiere dos métodos para restablecer la contraseña.

Junio de 2018

Aviso de cambio: Revisión de seguridad para el flujo de autorización delegado para aplicaciones que usan la API de registro de actividad de Azure AD

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Informes Supervisión e informes

Debido a nuestras medidas de seguridad más estrictas, hemos tenido que realizar un cambio en los permisos de las aplicaciones que usan un flujo de autorización delegado para acceder a la [API de registro de actividad de Azure AD](#). Este cambio se producirá el **26 de junio de 2018**.

Si alguna de sus aplicaciones usa la API de registro de actividad de Azure AD, siga estos pasos para asegurarse de que la aplicación no se interrumpa después de que se produzca el cambio.

Para actualizar los permisos de la aplicación

1. Inicie sesión en Azure Portal, seleccione **Azure Active Directory** y, a continuación, **Registros de aplicaciones**.
2. Seleccione la aplicación que usa la API de registro de actividad de Azure AD, seleccione **Configuración**, **Permisos necesarios** y, a continuación, seleccione la API de **Microsoft Azure Active Directory**.
3. En el área **Permisos delegados** de la hoja **Habilitar acceso**, active la casilla junto a **Leer datos de directorio** y seleccione **Guardar**.
4. Haga clic en **Conceder permisos** y, a continuación, haga clic en **Sí**.

NOTE

Debe ser un administrador global para conceder permisos a la aplicación.

Para obtener más información, consulte el área **Conceder permisos** de los requisitos previos para obtener acceso al artículo de la API de generación de informes de Azure AD.

Configuración de las opciones de TLS para conectarse a servicios de Azure AD para el cumplimiento de PCI DSS

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** N/D Plataforma

La Seguridad de la capa de transporte (TLS) es un protocolo que proporciona privacidad e integridad de datos para la comunicación entre dos aplicaciones, y es el protocolo de seguridad más implementado hoy en día.

El [PCI Security Standards Council](#) (Consejo de estándares de seguridad de PCI) ha determinado que las versiones anteriores de TLS y Capa de sockets seguros (SSL) deben deshabilitarse para habilitar protocolos de aplicaciones nuevos y más seguros, con el inicio del cumplimiento a partir del **30 de junio 2018**. Este cambio significa que, si se conecta a servicios de Azure AD y es necesario el cumplimiento con PCI DSS, deberá deshabilitar TLS 1.0. Hay varias versiones de TLS disponibles, pero TLS 1.2 es la más reciente para servicios de Azure Active Directory. Se recomienda encarecidamente moverse directamente a TLS 1.2 para las combinaciones de cliente/servidor y explorador/servidor.

Es posible que los exploradores obsoletos no admitan las versiones más recientes de TLS, como TLS 1.2. Para ver qué versiones de TLS son compatibles con el explorador, vaya al sitio de [Qualys SSL Labs](#) y haga clic en **Test your browser** (Probar el explorador). Le recomendamos que actualice a la versión más reciente del explorador web y, si es posible, que habilite solo TLS 1.2.

Para habilitar TLS 1.2 por explorador

- **Microsoft Edge e Internet Explorer** (ambos se establecen mediante Internet Explorer)
 1. Abra Internet Explorer, seleccione **Herramientas > Opciones de Internet > Opciones avanzadas**.
 2. En el área de **Seguridad**, seleccione **use TLS 1.2** (usar TLS 1.2) y, a continuación, seleccione **Aceptar**.
 3. Cierre todas las ventanas del explorador y reinicie Internet Explorer.
- **Google Chrome**
 1. Abra Google Chrome, escriba *chrome://settings/* en la barra de direcciones y presione **ENTRAR**.
 2. Expanda la **Configuración avanzada**, vaya al área de **Sistema** y seleccione **Abrir la configuración de proxy**.
 3. En el cuadro **Propiedades: Internet**, seleccione la pestaña **Opciones avanzadas**, vaya al área de **Seguridad**, seleccione **Usar TLS 1.2** y, a continuación, seleccione **Aceptar**.
 4. Cierre todas las ventanas del explorador y reinicie Google Chrome.
- **Mozilla Firefox**
 1. Abra Firefox, escriba *about:config* en la barra de direcciones y, a continuación, presione **ENTRAR**.

2. Busque el término *TLS* y, a continuación, seleccione la entrada **security.tls.version.max**.
3. Establezca el valor en 3 para forzar al explorador a usar hasta la versión TLS 1.2 y, a continuación, seleccione **Aceptar**.

NOTE

La versión de Firefox 60.0 admite TLS 1.3, por lo que también puede establecer el valor de **security.tls.version.max** en 4.

4. Cierre todas las ventanas del explorador y reinicie Mozilla Firefox.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: junio de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En junio de 2018, hemos agregado estas 15 nuevas aplicaciones con compatibilidad con la federación para la galería de aplicaciones:

[Skytap](#), [Settling music](#), aplicación de LOB con el token SAML 1.1 habilitado, [Supermood](#), [Autotask](#), [Endpoint Backup](#), [Skyhigh Networks](#), [Smartway2](#), [TonicDM](#), [Moconavi](#), [Zoho One](#), [SharePoint local](#), [ForeSee CX Suite](#), [Vidyard](#) y [ChronicX](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#). Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

La Protección con contraseña de Azure AD está disponible en versión preliminar pública.

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Autenticación de usuarios

Use la Protección con contraseña de Azure AD para ayudar a eliminar de su entorno las contraseñas que se pueden averiguar fácilmente. Al eliminar estas contraseñas, ayuda a reducir el riesgo de un tipo de ataque de difusión de contraseña.

En concreto, la Protección con contraseña de Azure AD:

- Le ayuda a proteger las cuentas de la organización en Azure AD y Windows Server Active Directory (AD).
- Impide que los usuarios usen las contraseñas de una lista que incluye más de 500 de las contraseñas utilizadas con más frecuencia y más de un millón de variaciones de sustitución de caracteres de esas contraseñas.
- Le ayuda a administrar la Protección con contraseña de Azure AD desde una única ubicación en el portal de Azure AD, tanto para Azure AD como para Windows Server AD local.

Para obtener más información acerca de la Protección con contraseña de Azure AD, consulte [Elimine las contraseñas incorrectas de su organización](#).

Nueva plantilla "todos los invitados" de la directiva de acceso condicional creada durante la creación de los términos de uso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Gobernanza

Durante la creación de los términos de uso, también se ha creado una nueva plantilla de la directiva de acceso condicional para "todos los invitados" y "todas las aplicaciones". Esta nueva plantilla de la directiva se aplica a los Términos de uso recién creados, lo que facilita el proceso de cumplimiento y creación para los invitados.

Para obtener más información, consulte [Característica Azure Active Directory Terms of Use](#).

Nueva plantilla "personalizado" de la directiva de acceso condicional creada durante la creación de los términos de uso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Gobernanza

Durante la creación de los términos de uso, también se ha creado una nueva plantilla "personalizada" de la directiva de acceso condicional. Esta nueva plantilla de la directiva le permite crear los términos de uso y luego pasar inmediatamente a la hoja de creación de la directiva de acceso condicional, sin necesidad de navegar por el portal de forma manual.

Para obtener más información, consulte [Característica Azure Active Directory Terms of Use](#).

Guía nueva y completa acerca de cómo implementar Azure Multi-Factor Authentication

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Otros Seguridad y protección de la identidad

Hemos lanzado la nueva guía paso a paso acerca de cómo implementar Azure Multi-Factor Authentication (MFA) en su organización.

Para ver la guía de implementación de MFA, vaya al repositorio [Guías de implementación de identidad](#) en GitHub.

Para enviar comentarios acerca de las guías de implementación, use el [formulario Comentarios del plan de implementación](#). Si tiene alguna pregunta acerca de las guías de implementación, póngase en contacto con nosotros en [IDGitDeploy](#).

Los roles de administración de aplicaciones delegadas de Azure AD están en versión preliminar pública.

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Control de acceso

Ahora los administradores pueden delegar tareas de administración de aplicaciones sin asignar el rol de administrador global. Los nuevos roles y funcionalidades son:

- **Nuevos roles de administrador de Azure AD estándar:**
 - **Administrador de aplicaciones** Concede la capacidad de administrar todos los aspectos de todas las aplicaciones, incluidos el registro, la configuración de SSO, las asignaciones de aplicaciones y licencias, la configuración del proxy de aplicación y el consentimiento (excepto para los recursos de Azure AD).
 - **Administrador de aplicaciones en la nube** Concede todas las capacidades de administrador de aplicaciones, excepto para el proxy de aplicación porque no proporciona acceso local.
 - **Desarrollador de aplicaciones** Concede permisos para crear registros de aplicaciones, incluso si está desactivada la opción **allow users to register apps** (permitir a los usuarios registrar aplicaciones).
- **Propiedad (configurar el registro por aplicación y la aplicación por empresa, similar al proceso de la propiedad de grupo):**
 - **Propietario de registro de aplicaciones** Concede la capacidad de administrar todos los aspectos del registro de aplicaciones en propiedad, incluidos el manifiesto de la aplicación y la adición de más propietarios.
 - **Propietario de aplicaciones empresariales** Concede la capacidad de administrar muchos aspectos de las aplicaciones empresariales en propiedad, incluidos el consentimiento, la configuración de SSO y las asignaciones de aplicaciones (excepto para los recursos de Azure AD).

Para obtener más información acerca de la versión preliminar pública, consulte el blog [Azure AD delegated application management roles are in public preview!](#) (Los roles de administración de aplicaciones delegadas de Azure AD están en versión preliminar pública).. Para obtener más información acerca de los roles y permisos, consulte [Assigning administrator roles in Azure Active Directory](#) (Asignación de roles de administrador en Azure Active Directory).

Mayo de 2018

Cambios de soporte técnico de ExpressRoute

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Plataforma

Las ofertas de software como servicio, como Azure Active Directory (Azure AD) están diseñadas para funcionar mejor a través de Internet, sin necesidad de ExpressRoute ni otros túneles VPN privados. Por este motivo, en **1 de agosto de 2018**, dejaremos de dar soporte técnico a ExpressRoute para los servicios de Azure AD que usen un emparejamiento público de Azure y a las comunidades de Azure que usen emparejamientos de Microsoft. Los servicios afectados por este cambio podrían observar que el tráfico de Azure AD gradualmente cambia de ExpressRoute a Internet.

Aunque vamos a cambiar el soporte, también sabemos que aún hay situaciones en las que tendrá que utilizar un conjunto de circuitos dedicado para el tráfico de autenticación. Por este motivo, Azure AD seguirá admitiendo restricciones de intervalos de IP por inquilino utilizando ExpressRoute y los servicios que ya tienen emparejamiento de Microsoft con la comunidad "Otros servicios en línea de Office 365". Si los servicios se ven afectados pero requieren ExpressRoute, debe hacer lo siguiente:

- **Si está en un emparejamiento público de Azure.** Cambie a un emparejamiento de Microsoft y suscríbase a la comunidad [Otros servicios en línea de Office 365 \(12076:5100\)](#) . Para más información sobre cómo cambiar de emparejamiento público de Azure a emparejamiento de Microsoft, consulte el artículo [Cambiar un emparejamiento público a emparejamiento de Microsoft](#).
- **Si está en un emparejamiento de Microsoft.** Suscríbase a la comunidad [Otros servicio en línea de Office 365 \(12076:5100\)](#) . Para más información sobre los requisitos de enrutamiento, consulte la sección [Soporte técnico para las comunidades de BGP](#) en el artículo de requisitos de enrutamiento de ExpressRoute.

Si debe continuar usando circuitos dedicados, deberá hablar con el equipo de su cuenta Microsoft acerca de cómo obtener autorización para utilizar la comunidad [Otros servicios en línea de Office 365 \(12076:5100\)](#) . El comité de revisión administrado por MS Office comprobará si necesita los circuitos y se asegurará de que comprende las implicaciones técnicas de su conservación. Las suscripciones no autorizadas que intenten crear filtros de ruta para Office 365 recibirán un mensaje de error.

Microsoft Graph API para escenarios administrativos de términos de uso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Experiencia para el desarrollador

Hemos agregado Microsoft Graph API para el funcionamiento de la administración de los términos de uso de Azure AD. Puede crear, actualizar y eliminar el objeto de términos de uso.

Agregar punto de conexión multiinquilino de Azure AD como proveedor de identidades en Azure AD B2C

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Con las directivas personalizadas, ahora puede agregar el punto de conexión común de Azure AD como proveedor de identidades en Azure AD B2C. Esto le permite tener un único punto de entrada para todos los usuarios de Azure

AD que inician sesión en sus aplicaciones. Para más información, consulte [Azure Active Directory B2C: Permitir que los usuarios inicien sesión en un proveedor de identidades de Azure AD multiinquilino mediante directivas personalizadas](#).

Uso de direcciones URL internas para acceder a aplicaciones desde cualquier lugar con My Apps Sign-in Extension y Azure AD Application Proxy

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones SSO

Los usuarios ya pueden acceder a las aplicaciones a través de direcciones URL internas, incluso desde fuera de la red corporativa, mediante My Apps Sign-in Extension para Azure AD. Esto funcionará con todas las aplicaciones que se ha publicado con Azure Active Directory Application Proxy, en cualquier explorador que también tenga instalada la extensión de explorador del Panel de acceso. La funcionalidad de redirección de direcciones URL se habilita automáticamente una vez que un usuario inicia sesión en la extensión. La extensión se puede descargar en [Microsoft Edge](#), [Chrome](#) y [Firefox](#).

Azure Active Directory: datos en Europa para los clientes europeos

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Otros GoLocal

Los clientes de Europa requieren que sus datos se queden en Europa y no se repliquen fuera de los centros de datos europeos para proteger la privacidad y cumplir la legislación europea. En este [artículo](#) se proporcionan detalles concretos no solo acerca de qué información de identidad se almacenará en Europa, sino también acerca de la que se almacenará fuera de los centros de datos europeos.

Nuevas integraciones de aplicaciones de SaaS de aprovisionamiento de usuarios: mayo de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Integración de terceros

Azure AD permite automatizar la creación, el mantenimiento y la eliminación de identidades de usuario en aplicaciones de SaaS, como Dropbox, Salesforce, ServiceNow, etc. En mayo de 2018, hemos agregado compatibilidad con el aprovisionamiento de usuarios a las siguientes aplicaciones de la Galería de aplicaciones de Azure AD:

- [BlueJeans](#)
- [Cornerstone OnDemand](#)
- [Zendesk](#)

Para obtener una lista de todas las aplicaciones que admiten el aprovisionamiento de usuarios en la Galería de Azure AD, consulte <https://aka.ms/appstutorial>.

Ahora, las revisiones de acceso de Azure AD de grupos y aplicaciones proporcionan revisiones periódicas

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Revisiones de acceso Gobernanza

La revisión de acceso de grupos y aplicaciones ya está disponible de forma generalizada como parte de Azure AD Premium P2. Los administradores podrán configurar las revisiones de acceso de los miembros de un grupo y las asignaciones de aplicaciones para que se repitan automáticamente a intervalos periódicos; por ejemplo, cada mes o cada trimestre.

Los registros de actividad de Azure AD (inicios de sesión y auditoría) ahora están disponibles a través de MS Graph

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Los registros de actividad de Azure AD, que incluyen los registros inicios de sesión y de auditorías, ahora están disponibles a través de Microsoft Graph API. Para acceder a dichos registros se han expuesto dos puntos de conexión a través de Microsoft Graph API. Consulte nuestros [documentos](#) para ver cómo acceder mediante programación a las API de informes de Azure AD.

Mejoras en la experiencia de canje de invitaciones B2B y en el abandono de una organización

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

Canje justo a tiempo: una vez que se comparte un recurso con un usuario invitado con la API B2B, no es preciso enviar un correo electrónico de invitación especial. En la mayoría de los casos, el usuario invitado puede acceder al recurso y pasar por la experiencia de canje justo a tiempo. Se acabaron los problemas por mensajes de correo electrónico perdidos. Se acabó preguntar a los usuarios invitados: "¿Ha hecho clic en el vínculo de canje que le envió el sistema?". Esto significa que una vez que la SPO utiliza el administrador de invitaciones, los elementos adjuntos de la nube pueden tener la misma dirección URL canónica para todos los usuarios, tanto internos como externos, con cualquier estado de canje.

Experiencia de canje moderna: se acabaron las páginas de aterrizaje para el canje con pantalla dividida. Los usuarios verán un consentimiento moderno con la declaración de privacidad de la organización que realiza la invitación, igual que en las aplicaciones de terceros.

Los usuarios invitados pueden abandonar la organización: Cuando termina la relación de un usuario con una organización, este puede salir de ella sin ayuda de nadie. No será preciso pedir al administrador de la organización que le invitó que lo "elimine" ni necesitará generar incidencias de soporte técnico.

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD: mayo de 2018

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En mayo de 2018, hemos agregado estas 18 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[AwardSpring](#), [Infogix Data3Sixty Govern](#), [Yodeck](#), [Jamf Pro](#), [KnowledgeOwl](#), [Envi MMIS](#), [LaunchDarkly](#), [Adobe Captivate Prime](#), [Montage Online](#), [まなびポケット](#), [OpenReel](#), [Arc Publishing - SSO](#), [PlanGrid](#), [iWellnessNow](#), [Proxyclick](#), [Riskware](#), [Flock](#), [Reviewsnap](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Nuevas guías de implementación paso a paso para Azure Active Directory

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Otros Directorio

Novedad: guía paso a paso sobre cómo implementar Azure Active Directory (Azure AD), incluido el autoservicio de restablecimiento de contraseña (SSPR), el inicio de sesión único (SSO), el acceso condicional (CA), el proxy de aplicación, el aprovisionamiento de usuarios, los Servicios de federación de Active Directory (AD FS) en Autenticación de paso a través (PTA) y ADFS para realizar la sincronización de hash de contraseña (PBS).

Para ver las guías de implementación, vaya al repositorio [Guías de implementación de identidad](#) en GitHub. Para enviar comentarios acerca de las guías de implementación, use el [formulario Comentarios del plan de implementación](#). Si tiene alguna pregunta acerca de las guías de implementación, póngase en contacto con nosotros en [IDGitDeploy](#).

Búsqueda de aplicaciones empresariales: cargar más aplicaciones

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

¿No consigue encontrar aplicaciones o entidades de servicio? Hemos agregado la posibilidad de cargar más aplicaciones en la lista de todas las aplicaciones empresariales. De manera predeterminada, se muestran 20 aplicaciones. Ahora puede hacer clic en **Cargar más** y ver otras aplicaciones.

La versión de mayo de AADConnect contiene una versión preliminar pública de la integración con PingFederate, actualizaciones de seguridad importantes, muchas correcciones de errores y nuevas y magníficas herramientas para la solución de problemas.

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Administración del ciclo de vida de la identidad

La versión de mayo de AADConnect contiene una versión preliminar pública de la integración con PingFederate, actualizaciones de seguridad importantes, muchas correcciones de errores y nuevas y magníficas herramientas para la solución de problemas. Puede encontrar las notas de la versión [aquí](#).

Revisões de acceso de Azure AD: aplicación automática

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Revisiones de acceso Gobernanza

Las revisiones de acceso de grupos y aplicaciones ahora están disponibles de forma generalizada como parte de Azure AD Premium P2. Un administrador puede realizar la configuración necesaria para aplicar automáticamente los cambios del revisor a un grupo o aplicación cuando se complete la revisión de acceso. El administrador también puede especificar lo que ocurre al acceso continuado del usuario si los revisores no responden: quitar el acceso, mantener el acceso o seguir las recomendaciones del sistema.

Los tokens de identificador no se pueden devolver mediante el valor de response_mode de una consulta en las nuevas aplicaciones.

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Las aplicaciones creadas a partir del 25 de abril de 2018 ya no podrán solicitar un valor de **id_token** mediante el argumento **response_mode** de **query**. De esta forma, Azure AD se alinea con las especificaciones de OIDC y se reduce la superficie de ataque de sus aplicaciones. No se impide que las aplicaciones creadas antes del 25 de abril de 2018 utilicen el argumento **response_mode** de **query** con un valor de **response_type** de **id_token**. El error que se devuelve al solicitar un **id_token** de AAD es **AADSTS70007: "query" no es un valor de "response_mode" que se admite al solicitar un token**.

Los valores de **response_mode fragment** y **form_post** siguen funcionando (al crear nuevos objetos de aplicación [por ejemplo, para el uso de proxy de aplicación]). Asegúrese de usar uno de estos valores de **response_mode** antes de que creen una aplicación nueva.

Abril de 2018

Los tokens de acceso de Azure AD B2C son GA

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Ya puede acceder a las API web que protege Azure AD B2C gracias a los tokens de acceso. Esta característica está pasando de la versión preliminar pública a la versión de disponibilidad general. A parte de otras mejoras menores, también se ha mejorado la experiencia de interfaz de usuario para configurar las aplicaciones de Azure AD B2C y las API web.

Para más información, consulte [Azure AD B2C: Solicitud de tokens de acceso](#).

Probar la configuración del inicio de sesión único para aplicaciones basadas en SAML

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Al configurar las aplicaciones SSO basadas en SAML, puede probar la integración en la página de configuración. Si se produce un error durante el inicio de sesión, puede proporcionar dicho error en la experiencia de prueba y Azure AD le proporcionará los pasos para resolver ese problema.

Para más información, consulte:

- [Configuración del inicio de sesión único en aplicaciones que no están en la Galería de aplicaciones de Azure Active Directory](#)
 - [Cómo depurar el inicio de sesión único basado en SAML en aplicaciones de Azure Active Directory](#)
-

Los términos de uso de Azure AD ahora tienen informes por usuario

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Los administradores pueden seleccionar una versión determinada de los Términos de uso y ver qué usuarios han dado su consentimiento y en qué fecha y hora.

Para obtener más información, consulte [Azure AD terms of use feature](#) (Característica de términos de uso de Azure AD).

Azure AD Connect Health: Direcciones IP de riesgo para la protección de bloqueo de extranet de AD FS

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Otros Supervisión e informes

Connect Health ahora tiene la capacidad de detectar direcciones IP que superan un umbral de inicios de sesión de U/P erróneos por hora o por día. Estas son las funcionalidades que proporciona esta característica:

- Un informe completo que muestra la dirección IP y el número de inicios de sesión erróneos generados por hora o por día y con un umbral personalizable.
- Alertas basadas en el correo electrónico que muestran el momento en que una dirección IP específica excede el umbral de inicios de sesión de U/P erróneos por hora o por día.
- Una opción de descarga para realizar un análisis detallado de los datos.

Para obtener más información, consulte [Informe de direcciones IP de riesgo](#).

Configuración sencilla de aplicaciones mediante una dirección URL o un archivo de metadatos

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

En la página de aplicaciones Enterprise, los administradores pueden cargar un archivo de metadatos SAML para configurar el inicio de sesión basado en SAML tanto de las aplicaciones de la galería de AAD, como de las que no pertenecen a la galería.

Asimismo, puede usar la dirección URL de metadatos de la federación de aplicaciones de Azure AD para configurar el SSO con la aplicación de destino.

Para obtener más información, consulte [Configuring single sign-on to applications that are not in the Azure Active Directory application gallery](#) (Configurar el inicio de sesión único de las aplicaciones que no forman parte de la galería de aplicaciones de Azure Active Directory).

Los Términos de uso de Azure AD están disponibles de forma general

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Los términos de uso de Azure AD han dejado de estar en versión preliminar pública y ahora están disponibles de forma general.

Para obtener más información, consulte [Azure AD terms of use feature](#) (Característica de términos de uso de Azure AD).

Permitir o bloquear invitaciones a usuarios B2B procedentes de determinadas organizaciones

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

Ya puede especificar con qué organizaciones de socio quiere compartir contenido y colaborar en Azure AD B2B Collaboration. Para hacer esto, puede elegir crear una lista de dominios específicos para otorgar permiso o denegarlo. Cuando se bloquea un dominio mediante estas funcionalidades, los empleados ya no pueden enviar invitaciones a los usuarios de ese dominio.

Esto le ayudará a controlar el acceso a los recursos, a la vez que ofrece una experiencia fluida a los usuarios aprobados.

La característica Colaboración B2B está disponible para todos los clientes de Azure Active Directory y se puede usar con las características de Azure AD Premium, como el acceso condicional y la protección de identidad, para saber al detalle cómo y cuándo inician sesión y obtienen acceso los usuarios comerciales externos.

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).

Nuevas aplicaciones federadas disponibles en la galería de aplicaciones de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En abril de 2018, hemos agregado estas 13 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

Criterion HCM, [FiscalNote](#), [Secret Server \(local\)](#), [Dynamic Signal](#), [mindWireless](#), [OrgChart Now](#), [Ziflow](#), [AppNeta Performance Monitor](#), [Elium](#), [Fluxx Labs](#), [Cisco Cloud Shelf](#), [SafetyNet](#)

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Conceder a los usuarios de B2B en Azure AD acceso a las aplicaciones locales (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2B B2B/B2C

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).

Para obtener más información, consulte [Conceder a los usuarios de B2B en Azure AD acceso a las aplicaciones locales](#).

Obtener tutoriales de integración de SSO en Azure Marketplace

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Otros Integración de terceros

Si una aplicación incluida en [Azure Marketplace](#) admite el proceso de inicio de sesión único basado en SAML, al hacer clic en **Obtener ahora** se proporciona el tutorial de integración asociado a esa aplicación.

Rendimiento más rápido del aprovisionamiento de usuarios automático de Azure AD para aplicaciones SaaS

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Integración de terceros

Anteriormente, los clientes que utilizaban los conectores de aprovisionamiento de usuarios de Azure Active Directory para aplicaciones de SaaS (por ejemplo, Salesforce, ServiceNow y Box) podían experimentar un rendimiento lento si sus inquilinos de Azure AD contenían más de 100 000 usuarios y grupos combinados, y si usaban asignaciones de usuarios y grupos para determinar qué usuarios debían aprovisionarse.

El 2 de abril de 2018 se implementaron mejoras de rendimiento significativas en el servicio de aprovisionamiento de Azure AD que reducen en gran medida la cantidad de tiempo necesario para realizar las sincronizaciones iniciales entre Azure Active Directory y las aplicaciones de SaaS de destino.

Como resultado, ahora se completan en cuestión de minutos u horas sincronizaciones iniciales que muchos clientes realizaban en sus aplicaciones y que antes tardaban días en completarse o que nunca llegaban a completarse.

Para obtener más información, consulte [¿Qué ocurre durante el aprovisionamiento?](#)

Restablecimiento de contraseña de autoservicio desde la pantalla de bloqueo de Windows 10 para máquinas híbridas unidas a Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Autenticación de usuarios

Hemos actualizado la característica SSPR de Windows 10 para incluir soporte técnico para máquinas híbridas que se hayan unido a Azure AD. Esta característica está disponible en Windows 10 RS4 y permite a los usuarios restablecer la contraseña en la pantalla de bloqueo de una máquina Windows 10. Los usuarios que están habilitados y registrados para poder realizar el restablecimiento de contraseña de autoservicio pueden utilizar esta característica.

Para obtener más información, consulte [Azure AD password reset from the login screen](#) (Restablecer la contraseña de Azure AD desde la pantalla de inicio de sesión).

Marzo de 2018

Notificación de expiración de certificado

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Aplicaciones empresariales SSO

Azure AD envía una notificación cuando un certificado de una aplicación incluida o no en una galería está a punto de expirar.

Algunos usuarios no recibían notificaciones sobre aplicaciones empresariales configuradas con el inicio de sesión único basado en SAML. Este problema se ha resuelto. Azure AD envía una notificación para los certificados que expiran en 7, 30 y 60 días. Este evento puede verse en los registros de auditoría.

Para más información, consulte:

- [Administrar certificados para inicio de sesión único federado en Azure Active Directory](#)

- [Informes de actividad de auditoría en el portal de Azure Active Directory](#)
-

Proveedores de identidades de Twitter y GitHub en Azure AD B2C

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** B2C: administración de identidades de consumidor B2B/B2C

Ahora, puede agregar Twitter o GitHub como proveedores de identidades en Azure AD B2C. Twitter está pasando de la versión preliminar pública a la versión de disponibilidad general. GitHub se va a publicar en la versión preliminar pública.

Para más información, consulte [¿Qué es la colaboración B2B de Azure AD?](#)

Restricción del acceso de explorador mediante Intune Managed Browser con acceso condicional basado en aplicaciones de Azure AD para iOS y Android

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Acceso condicional Seguridad y protección de la identidad

Ahora en versión preliminar pública

SSO de Intune Managed Browser: los empleados pueden utilizar el inicio de sesión único por los clientes nativos (por ejemplo, Microsoft Outlook) e Intune Managed Browser para todas las aplicaciones de Azure AD conectados.

Compatibilidad con el acceso condicional de Intune Managed Browser: ahora puede requerir que los empleados usen Intune Managed Browser mediante directivas de acceso condicional basado en aplicaciones.

Lea más sobre esto en nuestra [entrada de blog](#).

Para más información, consulte:

- [Configuración del acceso condicional basado en aplicaciones](#)
 - [Configuración de directivas de Managed Browser](#)
-

Cmdlets del proxy de aplicación en el módulo de disponibilidad general de PowerShell

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Control de acceso

Ahora, los cmdlets del proxy de aplicación pueden utilizarse en el módulo de disponibilidad general de PowerShell. Es necesario mantener actualizados los módulos de PowerShell; si lleva más de un año de retraso, es posible que algunos cmdlets dejen de funcionar.

Para más información, consulte [AzureAD](#).

Los clientes nativos de Office 365 son compatibles con SSO de conexión directa utilizando un protocolo no interactivo

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Los usuarios que utilizan clientes nativos de Office 365 (versión 16.0.8730.xxxx y posteriores) pueden iniciar sesión sin que sea necesaria su intervención mediante SSO de conexión directa. Esta funcionalidad es posible gracias a la incorporación de un protocolo no interactivo (WS-Trust) en Azure AD.

Para más información, consulte [¿Cómo funciona el inicio de sesión en un cliente nativo con SSO de conexión directa?](#)

Con SSO de conexión directa, no es necesaria la intervención del usuario para iniciar sesión cuando una aplicación envía solicitudes de inicio de sesión a puntos de conexión de inquilinos de Azure AD.

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Con el inicio de sesión único de conexión directa, los usuarios no necesitan intervenir para iniciar sesión si una aplicación (por ejemplo, <https://contoso.sharepoint.com>) envía solicitudes de inicio de sesión a puntos de conexión de inquilinos de Azure AD (por ejemplo, <https://login.microsoftonline.com/contoso.com/<...>> o https://login.microsoftonline.com/<tenant_ID>/<...>), en lugar de a puntos de conexión comunes de Azure AD (<https://login.microsoftonline.com/common/<...>>).

Para más información, consulte [Inicio de sesión único de conexión directa de Azure Active Directory](#).

Solo es necesario agregar una dirección URL de Azure AD, en lugar de las dos que se requerían anteriormente, en la configuración de la zona de intranet de los usuarios para activar el SSO de conexión directa

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Si desea activar el SSO de conexión directa para los usuarios, solo debe agregar una dirección URL de Azure AD en la configuración de la zona de intranet de los usuarios utilizando una directiva de grupo de Active Directory:

<https://autologon.microsoftazuread-sso.com>. Anteriormente, era necesario que los clientes agregaran dos direcciones URL.

Para más información, consulte [Inicio de sesión único de conexión directa de Azure Active Directory](#).

Nuevas aplicaciones federadas disponibles en la Galería de aplicaciones de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En abril de 2018, hemos agregado estas 15 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[Boxcryptor](#), [CylancePROTECT](#), [Wrike](#), [SignalFx](#), [Assistant by FirstAgenda](#), [YardiOne](#), [Vtiger CRM](#), [inwink](#), [Amplitude](#), [Spacio](#), [ContractWorks](#), [Bersin](#), [Mercell](#), [Trisotech Digital Enterprise Server](#) y [Qumu Cloud](#).

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

PIM de Azure Resources está disponible con carácter general

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

Si utiliza Azure AD Privileged Identity Management para los roles de directorio, ahora puede utilizar las funcionalidades de asignación y acceso con límite de tiempo de PIM con los roles de Recursos de Azure, como Suscripciones, Grupos de recursos, Máquinas virtuales y cualquier otro recurso compatible con Azure Resource Manager. Puede forzar la aplicación de la autenticación multifactor al activar roles Just-In-Time y programar activaciones de forma coordinada con los períodos de cambio aprobados. Además, esta versión incorpora mejoras que no están disponibles en la versión preliminar pública, como una interfaz de usuario actualizada, flujos de trabajo de aprobación y la capacidad de ampliar roles que van a expirar en breve y de renovar roles que han expirado.

Para obtener más información, consulte [PIM para recursos de Azure \(versión preliminar\)](#).

Incorporación de notificaciones opcionales en los tokens de aplicaciones (versión preliminar pública)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Ahora, las aplicaciones de Azure AD pueden solicitar notificaciones personalizadas u opcionales en los tokens SAML o JWT. Estas notificaciones sobre el usuario o el inquilino no se incluyen de forma predeterminada en el token por restricciones de tamaño o aplicabilidad. Actualmente, esta funcionalidad está en versión preliminar pública para las aplicaciones de Azure AD de los puntos de conexión 1.0 y 2.0. Consulte la documentación para obtener información acerca de qué notificaciones pueden agregarse y cómo editar el manifiesto de aplicación para solicitarlas.

Para más información, consulte [Optional claims in Azure AD](#) (Notificaciones opcionales de Azure AD)///.

Azure AD permite usar PKCE para disponer de flujos de OAuth más seguros

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Los documentos de Azure AD se han actualizado para que tengan en cuenta la compatibilidad con PKCE, lo que permite una comunicación más segura durante el flujo de concesión del código de autorización de OAuth 2.0. Los puntos de conexión de la versión 1.0 y 2.0 admiten S256 y code_challenges de texto no cifrado.

Para más información, consulte [Solicitud de un código de autorización](#).

Compatibilidad con el aprovisionamiento de todos los valores de atributo de usuario disponibles en Workday Get_Workers API

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aprovisionamiento de aplicaciones Integración de terceros

Ahora, la versión preliminar pública de aprovisionamiento de entrada de Workday a Active Directory y Azure AD permite extraer y aprovisionar todos los valores de atributo disponibles en Workday Get_Workers API. De este modo, se amplía la compatibilidad con cientos de atributos estándar y personalizados, que se suman a los que ya venían con la versión inicial del conector de aprovisionamiento de entrada de Workday.

Para más información, consulte: [Personalización de la lista de atributos de usuario de Workday](#)

Cambio de la pertenencia a grupos de dinámica a estática, y viceversa

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de grupos Colaboración

Es posible cambiar cómo se administra la pertenencia a un grupo. Esto es útil cuando desea mantener el mismo nombre de grupo y el identificador en el sistema, por lo que cualquier referencia existente al grupo sigue siendo válida; crear un nuevo grupo requeriría actualizar esas referencias. Hemos actualizado el centro de administración de Azure AD para incorporar la compatibilidad con esta funcionalidad. Ahora, los clientes pueden cambiar los grupos existentes para que tengan una pertenencia dinámica en lugar de una pertenencia asignada, y viceversa. Los cmdlets de PowerShell existentes seguirán estando disponibles.

Para obtener más información, consulte [Reglas de pertenencia dinámica a grupos de Azure Active Directory](#).

Comportamiento de cierre de sesión mejorado con SSO de conexión directa

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Anteriormente, aunque los usuarios cerraran sesión explícitamente en una aplicación protegida con Azure AD, la sesión se iniciaba de nuevo automáticamente mediante SSO de conexión directa si intentaban volver a acceder a una aplicación de Azure AD en la red corporativa desde los dispositivos unidos al dominio. Con este cambio, se

puede cerrar sesión. De este modo, los usuarios pueden elegir otra cuenta de Azure AD al iniciar sesión de nuevo, en lugar de la que la sesión se inicie automáticamente con el SSO de conexión directa.

Para más información, consulte [Inicio de sesión único de conexión directa de Azure Active Directory](#).

Se ha publicado la versión 1.5.402.0 del conector del proxy de aplicación

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Proxy de aplicaciones Seguridad y protección de la identidad

Esta versión del conector se irá implementando gradualmente hasta noviembre. Esta nueva versión del conector incluye los siguientes cambios:

- Ahora, el conector establece cookies de nivel de dominio en lugar de cookies de nivel de subdominio. De este modo, la experiencia de SSO resulta más fluida y se evita el envío de peticiones de autenticación redundantes.
- Se admiten solicitudes de codificación fragmentada.
- Se ha mejorado la supervisión del mantenimiento del conector.
- Se han solucionado algunos errores y se han hecho mejoras en la estabilidad.

Para más información, consulte [Descripción de los conectores de Azure Active Directory Application Proxy](#).

Febrero de 2018

Navegación mejorada para administrar usuarios y grupos

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Administración de directorios Directorio

Se ha simplificado la experiencia de navegación para administrar usuarios y grupos. Ahora puede ir directamente desde la información general del directorio a la lista de todos los usuarios, con un acceso más fácil a la lista de usuarios eliminados. Ahora puede ir directamente desde la información general del directorio a la lista de todos los grupos, con un acceso más fácil a la configuración de administración de grupos. Y también en la página de información general del directorio puede buscar un usuario, grupo, aplicación empresarial o registro de la aplicación.

Disponibilidad de los informes de inicios de sesión y auditoría en Microsoft Azure controlado por 21Vianet (Azure China 21Vianet)

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure Stack Supervisión e informes

Los informes de registro de actividad de Azure AD ya están disponibles en Microsoft Azure controlado por instancias de 21Vianet (Azure China 21Vianet). Se incluyen los siguientes registros:

- **Registros de actividad de inicios de sesión:** incluye todos los registros de inicios de sesión asociados con el inquilino.
- **Registros de auditoría de contraseñas de autoservicio:** incluye todos los registros de auditoría de SSPR.
- **Registros de auditoría de administración de directorios:** incluye todos los registros de auditoría relacionados con la administración de directorios como, por ejemplo, administración de usuarios, administración de aplicaciones y otros.

Con estos registros, puede obtener información detallada sobre el funcionamiento de su entorno. Los datos proporcionados le permiten:

- Determinar cómo utilizan los usuarios las aplicaciones y servicios.

- Solucionar problemas que impiden a los usuarios finalizar su trabajo.

Para más información sobre cómo usar estos informes, consulte [Informes de Azure Active Directory](#).

Use el rol "Lector de informes" (rol que no es de administrador) para ver los informes de actividad de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Informes Supervisión e informes

Como parte de los comentarios de los clientes para habilitar los roles que no son de administrador para acceder a los registros de actividades de Azure AD, hemos habilitado la posibilidad de que los usuarios con el rol "Lector de informes" puedan acceder a las actividades de inicio de sesión y de auditoría en Azure Portal, así como mediante Microsoft Graph API.

Para más información sobre cómo usar estos informes, consulte [Informes de Azure Active Directory](#).

Notificación de EmployeeID disponible como atributo de usuario e identificador de usuario

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales SSO

Puede configurar **EmployeeID** como el identificador de usuario y el atributo de usuario para los usuarios miembros y para los invitados B2B en aplicaciones de inicio de sesión basadas en SAML desde la interfaz de usuario de la aplicación empresarial.

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

Administración simplificada de aplicaciones mediante caracteres comodín en Azure AD Application Proxy

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Autenticación de usuarios

Para facilitar la implementación de aplicaciones y reducir la carga administrativa, ahora se admite la posibilidad de publicar aplicaciones mediante caracteres comodín. Para publicar una aplicación con comodín, puede seguir el flujo de publicación de aplicaciones estándar, pero usando un carácter comodín en las direcciones URL internas y externas.

Para más información, consulte [Aplicaciones con comodín en Azure Active Directory Application Proxy](#).

Nuevos cmdlets para admitir la configuración de Application Proxy

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Plataforma

La versión preliminar más reciente del módulo Azure AD PowerShell contiene nuevos cmdlets que permiten a los clientes configurar aplicaciones de Application Proxy mediante PowerShell.

Los nuevos cmdlets son:

- Get-AzureADApplicationProxyApplication
- Get-AzureADApplicationProxyApplicationConnectorGroup
- Get-AzureADApplicationProxyConnector
- Get-AzureADApplicationProxyConnectorGroup
- Get-AzureADApplicationProxyConnectorGroupMembers
- Get-AzureADApplicationProxyConnectorMemberOf
- New-AzureADApplicationProxyApplication
- New-AzureADApplicationProxyConnectorGroup

- Remove-AzureADApplicationProxyApplication
- Remove-AzureADApplicationProxyApplicationConnectorGroup
- Remove-AzureADApplicationProxyConnectorGroup
- Set-AzureADApplicationProxyApplication
- Set-AzureADApplicationProxyApplicationConnectorGroup
- Set-AzureADApplicationProxyApplicationCustomDomainCertificate
- Set-AzureADApplicationProxyApplicationSingleSignOn
- Set-AzureADApplicationProxyConnector
- Set-AzureADApplicationProxyConnectorGroup

Nuevos cmdlets para admitir la configuración de grupos

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Proxy de aplicaciones Plataforma

La versión más reciente del módulo de Azure AD PowerShell contiene cmdlets para administrar grupos en Azure AD. Estos cmdlets no estaban disponibles anteriormente en el módulo AzureADPreview y ahora se han agregado al módulo AzureAD.

Los cmdlets de grupo que ya se han publicado con disponibilidad general son:

- Get-AzureADMSGroup
- New-AzureADMSGroup
- Remove-AzureADMSGroup
- Set-AzureADMSGroup
- Get-AzureADMSGroupLifecyclePolicy
- New-AzureADMSGroupLifecyclePolicy
- Remove-AzureADMSGroupLifecyclePolicy
- Add-AzureADMSLifecyclePolicyGroup
- Remove-AzureADMSLifecyclePolicyGroup
- Reset-AzureADMSLifeCycleGroup
- Get-AzureADMSLifecyclePolicyGroup

Está disponible una nueva versión de Azure AD Connect

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Sincronización de AD Plataforma

Azure AD Connect es la herramienta preferida para sincronizar datos entre Azure AD y los orígenes de datos locales, incluidos Windows Server Active Directory y LDAP.

IMPORTANT

Esta compilación introduce cambios en las reglas de sincronización y en el esquema. El servicio de sincronización de Azure AD Connect desencadenará pasos de importación completa y sincronización completa después de una actualización. Para obtener información sobre cómo cambiar este comportamiento, consulte [Aplazamiento de la sincronización completa después de la actualización](#).

Esta versión incluye las siguientes actualizaciones y cambios:

Problemas corregidos:

- Corrección de la ventana de sincronización en las tareas en segundo plano para la página de filtrado de particiones al cambiar a la página siguiente.

- Se ha corregido un error que provocó una infracción de acceso durante la acción personalizada ConfigDB.
- Se ha corregido un error para recuperarse del tiempo de espera de la conexión de SQL.
- Se ha corregido un error que provocaba que los certificados con caracteres comodín de SAN generaran un error al realizar una comprobación de requisitos previos.
- Se ha corregido un error que provocaba que miiserver.exe se bloqueara durante una exportación del conector de AAD.
- Se ha corregido un error en el que un intento de contraseña incorrecta registrado en el controlador de dominio al ejecutarse provocaba que el asistente de AAD Connect cambiara la configuración.

Nuevas características y mejoras

- Telemetría de aplicaciones: los administradores pueden activar o desactivar este tipo de datos.
- Datos de mantenimiento de Azure AD: los administradores deben visitar el portal de mantenimiento para controlar la configuración de mantenimiento. Una vez se haya cambiado la directiva del servicio, los agentes la leerán y la aplicarán.
- Se han agregado acciones de configuración de escritura diferida de dispositivo y una barra de progreso para la inicialización de la página.
- Se han mejorado los diagnósticos generales con un informe HTML y una recopilación completa de datos en un informe HTML o de texto ZIP.
- Se ha mejorado la confiabilidad de la actualización automática y se ha agregado telemetría adicional para asegurarse de que se puede determinar el mantenimiento del servidor.
- Se han restringido los permisos disponibles para las cuentas con privilegios de la cuenta del conector AD. Para las nuevas instalaciones, el asistente restringe los permisos que las cuentas con privilegios tienen en la cuenta de MSOL tras la creación de esa cuenta. Los cambios afectan a las instalaciones rápidas y a las instalaciones personalizadas con la opción de creación automática de cuenta.
- Se ha cambiado el instalador, por lo que no se requiere el privilegio de asociación de seguridad en una instalación limpia de AADConnect.
- Se ha agregado una utilidad nueva para solucionar problemas de sincronización de un objeto específico. Actualmente, la utilidad comprueba los siguientes aspectos:
 - Error de coincidencia de UserPrincipalName entre el objeto de usuario sincronizado y la cuenta de usuario del inquilino de Azure AD.
 - Si se filtra el objeto de sincronización debido al filtrado de dominio
 - Si se filtra el objeto de sincronización debido al filtrado de unidad organizativa (UO)
- Se ha agregado una utilidad nueva para sincronizar el hash de contraseña actual almacenado en el Active Directory local para una cuenta de usuario específica. La utilidad no requiere un cambio de contraseña.

Se han agregado aplicaciones compatibles con directivas de Intune App Protection para usarlas con el acceso condicional basado en aplicaciones de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Acceso condicional Seguridad y protección de la identidad

Se han agregado más aplicaciones que admiten el acceso condicional basado en aplicaciones. Ahora, ya puede acceder a Office 365 y otras aplicaciones en la nube conectadas a Azure AD mediante estas aplicaciones cliente aprobadas.

Las siguientes aplicaciones se agregarán a finales del mes de febrero:

- Microsoft Power BI
- Microsoft Launcher
- Microsoft Invoicing

Para más información, consulte:

- [Requisito de aplicación cliente aprobada](#)
- [Acceso condicional basado en aplicaciones de Azure AD](#)

Actualización de los términos de uso relacionados con la experiencia móvil

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Cuando aparecen los términos de uso, puede hacer clic en **¿Tiene problemas con la visualización? Haga clic aquí.** Si hace clic en este vínculo se abren los términos de uso de forma nativa en el dispositivo.

Independientemente del tamaño de fuente en el documento o el tamaño de pantalla del dispositivo, puede acercar o alejar y leer el documento según sea necesario.

Enero de 2018

Nuevas aplicaciones federadas disponibles en la Galería de aplicaciones de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En enero de 2018, se agregaron a la galería de aplicaciones las siguientes aplicaciones nuevas compatibles con la federación:

[IBM OpenPages](#), [OneTrust Privacy Management Software](#), [Dealpath](#), [IriusRisk Federated Directory](#) y [Fidelity NetBenefits](#).

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Inicio de sesión con riesgo adicional detectado

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Identity Protection Seguridad y protección de la identidad

La perspectiva que se obtiene de una detección de riesgos identificada está asociada a su suscripción de Azure AD. Con la edición de Azure AD Premium P2, obtiene la información más detallada acerca de todas las detecciones subyacentes.

Con la edición de Azure AD Premium P1, las detecciones que no están cubiertas por su licencia aparecen como la detección de riesgos Inicio de sesión con riesgo adicional detectado.

Para más información, consulte [Detecciones de riesgos de Azure Active Directory](#).

Ocultación de aplicaciones de Office 365 de los paneles de acceso del usuario final

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones SSO

Ahora puede administrar mejor el modo en que se muestran las aplicaciones de Office 365 en los paneles de acceso de sus usuarios mediante una nueva configuración de usuario. Esta opción le resultará útil para reducir el número de aplicaciones de los paneles de acceso de los usuarios si prefiere mostrar solo las aplicaciones de Office en el Portal de Office. La configuración se encuentra en **Configuración de usuario** y tiene la etiqueta **Los usuarios solo pueden ver las aplicaciones de Office 365 en el Portal de Office 365**.

Para obtener más información, consulte [Ocultación de una aplicación de la experiencia del usuario en Azure Active Directory](#).

Inicio de sesión sin problemas en aplicaciones habilitadas para SSO de contraseña directamente desde la dirección URL de la aplicación

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones SSO

La extensión del explorador Mis aplicaciones ahora está disponible en una cómoda herramienta que ofrece la funcionalidad de inicio de sesión único Mis aplicaciones como acceso directo del explorador. Tras la instalación, los usuarios verán un ícono de gofre en el explorador que proporciona acceso rápido a las aplicaciones. Ahora, los usuarios podrán disfrutar de las ventajas siguientes:

- Capacidad para iniciar sesión directamente en aplicaciones de SSO de contraseña desde la página de inicio de sesión de la aplicación.
- Inicio de cualquier aplicación mediante la característica de búsqueda rápida.
- Accesos directos a aplicaciones usadas recientemente desde la extensión.
- La extensión está disponible en Microsoft Edge, Chrome y Firefox.

Para obtener más información, consulte [Extensión de inicio de sesión seguro de Mis aplicaciones](#).

Retirada de la experiencia de administración de Azure AD del Portal de Azure clásico

Tipo: Categoría del servicio: En desuso **Funcionalidad del producto:** Azure AD Directorio

El 8 de enero de 2018, la experiencia de administración de Azure AD se retiró del Portal de Azure clásico. Esto tuvo lugar junto con la retirada del Portal de Azure clásico. En el futuro, deberá usar el [Centro de administración de Azure AD](#) para todas las tareas de administración de Azure AD basadas en el portal.

El portal web PhoneFactor se ha retirado.

Tipo: Categoría del servicio: En desuso **Funcionalidad del producto:** Azure AD Directorio

El 8 de enero de 2018 se retiró el portal web PhoneFactor. Este portal se usaba para la administración del servidor MFA; sin embargo, sus funciones se han movido a Azure Portal en portal.azure.com.

La configuración de MFA se encuentra en: [Azure Active Directory > Servidor MFA](#)

Informes de Azure AD obsoletos

Tipo: Categoría del servicio: En desuso **Funcionalidad del producto:** Informes Administración del ciclo de vida de la identidad

Con la disponibilidad general de la nueva consola de administración de Azure Active Directory y las nuevas API disponibles para los informes de actividad y seguridad, las API de informes que se encontraban en el punto de conexión "/reports" se retiraron el 31 de diciembre de 2017.

¿Qué está disponible?

Como parte de la transición a la nueva consola de administración, existen dos nuevas API disponibles para recuperar los registros de actividad de Azure AD. El nuevo conjunto de API proporciona más funciones de filtro y ordenación, así como actividades de auditoría e inicio de sesión. Los datos que estaban disponibles anteriormente en los informes de seguridad ahora son accesibles a través de la API de detecciones de riesgos de Identity

Protection en Microsoft Graph.

Para más información, consulte:

- [Introducción a la API de informes de Azure Active Directory](#)
 - [Introducción a Azure Active Directory Identity Protection y Microsoft Graph](#)
-

Diciembre de 2017

Términos de uso del panel de acceso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Ahora puede ir al panel de acceso y ver los términos de uso previamente aceptados.

Siga estos pasos:

1. Abra el [portal de Mis aplicaciones](#) e inicie sesión.
2. En la esquina superior derecha, seleccione su nombre y seleccione **Perfil** en la lista.
3. En su **Perfil**, seleccione **Revisar los términos de uso**.
4. Ahora podrá revisar los términos de uso que aceptó.

Para obtener más información, consulte [Característica Términos de uso de Azure Active Directory \(versión preliminar\)](#).

Nueva experiencia de inicio de sesión de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Autenticación de usuarios

Azure AD y las interfaces de usuario del sistema de identidades de cuentas de Microsoft se han rediseñado para ofrecer un aspecto más homogéneo. Además, la página de inicio de sesión de Azure AD primero recopila el nombre de usuario, seguido de la credencial en una segunda pantalla.

Para obtener más información, consulte [The new Azure AD Signin Experience is now in Public Preview](#) (Nueva experiencia de inicio de sesión de Azure AD disponible en versión preliminar pública).

Menos solicitudes de inicio de sesión: nueva experiencia "Mantener la sesión iniciada" para el inicio de sesión de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Autenticación de usuarios

Hemos sustituido la casilla **Mantener la sesión iniciada** de la página de inicio de sesión de Azure AD por un nuevo mensaje que se muestra al realizar la autenticación correctamente.

Si se responde **Sí** a este mensaje, el servicio proporciona un token de actualización persistente. Este es el mismo comportamiento que se produce cuando se activa la casilla **Mantener la sesión iniciada** en la experiencia antigua. Para los inquilinos federados, este mensaje se muestra al autenticarse correctamente en el servicio federado.

Para más información, consulte [Fewer sign-in prompts: The new "keep me signed in" experience for Azure AD is in preview](#) (Menos avisos de inicio de sesión: la nueva experiencia "Mantener la sesión iniciada" para Azure AD está en versión preliminar).

Agregar configuración para exigir expandir los términos de uso antes de su aceptación

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Se ha agregado una opción para los administradores con el fin de exigir a usuarios finales que expandan los términos de uso antes de aceptarlos.

Seleccione **Activado** o **Desactivado** para exigir que los usuarios expandan los términos de uso. El valor **Activado** exige a usuarios que lean los términos de uso antes de aceptarlos.

Para obtener más información, consulte [Característica Términos de uso de Azure Active Directory \(versión preliminar\)](#).

Activación de ámbito para las asignaciones de roles válidos

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

Puede usar la activación con ámbito para activar las asignaciones de roles de recursos de Azure válidas con menos autonomía que los valores predeterminados de las asignaciones originales. Un ejemplo de esto es si se le asigna como propietario de una suscripción en su inquilino. Con la activación con ámbito, podrá activar el rol de propietario para hasta cinco de los recursos incluidos en la suscripción (por ejemplo, los grupos de recursos y las máquinas virtuales). La definición del ámbito de la activación puede reducir la posibilidad de ejecutar cambios no deseados en recursos importantes de Azure.

Para más información, vea [¿Qué es Azure AD Privileged Identity Management?](#).

Nuevas aplicaciones federadas en la galería de aplicaciones de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Aplicaciones empresariales Integración de terceros

En diciembre de 2017, hemos agregado estas 15 nuevas aplicaciones con compatibilidad con la federación a nuestra galería de aplicaciones:

[Accredible](#), [Adobe Experience Manager](#), [EFI Digital StoreFront](#), [Communifire](#), [CybSafe](#), [FactSet](#), [IMAGE WORKS](#), [MOBI](#), [Integración de Azure AD con MobileIron](#), [Reflektive](#), [SAML SSO for Bamboo by resolution GmbH](#), [SAML SSO for Bitbucket by resolution GmbH](#), [Vodeclic](#), [WebHR](#), [Zenegy Azure AD Integration](#).

Para obtener más información acerca de las aplicaciones, consulte [Integración de aplicación SaaS con Azure Active Directory](#).

Para obtener más información para que una aplicación se muestre en la galería de aplicaciones de Azure AD, consulte [Aprenda a mostrar su aplicación en la galería de aplicaciones de Azure Active Directory](#).

Flujos de trabajo de aprobación de roles de directorio de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

El flujo de trabajo de aprobación de roles de directorio de Azure AD está disponible de manera general.

Con el flujo de trabajo de aprobación, los administradores de roles con privilegios pueden exigir que los miembros de roles aptos soliciten la activación de roles para poder usar el rol con privilegios. Ahora es posible delegar responsabilidades de aprobación en múltiples usuarios y grupos. Los miembros del rol aptos recibirán notificaciones cuando termine la aprobación y sus roles estén activos.

Autenticación de paso a través: Compatibilidad con Skype Empresarial

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Autenticaciones (inicios de sesión) Autenticación de usuarios

Ahora, la autenticación de paso a través admite inicios de sesión de usuarios en aplicaciones cliente de Skype Empresarial compatibles con la autenticación moderna, incluidas las topologías híbridas y en línea.

Para obtener más información, consulte [Topologías de Skype Empresarial compatibles con la autenticación moderna](#).

Actualizaciones de Azure AD Privileged Identity Management para RBAC de Azure (versión preliminar)

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Privileged Identity Management Privileged Identity Management

Con la actualización de versión preliminar pública de Azure AD Privileged Identity Management (PIM) para el control de acceso basado en roles (RBAC) de Azure, ahora podrá realizar lo siguiente:

- Usar Just Enough Administration.
- Solicitar aprobación para activar roles de recursos.
- Programar la activación futura de un rol que requiere la aprobación de roles de Azure AD y de RBAC de Azure.

Para obtener más información, consulte [PIM para recursos de Azure \(versión preliminar\)](#).

Noviembre de 2017

Retirada del servicio de control de acceso

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Access Control Service Servicio Access Control

Azure Active Directory Access Control (también conocido como Access Control Service) se retirará a finales de 2018. En las próximas semanas se ofrecerá más información, como, por ejemplo, una programación detallada y una guía de migración de alto nivel. Puede dejar comentarios en esta página con preguntas acerca de Access Control Service y un miembro del equipo le responderá.

Restringir el acceso desde el explorador a Intune Managed Browser

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

El uso de Intune Managed Browser como aplicación aprobada le permite restringir el acceso desde el explorador a Office 365 y otras aplicaciones en la nube conectadas a Azure AD.

Ahora podrá configurar la siguiente condición para el acceso condicional basado en aplicaciones:

Aplicaciones cliente: Browser

¿Cuál es el efecto del cambio?

En la actualidad, el acceso está bloqueado cuando se usa esta condición. Cuando la vista previa está disponible, todos los accesos requerirán el uso de la aplicación Manager Browser.

Busque esta funcionalidad y más información en las próximas entradas de blogs y notas de versión.

Para obtener más información, consulte [Acceso condicional en Azure AD](#).

Nuevas aplicaciones cliente aprobadas para el acceso condicional basado en aplicaciones de Azure AD

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

Las siguientes aplicaciones se incluyen en la lista de [aplicaciones cliente aprobadas](#):

- [Microsoft Kaizala](#)
- Microsoft StaffHub

Para más información, consulte:

- [Requisito de aplicación cliente aprobada](#)
- [Acceso condicional basado en aplicaciones de Azure AD](#)

Disponibilidad de los términos de uso en varios idiomas

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso Cumplimiento normativo

Ahora, los administradores pueden crear nuevos términos de uso que contengan varios documentos PDF. Puede etiquetar estos documentos PDF con el idioma correspondiente. De este modo, se mostrará a los usuarios el documento PDF en el idioma correspondiente a sus preferencias. Si no hay ninguna coincidencia, se muestra el idioma predeterminado.

Estado del cliente de escritura diferida de contraseñas en tiempo real

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Autoservicio de restablecimiento de contraseña Autenticación de usuarios

Ahora podrá revisar el estado de su cliente de escritura diferida de contraseñas local. Esta opción está disponible en la sección **Integración local** de la página [Restablecimiento de contraseña](#).

Si hay problemas con la conexión al cliente de escritura diferida local, se mostrará un mensaje de error con los elementos siguientes:

- Información del motivo por el que no puede conectarse a su cliente de escritura diferida local.
- Un vínculo a documentación que le ayuda a resolver el problema.

Para obtener más información, consulte [Integración local](#).

Acceso condicional basado en aplicaciones de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Azure AD Protección y seguridad de la identidad

Ahora puede restringir el acceso a Office 365 y a otras aplicaciones en la nube conectadas a Azure AD para [aplicaciones cliente aprobadas](#) que admiten directivas de Intune App Protection mediante el [acceso condicional basado en aplicaciones de Azure AD](#). Las directivas de Intune App Protection se utilizan para configurar y proteger los datos de empresa en estas aplicaciones cliente.

Al combinar directivas de acceso condicional [basado en aplicaciones](#) con las directivas de acceso condicional [basado en dispositivos](#), tiene la flexibilidad necesaria para proteger los datos de dispositivos personales y de la empresa.

Ahora puede usar los siguientes controles y condiciones con el acceso condicional basado en aplicaciones:

Condición de plataforma admitida

- iOS
- Android

Condición de aplicaciones cliente

- Aplicaciones móviles y aplicaciones de escritorio

Control de acceso

- Requerir aplicación cliente aprobada

Para obtener más información, consulte [Acceso condicional basado en aplicaciones de Azure AD](#).

Administración de dispositivos de Azure AD en Azure Portal

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración y registro de dispositivos Protección y seguridad de la identidad

Ahora podrá encontrar todos los dispositivos conectados a Azure AD y las actividades relacionadas con dispositivos en un solo lugar. Hay una nueva experiencia de administración para administrar todas las configuraciones e identidades de dispositivos en Azure Portal. En esta versión podrá hacer lo siguiente:

- Ver todos los dispositivos que están disponibles para el acceso condicional en Azure AD.
- Ver propiedades, incluidos los dispositivos unidos a Azure AD híbrido.
- Encontrar las claves de BitLocker para los dispositivos unidos a Azure AD, administrar el dispositivo con Intune y mucho más.
- Administrar la configuración relacionada con dispositivos de Azure AD.

Para obtener más información, consulte [Administración de dispositivos con Azure Portal](#).

Compatibilidad con macOS como plataforma de dispositivos para el acceso condicional de Azure AD

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

Ahora puede incluir (o excluir) macOS como condición de plataforma de dispositivos en la directiva de acceso condicional de Azure AD. Con la incorporación de macOS a las plataformas de dispositivos compatibles, puede:

- **Inscribir y administrar dispositivos Mac OS con Intune.** Al igual que en otras plataformas, como iOS y Android, existe una aplicación de portal de empresa para macOS que permite realizar inscripciones unificadas. Utilice la nueva aplicación de portal de empresa para macOS para inscribir un dispositivo con Intune y registrarlo con Azure AD.
- **Asegurarse de que los dispositivos macOS se ajustan a las directivas de cumplimiento de su organización definidas en Intune.** En Intune en Azure Portal, ahora podrá configurar directivas de cumplimiento para dispositivos macOS.
- **Restringir el acceso a las aplicaciones de Azure AD a solo los dispositivos macOS que cumplan las directivas.** La creación de directivas de acceso condicional usa macOS como una opción de plataforma de dispositivos independiente. Ahora puede crear directivas de acceso condicional específicas de macOS para el conjunto de aplicaciones de destino en Azure.

Para más información, consulte:

- [Creación de una directiva de cumplimiento para dispositivos macOS con Intune](#)
- [Acceso condicional en Azure AD](#)

Extensión Servidor de directivas de redes para Azure Multi-Factor Authentication

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Multi-Factor Authentication Autenticación de usuarios

La extensión Servidor de directivas de redes para Azure Multi-Factor Authentication incorpora funcionalidades de Multi-Factor Authentication basadas en la nube para su infraestructura de autenticación mediante los servidores existentes. Con la extensión Servidor de directivas de redes, podrá agregar mecanismos de verificación mediante

Llamadas de teléfono, mensajes de texto o aplicaciones de teléfono al flujo de autenticación existente. Para ello, no tendrá que instalar, configurar ni mantener servidores nuevos.

Esta extensión se creó para las organizaciones que quieren proteger las conexiones de redes privadas virtuales sin tener que implementar el Servidor Microsoft Azure Multi-Factor Authentication. La extensión Servidor de directivas de redes actúa como un adaptador entre RADIUS y Azure Multi-Factor Authentication basada en la nube para proporcionar un segundo factor de autenticación a los usuarios federados o sincronizados.

Para obtener más información, consulte [Integración de la infraestructura existente de NPS con Azure Multi-Factor Authentication](#).

Restauración o eliminación permanente de usuarios eliminados

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Administración de usuarios Directorio

En el centro de administración de Azure AD, ahora puede:

- Restaurar un usuario eliminado.
- Eliminar un usuario permanentemente.

Para probarlo:

1. En el centro de administración de Azure AD, seleccione [Todos los usuarios](#) en la sección **Administrar**.
2. En la lista **Mostrar**, seleccione **Usuarios eliminados recientemente**.
3. Seleccione uno o varios usuarios eliminados recientemente y después restáurelos o elimínelos permanentemente.

Nuevas aplicaciones cliente aprobadas para el acceso condicional basado en aplicaciones de Azure AD

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

Las siguientes aplicaciones se agregaron a la lista de [aplicaciones cliente aprobadas](#):

- Microsoft Planner
- Azure Information Protection

Para más información, consulte:

- [Requisito de aplicación cliente aprobada](#)
- [Acceso condicional basado en aplicaciones de Azure AD](#)

Uso del operador "OR" entre controles de una directiva de acceso condicional

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Acceso condicional Protección y seguridad de la identidad

Ahora puede usar el operador "OR" (requerir uno de los controles seleccionados) en los controles de acceso condicional. Puede usar esta característica para crear directivas con el operador "OR" entre controles de acceso. Por ejemplo, puede usar esta característica para crear una directiva que requiera que un usuario inicie sesión mediante Multi-Factor Authentication "O" que esté en un dispositivo compatible.

Para obtener más información, consulte [Controles en el acceso condicional de Azure AD](#).

Agregación de detecciones de riesgos en tiempo real

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Identity Protection

Protección y seguridad de la identidad

En Azure AD Identity Protection, todas las detecciones de riesgos en tiempo real que se han originado desde la misma dirección IP en un día determinado ahora se agregan para cada tipo de detección de riesgos. Este cambio limita el volumen de las detecciones de riesgos que se muestran sin ningún cambio en la seguridad del usuario.

La detección en tiempo real subyacente funciona cada vez que el usuario inicia sesión. Si tiene configurada una directiva de seguridad de riesgo de inicio de sesión para Multi-Factor Authentication o para bloquear el acceso, esta se desencadena durante cada inicio de sesión con riesgo.

Octubre de 2017

Informes de Azure AD obsoletos

Tipo: Categoría del servicio: Plan de cambio **Funcionalidad del producto:** Informes Administración del ciclo de vida de la identidad

Azure Portal proporciona lo siguiente:

- Una nueva consola de administración de Azure AD.
- Nuevas API de informes de actividades y de seguridad.

Debido a estas nuevas funcionalidades, las API de informes que se encuentran en el punto de conexión /reports se retiraron el 10 de diciembre de 2017.

Detección automática de campos de inicio de sesión

Tipo: Categoría del servicio: Corregida **Funcionalidad del producto:** Mis aplicaciones Inicio de sesión único

Azure AD admite la detección automática de campos de inicio de sesión para las aplicaciones que presentan un campo de nombre de usuario y contraseña HTML. Estos pasos se documentan en [Captura automática de campos de inicio de sesión para una aplicación](#). Puede encontrar esta funcionalidad mediante la adición de una aplicación *situada fuera de la galería* en la página [Aplicaciones empresariales](#) en [Azure Portal](#). Además, en esta nueva aplicación podrá configurar el modo **Inicio de sesión único** en **Inicio de sesión único basado en contraseña**, especificar una URL web y, a continuación, guardar la página.

Debido a un problema del servicio, esta funcionalidad se deshabilitó temporalmente. El problema se ha resuelto y la detección automática del campo de inicio de sesión vuelve a estar disponible.

Nuevas características de Multi-Factor Authentication

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Multi-Factor Authentication Protección y seguridad de la identidad

Multi-Factor Authentication (MFA) es un componente esencial para la protección de su organización. Para hacer que las credenciales tengan mayor capacidad de adaptación y que la experiencia resulte más sencilla, se han agregado las siguientes características:

- Integración de los resultados del desafío multifactor directamente en el informe de inicio de sesión de Azure AD, incluido el acceso mediante programación a los resultados de MFA.
- Integración más profunda de la configuración de MFA en la experiencia de configuración de Azure AD en Azure Portal.

Con esta versión preliminar pública, los informes y la administración de MFA son una parte integrada de la experiencia de configuración principal de AD Azure. Ahora podrá administrar la funcionalidad del portal de administración de MFA en la experiencia de Azure AD.

Para obtener más información, consulte [Referencia para los informes de la autenticación multifactor en Azure](#)

Términos de uso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Términos de uso
Cumplimiento normativo

Puede usar los términos de uso de Azure AD para presentar información a los usuarios, como, por ejemplo, renuncias relevantes para los requisitos legales o de cumplimiento.

Los términos de uso de Azure AD puede utilizarse en los escenarios siguientes:

- Términos de uso generales para todos los usuarios de su organización.
- Términos de uso específicos basados en los atributos de un usuario (por ejemplo, médicos frente a enfermeras o empleados nacionales frente a internacionales, creados por grupos dinámicos).
- Términos de uso específicos para el acceso a aplicaciones empresariales de alto impacto, como, por ejemplo, Salesforce.

Para obtener más información, consulte [Términos de uso de Azure AD](#).

Mejoras en Privileged Identity Management

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Privileged Identity Management
Privileged Identity Management

Con Privileged Identity Management (PIM) de Azure AD, podrá administrar, controlar y supervisar el acceso a los recursos de Azure (vista preliminar) dentro de su organización por parte de:

- Suscripciones
- Grupos de recursos
- Máquinas virtuales

Todos los recursos de Azure Portal que usan la funcionalidad RBAC de Azure pueden usar las funcionalidades de seguridad y administración del ciclo de vida que ofrece Privileged Identity Management de Azure AD.

Para obtener más información, consulte [PIM para recursos de Azure \(versión preliminar\)](#).

Revisões de acceso

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Revisiones de acceso
Cumplimiento normativo

Las organizaciones pueden usar las revisiones de acceso (versión preliminar) para administrar de manera eficaz las pertenencias a grupos y el acceso a las aplicaciones empresariales:

- Puede volver a certificar el acceso de usuario invitado mediante las revisiones de acceso a las aplicaciones y la pertenencia a grupos. La información que proporcionan las revisiones de acceso permite a los revisores decidir de manera eficaz si deben permitir el acceso continuado a los invitados.
- Puede volver a certificar el acceso de los empleados a las aplicaciones y la pertenencia a grupos con las revisiones de acceso.

Puede recopilar los controles de revisiones de acceso en programas importantes para que su organización realice un seguimiento de las revisiones de aplicaciones vulnerables o de cumplimiento normativo.

Para obtener más información, consulte [Revisiones de acceso de Azure AD](#).

Ocultación de aplicaciones de terceros de Mis aplicaciones y del iniciador de aplicaciones de Office 365

Tipo: Categoría del servicio: Nueva característica **Funcionalidad del producto:** Mis aplicaciones Inicio de

sesión único

Ahora podrá administrar mejor las aplicaciones que se muestran en los portales de usuario con la nueva propiedad **hide app**. Puede ocultar aplicaciones para ayudar en casos en los que se muestran iconos de aplicaciones para servicios back-end o iconos duplicados que se acumulan en los iniciadores de aplicaciones de usuarios. El botón de alternancia se encuentra en la sección **Propiedades** de la aplicación de terceros con la etiqueta **Visible to user?** (¿Visible para el usuario?). También puede ocultar una aplicación mediante programación con PowerShell.

Para obtener más información, consulte [Ocultación de una aplicación de la experiencia del usuario en Azure Active Directory](#).

¿Qué está disponible?

Como parte de la transición a la nueva consola de administración, hay disponibles dos nuevas API que permiten recuperar los registros de actividad de Azure AD. El nuevo conjunto de API proporciona más funciones de filtro y ordenación, así como actividades de auditoría e inicio de sesión. Los datos que estaban disponibles anteriormente a través de los informes de seguridad ahora se proporcionan mediante la API de detecciones de riesgos de Identity Protection en Microsoft Graph.

Septiembre de 2017

Revisión para Identity Manager

Tipo: Categoría del servicio: Característica modificada **Funcionalidad del producto:** Identity Manager Administración del ciclo de vida de la identidad

Un paquete acumulativo de revisiones (compilación 4.4.1642.0) está disponible desde el 25 de septiembre de 2017 para Microsoft Identity Manager 2016 Service Pack 1. Este paquete acumulativo de revisiones:

- Resuelve problemas e incorpora mejoras.
- Es una actualización acumulativa que reemplaza a todas las actualizaciones de Identity Manager 2016 Service Pack 1 hasta la compilación 4.4.1459.0 de Identity Manager 2016.
- Requiere disponer de Identity Manager 2016, compilación 4.4.1302.0.

Para obtener más información, consulte [Paquete acumulativo de revisiones \(compilación 4.4.1642.0\) está disponible para Microsoft Identity Manager SP1 de 2016](#).

Inicio rápido: Creación de un inquilino en Azure Active Directory

21/05/2020 • 3 minutes to read • [Edit Online](#)

Puede hacer todas las tareas administrativas mediante el portal de Azure Active Directory (Azure AD), incluida la creación de un inquilino para su organización.

En este tutorial, obtendrá información sobre cómo acceder a Azure Portal y a Azure Active Directory y sobre cómo crear un inquilino básico para su organización.

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

Creación de un inquilino para la organización

Después de iniciar sesión en Azure Portal, puede crear un inquilino para su organización. El nuevo inquilino representa a su organización y le ayuda a administrar una instancia específica de Servicios en la nube de Microsoft para los usuarios internos y externos.

Para crear un inquilino

1. Inicie sesión en la instancia de [Azure Portal](#) de la organización.
2. En el menú de Azure Portal, seleccione **Crear un recurso**.

The screenshot shows the Azure portal interface. On the left, there's a sidebar with various service icons and links like 'Inicio', 'Panel', 'Todos los servicios', and 'FAVORITOS'. A red box highlights the 'Crear un recurso' (Create a resource) button at the top of the sidebar. The main content area has a search bar at the top right with the placeholder 'Buscar recursos, servicios y documentos (G+/-)'. Below the search bar, there are some icons and the text 'Última actualización: hace un minuto' (Last updated: one minute ago). The central part of the screen features a section titled 'Introducción a Azure simplificada' (Simplified introduction to Azure) with a 'Crear un proyecto de DevOps' (Create a DevOps project) button. To the right, there's a 'Inicios rápidos y tutoriales' (Quick starts and tutorials) section with several items listed:

- Windows Virtual Machines
- Máquinas virtuales Linux
- App Service
- Funciones
- SQL Database

At the bottom of the sidebar, there's a 'Marketplace' link.

3. Seleccione **Identidad** y después seleccione **Azure Active Directory**.

Aparece la página **Crear directorio**.

Home > New > Create directory

Create directory

* Organization name ⓘ
Contoso ✓

* Initial domain name ⓘ
contoso ✓
contoso.onmicrosoft.com

Country or region ⓘ
United States

i Directory creation will take about one minute.

Create

4. En la página **Crear directorio**, escriba la información siguiente:

- Escriba *Contoso* en el cuadro **Nombre de la organización**.
- Escriba *Contoso* en el cuadro **Nombre de dominio inicial**.
- Deje la opción *Estados Unidos* en el cuadro **País o región**.

5. Seleccione **Crear**.

El nuevo inquilino se crea con el dominio contoso.onmicrosoft.com.

Limpieza de recursos

Si no va a seguir usando esta aplicación, puede eliminar el inquilino mediante los siguientes pasos:

- Asegúrese de que ha iniciado sesión en el directorio que desea eliminar mediante el filtro **Directorio + suscripción** de Azure Portal y cambie al directorio de destino, si es necesario.
- Seleccione **Azure Active Directory** y, después, en la página **Contoso - Información general**, seleccione **Eliminar directorio**.

El inquilino y su información asociada se eliminarán.

Inicio > Contoso - Información general

Contoso - Información general

Azure Active Directory

Cambiar directorio Eliminar el directorio

Buscar (Ctrl+ /)

Información general

Introducción

Administrar

- Usuarios
- Grupos
- Relaciones organizativas
- Roles y administradores
- Aplicaciones empresariales
- Dispositivos
- Registros de aplicaciones
- Proxy de la aplicación
- Licencias
- Azure AD Connect
- Nombres de dominio personalizados
- Movilidad (MDM y MAM)
- Restablecimiento de contraseña
- Personalización de marca de empresa

contoso.com

Contoso

Azure AD para Office 365

Inicios de sesión

9 sep

What's new in Azure AD

Manténgase al día con las notas de la versión y entradas de blog más recientes.

36 entradas desde el 15 de mayo de 2018. [Ver archivo](#)

Todos los servicios	(36)	Característica modificada
<input type="checkbox"/>	Administración del ciclo...	(8)
<input type="checkbox"/>	Supervisión e informes	(5)
<input type="checkbox"/>	Seguridad y protección...	(2)
	Otro: Administración del ciclo de vida...	20 de julio de 2018

Su rol

Administrador global
Más información

Buscar

Usuarios

Buscar

Sincronización de Azure AD Connect

Estado Habilitado
Sincronización... Hace más de un día

Create

Usuario
Usuario invitado
Grupo
Aplicación empresarial
Registro de aplicación

Pasos siguientes

- Para cambiar o agregar nombres de dominio adicionales, vea [Incorporación de su nombre de dominio personalizado a Azure Active Directory](#).
- Para agregar usuarios, vea [Incorporación o eliminación de un nuevo usuario](#).
- Para agregar grupos y miembros, vea [Creación de un grupo básico y adición de miembros](#).
- Obtenga información sobre el [acceso basado en rol mediante Privileged Identity Management](#) y el [acceso condicional](#) para ayudar a administrar el acceso a aplicaciones y recursos de su organización.
- Obtenga información sobre Azure AD, incluida la [información de licencia básica](#), [terminología](#) y [características asociadas](#).

Inicio rápido: Visualización de los grupos y miembros de la organización en Azure Active Directory

21/05/2020 • 6 minutes to read • [Edit Online](#)

Puede ver los grupos existentes en la organización y los miembros de los grupos mediante Azure Portal. Los grupos se usan para administrar usuarios (miembros) que necesitan el mismo acceso y permisos para servicios y aplicaciones potencialmente restringidos.

En esta guía de inicio rápido podrá ver todos los grupos existentes en la organización y ver los miembros asignados.

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

Prerrequisitos

Antes de comenzar, deberá:

- Crear un inquilino de Azure Active Directory. Para más información, consulte [Acceso al portal de Azure Active Directory y creación de un nuevo inquilino](#).

Inicio de sesión en Azure Portal

Debe iniciar sesión en [Azure Portal](#) con una cuenta de administrador global del directorio.

Creación de un grupo nuevo

Cree un nuevo grupo llamado *MDM policy - West*. Para más información acerca de cómo crear un grupo, consulte [Cómo crear un grupo básico y agregar miembros](#).

1. Seleccione **Azure Active Directory**, **Grupos** y, a continuación, seleccione **Nuevo grupo**.
2. Rellene la página **Grupo**:
 - **Tipo de grupo**: seleccione **Seguridad**.
 - **Nombre del grupo**: escriba *MDM policy - West (Directiva de MDM - Oeste)*
 - **Tipo de pertenencia**: seleccione **Asignado**.
3. Seleccione **Crear**.

Creación de un nuevo usuario

Cree un nuevo usuario llamado *Alain Charon*. El usuario debe existir antes de ser agregado como miembro del grupo. Revise primero la pestaña “Nombres de dominio personalizados” para obtener el nombre de dominio verificado en el que quiera crear usuarios. Para más información acerca de cómo crear un usuario, consulte [Cómo agregar o eliminar usuarios](#).

1. Seleccione **Azure Active Directory**, **Usuarios** y, a continuación, seleccione **Nuevo usuario**.
2. Rellene la página **Usuario**:
 - **Nombre**: escriba *Alain Charon*.

- **Nombre de usuario:** Escriba *alain@contoso.com*.
3. Copie la contraseña generada automáticamente proporcionada en el cuadro de texto **Contraseña** y, a continuación, seleccione **Crear**.

Adición de un miembro del grupo

Ahora que tiene un grupo y un usuario, puede agregar a *Alain Charon* como un miembro del grupo *MDM policy - West*. Para más información acerca de cómo agregar miembros del grupo, consulte [Cómo agregar o eliminar miembros del grupo](#).

1. Seleccione Azure Active Directory > Grupos.
2. En la página **Grupos - Todos los grupos**, busque y seleccione el grupo **MDM policy - West**.
3. En la página **Información general de MDM policy - West**, seleccione **Miembros** en el área **Administrar**.
4. Seleccione **Agregar miembros** y, a continuación, busque y seleccione **Alain Charon**.
5. Elija **Seleccionar**.

Visualización de todos los grupos

Puede ver todos los grupos de la organización en la página **Grupos - Todos los grupos** de Azure Portal.

- Seleccione Azure Active Directory > Grupos.

Aparecerá la página **Grupos - Todos los grupos** con todos los grupos activos.

NOMBRE	TIPO DE GRUPO	TIPO DE PERTENENCIA
AD SyncAdmins	Seguridad	Sincronizada
AD SyncBrowse	Seguridad	Sincronizada
AD SyncOperators	Seguridad	Sincronizada
AD SyncPasswordSet	Seguridad	Sincronizada
AzureADPremiumP2-ALL	Seguridad	Sincronizada
Converged	Seguridad	Asignado
DnsAdmins	Seguridad	Sincronizada
DnsAdmins	Seguridad	Sincronizada

Búsqueda del grupo

Utilice la página **Grupos - Todos los grupos** para buscar el grupo *MDM policy - West*.

1. En la página **Grupos - Todos los grupos**, escriba *MDM* en el cuadro **Buscar**.

Los resultados de la búsqueda aparecen bajo el cuadro **Buscar**, incluido el grupo *MDM policy - West*.

Home > Contoso > Groups - All groups

Groups - All groups

Contoso - Azure Active Directory

All groups

New group Refresh Columns

Name	GROUP TYPE	MEMBERSHIP TYPE
MDM	Security	Assigned
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

Settings

- General
- Expiration
- Activity
- Access reviews
- Audit logs
- Troubleshooting + Support
- Troubleshoot
- New support request

2. Seleccione el grupo **MDM policy – West**.
3. Puede ver la información del grupo en la página **Información general de MDM policy - West**, incluido el número de miembros del grupo.

Home > Contoso > Groups - All groups > MDM policy - West

MDM policy - West

Group

Overview

Members

Properties

Owners

Group memberships

Applications

Licenses

Azure resources

Activity

Access reviews

Audit logs

Troubleshooting + Support

Troubleshoot

New support request

Delete

MDM policy - West

MP

Membership type	Type
Assigned	Security
Source	Object ID
Cloud	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

Members 50 User(s)

0 Group(s) 50 Device(s) 0 Other(s)

Group memberships 0 Owners 2

Visualización de los miembros del grupo

Ahora que ha encontrado el grupo, puede ver todos los miembros asignados.

- Seleccione **Miembros** en el área **Administrar** y, a continuación, revise la lista completa de los nombres de los miembros asignados a ese grupo específico, incluido *Alain Charon*.

Home > Contoso > Groups - All groups > MDM policy - West - Members

MDM policy - West - Members

Group

Overview

Add members Refresh

NAME	TYPE
AC Alain Charon	User
DM Danielle McKay	User
ES Eggert Schafer	User

Manage

- Properties
- Members**
- Owners
- Group memberships
- Applications
- Licenses
- Azure resources

Activity

- Access reviews
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Limpieza de recursos

Este grupo se utiliza en varios de los procesos de procedimientos disponibles en la sección **Guías de procedimientos** de esta documentación. Sin embargo, si prefiere no utilizar este grupo, puede eliminarlo y también los miembros asignados mediante los siguientes pasos:

1. En la página **Grupos - Todos los grupos**, busque el grupo **MDM policy - West**.
2. Seleccione el grupo **MDM policy - West**.

Aparece la página **Información general de MDM policy - West**.

3. Seleccione **Eliminar**.

El grupo y los miembros asociados se eliminan.

Home > Contoso > Groups - All groups > MDM policy - West

MDM policy - West

Group

Delete

MDM policy - West

MP

Membership type	Type
Assigned	Security
Source	Object ID
Cloud	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

Members
50 User(s) | 0 Group(s) | 50 Device(s) | 0 Other(s)

Group memberships
0

Owners
2

Activity

- Access reviews
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

IMPORTANT

Esta operación no elimina al usuario Alain Charon, solo su pertenencia al grupo eliminado.

Pasos siguientes

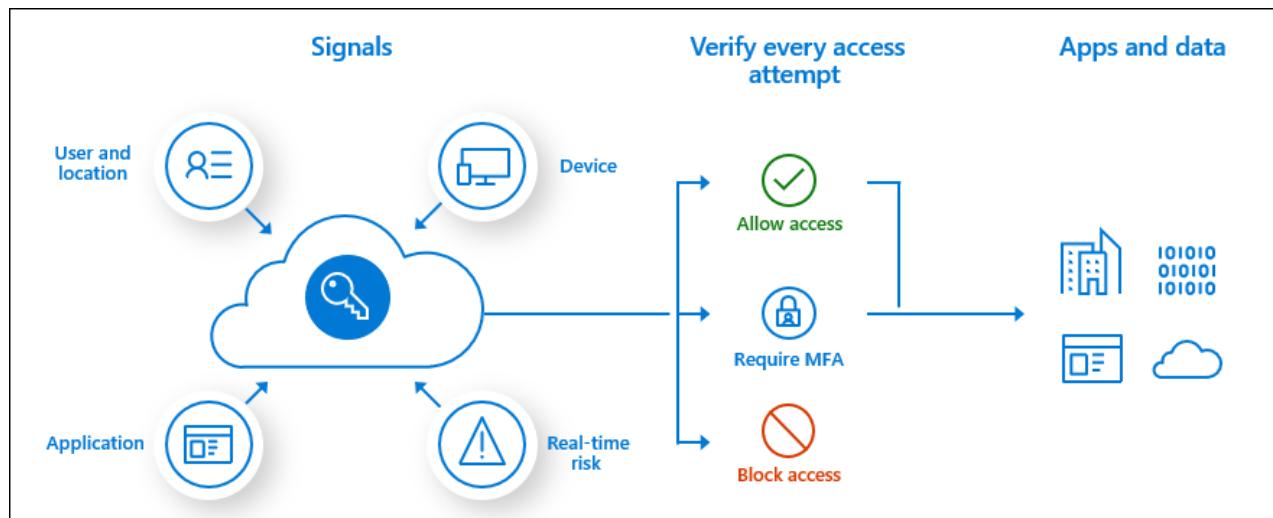
Avance al siguiente artículo para obtener información sobre cómo asociar una suscripción al directorio de Azure AD.

[Asociación de una suscripción de Azure](#)

Introducción a Azure Multi-Factor Authentication en una organización

22/07/2020 • 3 minutes to read • [Edit Online](#)

Hay varias maneras de habilitar Azure Multi-Factor Authentication para los usuarios de Azure Active Directory (AD) en función de las licencias que posea una organización.



Según nuestros estudios, es muy improbable que una cuenta se vea comprometida si se usa la autenticación multifactor (MFA).

Así pues, ¿cómo puede activar su organización MFA incluso de forma gratuita antes de convertirse en una estadística?

Opción gratuita

Los clientes que usen las ventajas gratuitas de Azure AD pueden emplear [valores predeterminados de seguridad](#) para habilitar la autenticación multifactor en su entorno.

Microsoft 365 Empresa, E3 o E5

En el caso de los clientes con Office 365, hay dos opciones:

- Azure Multi-Factor Authentication está o bien habilitado o bien deshabilitado para todos los usuarios, para todos los eventos de inicio de sesión. No se puede habilitar la autenticación multifactor solo para un subconjunto de usuarios o solo en determinados escenarios. La administración se realiza a través del portal de Office 365.
- Para mejorar la experiencia del usuario, actualice a Azure AD Premium P1 o P2 y use el acceso condicional. Para más información, consulte el artículo sobre la protección de los recursos de Office 365 con la autenticación multifactor.

Azure AD Premium P1

Para clientes con Azure AD Premium P1 o licencias similares que incluyen esta funcionalidad, como Enterprise Mobility + Security E3, Microsoft 365 F1 o Microsoft 365 E3:

Utilice el [acceso condicional de Azure AD](#) si desea solicitar la autenticación multifactor a los usuarios en determinados escenarios o eventos, lo que le permitirá adaptarse a los requisitos empresariales.

Azure AD Premium P2

Para clientes con Azure AD Premium P2 o licencias similares que incluyen esta funcionalidad, como Enterprise Mobility + Security E5 o Microsoft 365 E5:

Proporciona la opción de seguridad más potente y una experiencia de usuario mejorada. Agrega [acceso condicional basado en riesgos](#) a las características de Azure AD Premium P1; se adapta a los patrones del usuario y reduce el número de solicitudes de la autenticación multifactor.

Métodos de autenticación

MÉTODO	VALORES PREDETERMINADOS DE SEGURIDAD	TODOS LOS DEMÁS MÉTODOS
Notificación a través de aplicación móvil	X	X
Código de verificación de aplicación móvil o token de hardware		X
Mensaje de texto al teléfono		X
Llamada al teléfono		X

Pasos siguientes

Para empezar, consulte el tutorial para [eventos de inicio de sesión de usuario seguro con Azure Multi-Factor Authentication](#).

Para más información sobre las licencias, consulte este artículo sobre las [características y licencias de Azure Multi-Factor Authentication](#).

¿Cuáles son los valores de seguridad predeterminados?

22/07/2020 • 15 minutes to read • [Edit Online](#)

Administrar la seguridad puede resultar difícil porque los ataques comunes relacionados con la identidad, como la difusión o reproducción de contraseñas y la suplantación de identidad, se están volviendo cada vez más populares. Los valores predeterminados de seguridad facilitan la protección de la organización frente a estos ataques con opciones de configuración de seguridad preconfiguradas:

- Exigir que todos los usuarios se registren en Azure Multi-Factor Authentication.
- Requerir que los administradores realicen la autenticación multifactor.
- Bloquear los protocolos de autenticación heredados.
- Exigir a los usuarios que realicen la autenticación multifactor cuando sea necesario.
- Proteger las actividades con privilegios, como el acceso a Azure Portal.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons. In the center, under 'Contoso - Properties' (Azure Active Directory), the 'Properties' blade is open. At the bottom of this blade, there are two red boxes: one around the 'Properties' link and another around the 'Manage Security defaults' button. A modal window titled 'Enable Security defaults' is displayed on the right. It contains a descriptive text about security defaults and a toggle switch with 'Yes' and 'No' options, where 'Yes' is selected. This 'Yes' option is also highlighted with a red box.

Para más información sobre por qué los valores predeterminados de seguridad se están poniendo a disposición de todos, vea la entrada de blog de Alex Weinert, [Presentación de los valores predeterminados de seguridad](#).

Disponibilidad

Microsoft pone los valores de seguridad predeterminados a disposición de todos los usuarios. El objetivo es asegurarse de que todas las organizaciones gozen de un nivel básico de seguridad sin ningún costo adicional. Los valores predeterminados de seguridad se activan en Azure Portal. Si el inquilino se creó a partir del 22 de octubre

de 2019, es posible que los valores predeterminados de seguridad ya estén habilitados en el inquilino. En un esfuerzo por proteger a todos nuestros usuarios, los valores predeterminados de seguridad se están implementando en todos los nuevos inquilinos creados.

¿Para quiénes son?

- Para organizaciones que deseen aumentar la posición de seguridad, pero no saben cómo empezar o por dónde.
- Para organizaciones que utilizan el nivel gratis de licencias de Azure Active Directory.

¿Quién debe usar el acceso condicional?

- Si es una organización que usa actualmente directivas de acceso condicional para unificar las señales, tomar decisiones y aplicar las directivas de la organización, es probable que los valores predeterminados de seguridad no sean los más adecuados.
- Si es una organización con licencias de Azure Active Directory Premium, es probable que los valores predeterminados de seguridad tampoco le convengan.
- Sin embargo, si su organización tiene requisitos de seguridad complejos, debería plantearse en cuenta el acceso condicional.

Directivas aplicadas

Registro unificado de Multi-Factor Authentication

Todos los usuarios del inquilino deben registrarse para la autenticación multifactor (MFA) en la forma del servicio Azure Multi-Factor Authentication. Los usuarios tendrán 14 días para registrarse en Azure Multi-Factor Authentication con la aplicación Microsoft Authenticator. Una vez transcurridos los 14 días, el usuario no podrá iniciar sesión hasta que se complete el registro. El período de 14 días de un usuario comienza después del primer inicio de sesión interactivo correcto después de habilitar los valores de seguridad predeterminados.

Protección de los administradores

Los usuarios con acceso a cuentas con privilegios tienen un mayor acceso a su entorno. Dadas las facultades de estas cuentas, debe tratarlas con un cuidado especial. Un método común para mejorar la protección de las cuentas con privilegios es exigir una forma de verificación de la cuenta más estricta para iniciar sesión. En Azure AD, puede exigir el uso de Multi-Factor Authentication para conseguir una verificación de cuentas más estricta.

Una vez finalizado el registro con Azure Multi-Factor Authentication, los nueve roles de administrador de Azure AD siguientes deberán realizar una autenticación adicional cada vez que inicien sesión:

- Administrador global
- Administrador de SharePoint
- Administrador de Exchange
- Administrador de acceso condicional
- Administrador de seguridad
- Administrador del departamento de soporte técnico
- Administrador de facturación
- Administrador de usuarios
- Administrador de autenticación

Protección de todos los usuarios

Se tiende a pensar que las cuentas de administrador son las únicas cuentas que necesitan capas adicionales de autenticación. Los administradores tienen un amplio acceso a información confidencial y pueden realizar cambios en la configuración de toda la suscripción. Sin embargo, los atacantes suelen dirigirse a los usuarios finales.

Una vez que estos atacantes obtienen acceso, pueden solicitar acceso a información privilegiada en nombre del titular de la cuenta original. Incluso pueden descargar todo el directorio para realizar un ataque de suplantación de identidad (phishing) en toda la organización.

Un método común para mejorar la protección de todos los usuarios es exigir a todos una forma más estricta de verificación de cuentas, como Multi-Factor Authentication (MFA). Cuando los usuarios finalicen el registro de Multi-Factor Authentication, se les pedirá una autenticación adicional siempre que sea necesario. Esta funcionalidad protege todas las aplicaciones registradas con Azure AD, incluidas las aplicaciones SaaS.

Bloqueo de la autenticación heredada

Para brindar a los usuarios un acceso sencillo a las aplicaciones en la nube, Azure AD admite una variedad de protocolos de autenticación, incluida la autenticación heredada. La *autenticación heredada* es un término que hace referencia a una solicitud de autenticación realizada por:

- Clientes que no usan la autenticación moderna (por ejemplo, el cliente de Office 2010).
- Cualquier cliente que use protocolos de correo antiguos, como IMAP, SMTP o POP3.

Hoy en día, la mayoría de los intentos de inicio de sesión que ponen en peligro la seguridad proceden de la autenticación heredada. La autenticación heredada no admite Multi-Factor Authentication. Incluso si tiene una directiva de Multi-Factor Authentication habilitada en el directorio, un atacante puede autenticarse mediante un protocolo antiguo y omitir Multi-Factor Authentication.

Después de habilitar los valores de seguridad predeterminados en el inquilino, se bloquearán todas las solicitudes de autenticación realizadas con un protocolo antiguo. Los valores predeterminados de seguridad bloquean la autenticación básica de Exchange Active Sync.

WARNING

Antes de habilitar los valores predeterminados de seguridad, asegúrese de que los administradores no estén usando protocolos de autenticación antiguos. Para más información, consulte [Cómo cambiar la autenticación heredada](#).

- [Cómo configurar una aplicación o dispositivo multifunción para enviar correos electrónicos mediante Office 365 y Microsoft 365](#)

Protección de acciones con privilegios

Las organizaciones usan diversos servicios de Azure que se administran mediante la API de Azure Resource Manager, entre ellos:

- Azure portal
- Azure PowerShell
- Azure CLI

El uso de Azure Resource Manager para administrar los servicios es una acción con privilegios elevados. Azure Resource Manager puede modificar las configuraciones de todo el inquilino, como la configuración del servicio y la facturación de la suscripción. La autenticación de factor único es vulnerable a una variedad de ataques, como la suplantación de identidad (phishing) y la difusión de contraseñas.

Es importante comprobar la identidad de los usuarios que quieren acceder a Azure Resource Manager y actualizar las configuraciones. Para comprobar su identidad, solicite una autenticación adicional antes de permitir el acceso.

Después de habilitar los valores de seguridad predeterminados en el inquilino, se pedirá a todos los usuarios que accedan al Azure Portal, Azure PowerShell o la CLI de Azure que completen una autenticación adicional. Esta directiva se aplica a todos los usuarios que acceden a Azure Resource Manager, independientemente de si son administradores o usuarios.

NOTE

Los inquilinos de Exchange Online anteriores a 2017 tienen la autenticación moderna deshabilitada de forma predeterminada. Para evitar la posibilidad de que se produzca un bucle de inicio de sesión durante la autenticación a través de estos inquilinos, debe [habilitar la autenticación moderna](#).

NOTE

La cuenta de sincronización de Azure AD Connect se excluye de los valores predeterminados de seguridad y no se le pedirá que se registre ni que realice la autenticación multifactor. Las organizaciones no deben usar esta cuenta para otros fines.

Consideraciones de la implementación

A continuación, se muestran consideraciones adicionales relacionadas con la implementación de los valores de seguridad predeterminados.

Métodos de autenticación

Los valores predeterminados de seguridad permiten el registro y el uso de Azure Multi-Factor Authentication mediante **el uso exclusivo de la aplicación Microsoft Authenticator con notificaciones**. El acceso condicional permite el uso de cualquier método de autenticación que el administrador decida habilitar.

MÉTODO	VALORES PREDETERMINADOS DE SEGURIDAD	ACCESO CONDICIONAL
Notificación a través de aplicación móvil	X	X
Código de verificación de aplicación móvil o token de hardware	X**	X
Mensaje de texto al teléfono		X
Llamada al teléfono		X
Contraseñas de aplicación		X***

- ** Los usuarios pueden usar códigos de verificación de la aplicación Microsoft Authenticator, pero solo pueden registrarse mediante la opción de notificación.
- *** Las contraseñas de aplicación solo están disponibles en MFA por usuario con escenarios de autenticación heredados si las habilitan los administradores.

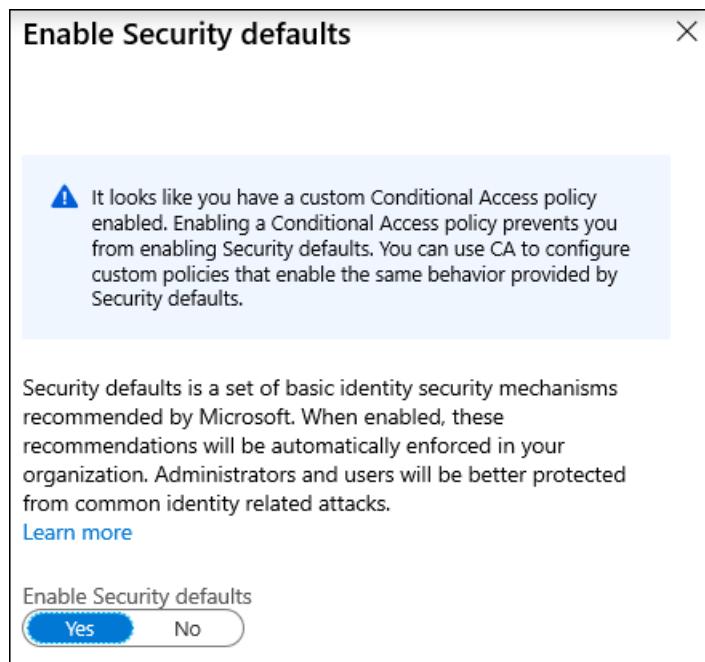
Estado de MFA deshabilitado

Si su organización es un usuario anterior de Azure Multi-Factor Authentication basado en usuarios, no se alarme si no ve usuarios con el estado **Habilitado** o **Aplicado** en la página de estado de Microsoft Azure Multi-Factor Authentication. **Deshabilitado** es el estado adecuado para los usuarios que usan valores predeterminados de seguridad o Azure Multi-Factor Authentication basado en el acceso condicional.

Acceso condicional

Puede usar el acceso condicional para configurar directivas similares a los valores predeterminados de seguridad, pero con más granularidad, incluidas las exclusiones de usuario, que no están disponibles en los valores predeterminados de seguridad. Si usa acceso condicional y tiene habilitadas directivas de acceso condicional en su entorno, los valores de seguridad predeterminados no estarán disponibles. Si tiene una licencia que proporciona acceso condicional, pero no tiene ninguna directiva de acceso condicional habilitada en su entorno, puede usar los

valores de seguridad predeterminados hasta que habilite las directivas de acceso condicional. Para más información sobre las licencias de Azure AD, consulte la [página de precios de Azure AD](#).



Estas son las guías paso a paso sobre cómo se puede usar el acceso condicional para configurar directivas equivalentes en las directivas habilitadas por los valores predeterminados de seguridad:

- [Exigir autenticación multifactor para administradores](#)
- [Exigir autenticación multifactor para la administración de Azure](#)
- [Bloquear la autenticación heredada](#)
- [Exigir autenticación multifactor para todos los usuarios](#)
- [Requerir el registro de Azure MFA](#): Requiere Azure AD Identity Protection como parte de Azure AD Premium P2.

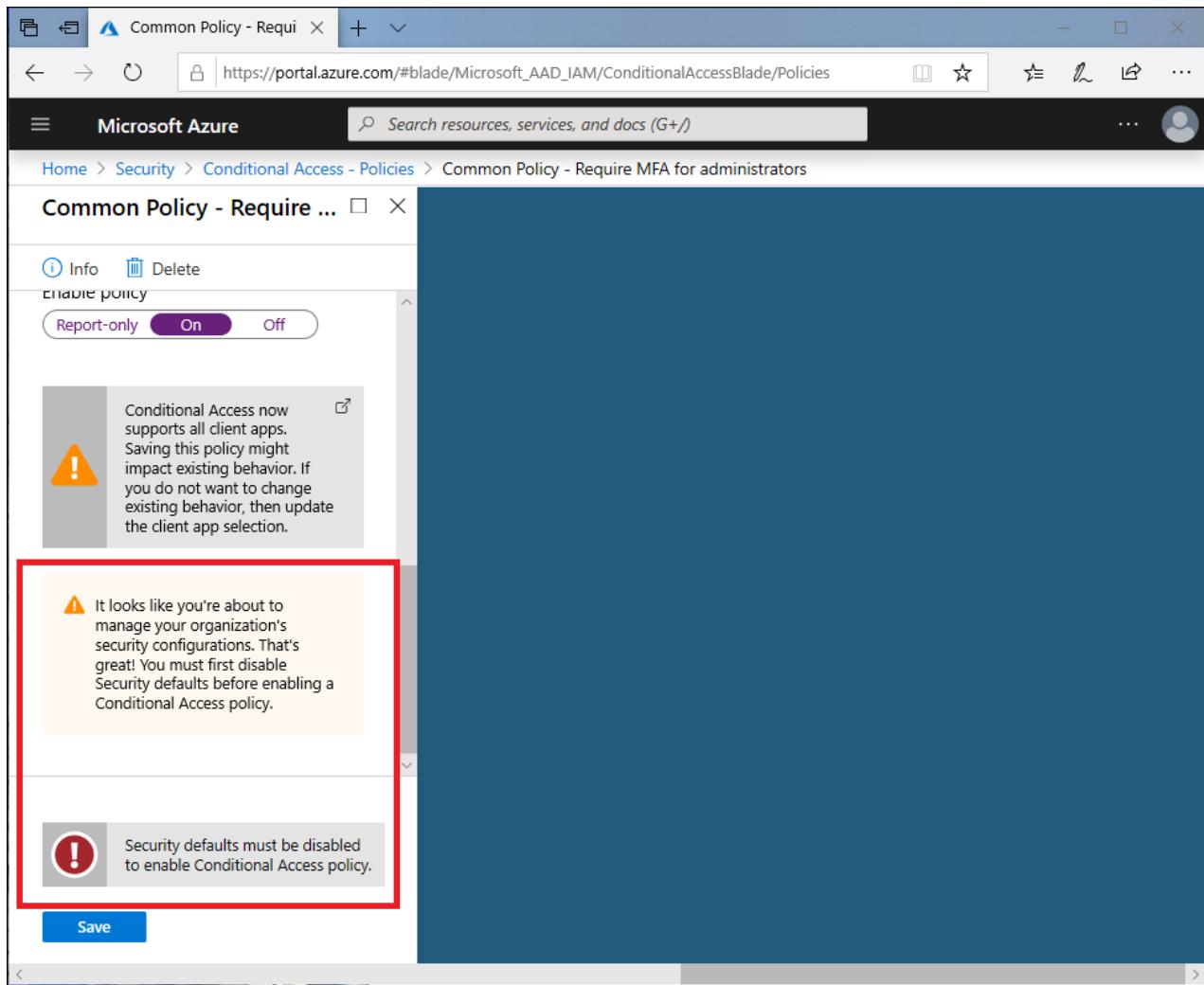
Habilitación de los valores de seguridad predeterminados

Para habilitar los valores de seguridad predeterminados en su directorio:

1. Inicie sesión en [Azure Portal](#) como administrador global, administrador de seguridad o administrador de acceso condicional.
2. Vaya a **Azure Active Directory > Propiedades**.
3. Seleccione **Administrar valores predeterminados de seguridad**.
4. Establezca **Habilitar valores predeterminados de seguridad** en **Sí**.
5. Seleccione **Guardar**.

Deshabilitación de los valores predeterminados de seguridad

Las organizaciones que decidan implementar directivas de acceso condicional que reemplacen los valores predeterminados de seguridad deben deshabilitar estos últimos.



Para deshabilitar los valores predeterminados de seguridad en el directorio:

1. Inicie sesión en [Azure Portal](#) como administrador global, administrador de seguridad o administrador de acceso condicional.
2. Vaya a **Azure Active Directory > Propiedades**.
3. Seleccione **Administrar valores predeterminados de seguridad**.
4. Establezca **Activación de los valores predeterminados de seguridad** en **No**.
5. Seleccione **Guardar**.

Pasos siguientes

[Directivas de acceso condicional habituales](#)

Bloqueo de la autenticación heredada

22/07/2020 • 14 minutes to read • [Edit Online](#)

Para brindar a los usuarios un acceso sencillo a las aplicaciones en la nube, Azure Active Directory (Azure AD) admite una amplia variedad de protocolos de autenticación, incluida la autenticación heredada. La autenticación heredada es un término que hace referencia a una solicitud de autenticación realizada por:

- Clientes de Office antiguos que no usan la autenticación moderna (por ejemplo, el cliente de Office 2010)
- Cualquier cliente que use protocolos de correo heredados, como IMAP, SMTP o POP3

Hoy en día, la mayoría de los intentos de inicio de sesión que ponen en peligro la seguridad proceden de la autenticación heredada. La autenticación heredada no admite la autenticación multifactor (MFA). Aunque tenga una directiva MFA habilitada en su directorio, un actor malintencionado puede autenticarse mediante un protocolo heredado y omitir MFA. La mejor manera de proteger su cuenta frente a las solicitudes de autenticación malintencionadas que realizan los protocolos heredados es bloquear todos estos intentos.

Identificación del uso de la autenticación heredada

Para poder bloquear la autenticación heredada en su directorio, primero debe entender si los usuarios tienen aplicaciones que la usen y cómo afecta a su directorio global. Se pueden usar los registros de inicio de sesión de Azure AD para saber si usa la autenticación heredada.

1. Vaya a [Azure Portal](#) > Azure Active Directory > Inicios de sesión.
2. Agregue la columna **Aplicación cliente** si no se muestra; para ello, haga clic en **Columnas** > **Aplicación cliente**.
3. Filtre por **Aplicación cliente** y marque todas las opciones de **Clientes de autenticación heredados** que se presentan.
4. Filtre por **Estado > Correcto**.
5. Expanda el intervalo de fechas si es necesario con el filtro **Fecha**.

Al filtrar solo se mostrarán los intentos de inicio de sesión correctos que se realizaron con los protocolos seleccionados de autenticación heredada. Al hacer clic en cada intento de inicio de sesión individual se muestran detalles adicionales. La columna Aplicación cliente o el campo Aplicación cliente de la pestaña Información básica indicará el protocolo de autenticación heredado que se usó, después de seleccionar una fila de datos individual. Estos registros indicarán qué usuarios dependen todavía de la autenticación heredada y qué aplicaciones usan protocolos heredados para realizar solicitudes de autenticación. Para los usuarios que no aparecen en estos registros y se les confirme que no van a usar la autenticación heredada, implemente una directiva de acceso condicional o habilite la directiva de base de referencia: bloqueo de la autenticación heredada solo para estos usuarios.

Retirada de la autenticación heredada

Una vez que tenga una idea más clara de quién está usando la autenticación heredada en su directorio y las aplicaciones que dependen de esta, el siguiente paso es actualizar a los usuarios para que usen la autenticación moderna. La autenticación moderna es un método de administración de identidades que ofrece una autenticación y autorización de usuario más seguras. Si tiene una directiva de MFA implementada en su directorio, la autenticación moderna garantiza que MFA se solicita al usuario cuando es necesario. Se trata de la alternativa más segura a los protocolos de autenticación heredados.

En esta sección se ofrece una introducción paso a paso sobre cómo actualizar el entorno para la autenticación

moderna. Lea los pasos siguientes antes de habilitar una directiva de bloqueo de la autenticación heredada en su organización.

Paso 1: Habilitación de la autenticación moderna en su directorio

El primer paso para habilitar la autenticación moderna es asegurarse de que el directorio admite la autenticación moderna. La autenticación moderna está habilitada de forma predeterminada para los directorios que creó el día 1 de agosto de 2017 o a partir de esta fecha. Si el directorio se creó antes de esta fecha, deberá habilitar manualmente la autenticación moderna para su directorio mediante los pasos siguientes:

1. Compruebe si el directorio ya admite la autenticación moderna mediante la ejecución de `Get-CsOAuthConfiguration` desde el [módulo de PowerShell de Skype Empresarial en la Web](#).
2. Si el comando devuelve una propiedad `OAuthServers` vacía, la autenticación moderna se deshabilita. Actualice la configuración para habilitar la autenticación moderna mediante `Set-CsOAuthConfiguration`. Si la propiedad `OAuthServers` contiene una entrada, significa que está listo para empezar.

Asegúrese de completar este paso antes de continuar. Es fundamental cambiar primero las configuraciones de directorio, ya que estas dictan qué protocolo usarán todos los clientes de Office. Aunque use clientes de Office que admitan la autenticación moderna, usarán de manera predeterminada protocolos heredados si la autenticación moderna está deshabilitada en su directorio.

Paso 2: Aplicaciones de Office

Una vez que haya habilitado la autenticación moderna en su directorio, puede empezar a actualizar las aplicaciones mediante la habilitación de la autenticación moderna para clientes de Office. Office 2016 o los clientes posteriores admiten la autenticación moderna de forma predeterminada. No se requiere ningún paso adicional.

Si usa clientes de Windows con Office 2013 o una versión anterior, se recomienda actualizar a Office 2016 o posterior. Incluso después de completar el paso anterior para habilitar la autenticación moderna en su directorio, las aplicaciones de Office anteriores seguirán usando protocolos de autenticación heredados. Si usa clientes de Office 2013 y no puede actualizar inmediatamente a Office 2016 o posterior, siga los pasos descritos en el siguiente artículo para [Habilitar la autenticación moderna para Office 2013 en los dispositivos Windows](#). Para ayudar a proteger su cuenta mientras usa la autenticación heredada, le recomendamos que use contraseñas seguras en su directorio. Consulte el artículo sobre [protección con contraseña de Azure AD](#) para prohibir las contraseñas no seguras en su directorio.

Office 2010 no admite la autenticación moderna. Deberá actualizar todos los usuarios con Office 2010 a una versión más reciente de Office. Le recomendamos que actualice a Office 2016 o posterior, ya que bloquea la autenticación heredada de forma predeterminada.

Si usa macOS, se recomienda actualizar a Office para Mac 2016 o posterior. Si usa el cliente de correo electrónico nativo, deberá tener la versión de macOS 10.14 o posterior en todos los dispositivos.

Paso 3: Exchange y SharePoint

Para que los clientes de Outlook basado en Windows usen la autenticación moderna, Exchange Online también debe tener habilitada la autenticación moderna. Si se deshabilita la autenticación moderna para Exchange Online, los clientes de Outlook basado en Windows que admiten la autenticación moderna (Outlook 2013 o versiones posteriores) usarán la autenticación básica para conectarse a buzones de Exchange Online.

SharePoint Online está habilitado de forma predeterminada para la autenticación moderna. En el caso de los directorios creados a partir del 1 de agosto de 2017, la autenticación moderna está habilitada de forma predeterminada en Exchange Online. Sin embargo, si anteriormente tenía deshabilitada la autenticación moderna o usa un directorio creado antes de esta fecha, siga los pasos descritos en el artículo [Habilitar la autenticación moderna en Exchange Online](#).

Paso 4: Skype Empresarial

Para evitar las solicitudes de autenticación heredadas realizadas por Skype Empresarial, es necesario habilitar la

autenticación moderna para Skype Empresarial en la Web. En el caso de los directorios creados a partir del 1 de agosto de 2017, la autenticación moderna está habilitada de forma predeterminada en Skype Empresarial.

Le sugerimos que realice la transición a Microsoft Teams, que admite la autenticación moderna de forma predeterminada. Sin embargo, si no puede migrar en este momento, deberá habilitar la autenticación moderna para Skype Empresarial en la Web para que Skype Empresarial empiece a usar la autenticación moderna. Consulte los pasos del artículo [Topologías de Skype Empresarial admitidas con la autenticación moderna](#) para habilitar la autenticación moderna para Skype Empresarial.

Además de habilitar la autenticación moderna para Skype Empresarial en la Web, le recomendamos que habilite la autenticación moderna para Exchange Online cuando habilite la autenticación moderna para Skype Empresarial. Este proceso permitirá sincronizar el estado de la autenticación moderna en Exchange Online y Skype Empresarial en la Web y evitará que se realicen varias solicitudes de inicio de sesión de los clientes de Skype Empresarial.

Paso 5: Uso de dispositivos móviles

Las aplicaciones de su dispositivo móvil también necesitan bloquear la autenticación heredada. Le recomendamos usar Outlook para dispositivos móviles. Outlook para móviles admite la autenticación moderna de forma predeterminada y cumplirá otras directivas de protección de la base de referencia de MFA.

Para usar el cliente de correo electrónico nativo de iOS, deberá ejecutar la versión 11.0 u otra posterior de iOS para asegurarse de que el cliente de correo electrónico se ha actualizado a fin de bloquear la autenticación heredada.

Paso 6: Clientes locales

Si es un cliente híbrido que usa Exchange Server y Skype Empresarial en el entorno local, ambos servicios deberán actualizarse para habilitar la autenticación moderna. Cuando usa la autenticación moderna en un entorno híbrido, igualmente autentica a los usuarios en el entorno local. Sin embargo, el proceso para autorizar su acceso a los recursos (archivos o mensajes de correo electrónico) cambia.

Antes de poder empezar a habilitar la autenticación moderna en el entorno local, asegúrese de que cumple los requisitos previos. Ahora está listo para habilitar la autenticación moderna en el entorno local.

Los pasos para habilitar la autenticación moderna se encuentran en los artículos siguientes:

- [Cómo configurar Exchange Server local para usar la autenticación moderna híbrida](#)
- [Cómo usar la autenticación moderna \(ADAL\) con Skype Empresarial](#)

Pasos siguientes

- [Cómo configurar Exchange Server local para usar la autenticación moderna híbrida](#)
- [Cómo usar la autenticación moderna \(ADAL\) con Skype Empresarial](#)
- [Bloquear la autenticación heredada](#)

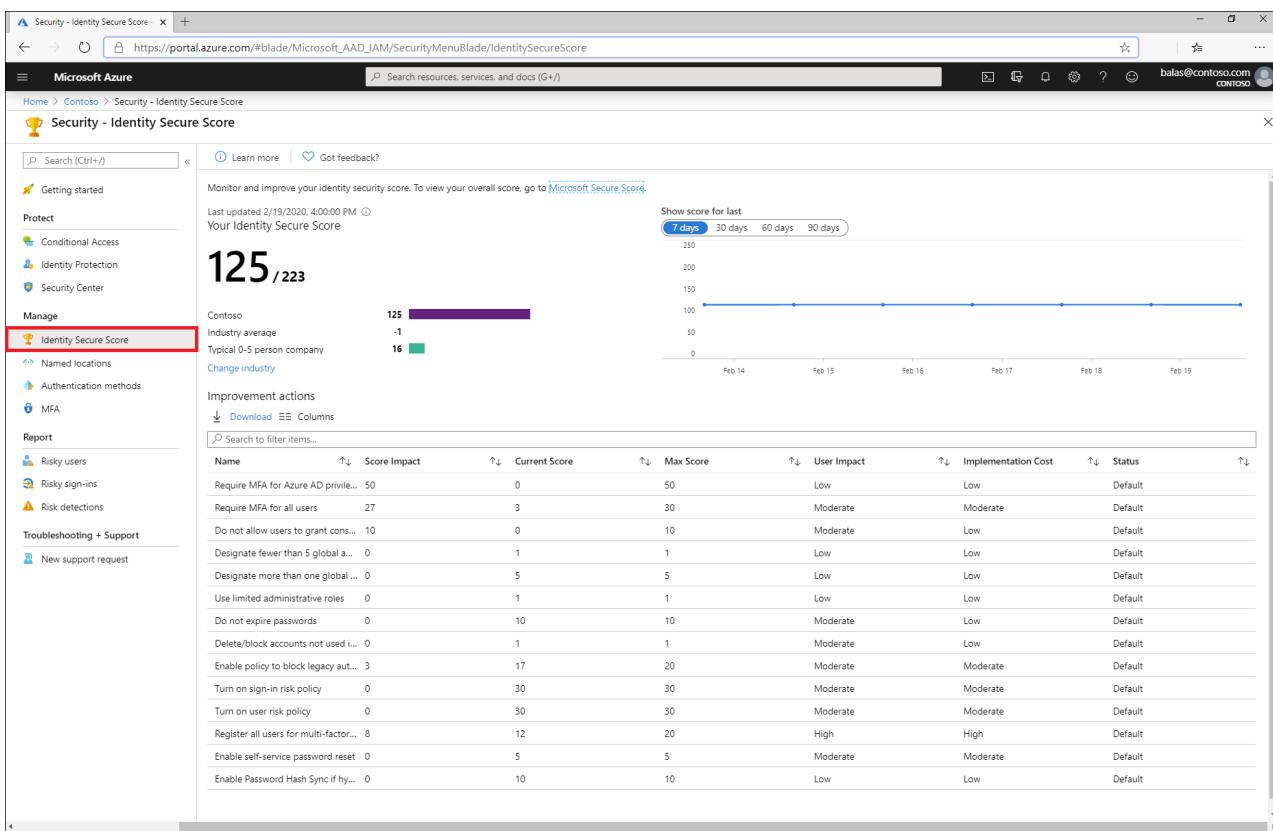
¿Qué es la puntuación segura de identidad en Azure Active Directory?

22/07/2020 • 10 minutes to read • [Edit Online](#)

¿Es seguro un inquilino de Azure AD? Si no sabe qué responder a esta pregunta, en este artículo se explica cómo le ayuda la puntuación segura de identidad a supervisar y mejorar el nivel de seguridad de la identidad.

¿Qué es una puntuación segura de identidad?

La puntuación segura de identidad es un número entre 1 y 223 que funciona como indicador del grado de cumplimiento de las recomendaciones del procedimiento recomendado de Microsoft relativo a la seguridad. Cada acción de mejora de la puntuación segura de identidad se adapta a la configuración específica.



La puntuación le ayuda a:

- Medir de forma objetiva su nivel de seguridad de la identidad
- Planear la realización de mejoras en la seguridad de la identidad
- Ver si las mejoras han logrado sus objetivos

Puede acceder tanto a la puntuación como a la información relacionada en el panel de la puntuación segura de identidad. En dicho panel, encontrará:

- Su puntuación segura de identidad
- Un gráfico de comparación de su puntuación segura de identidad con otros inquilinos del mismo sector y tamaño similar
- Un gráfico de tendencias que muestra cómo ha cambiado su puntuación segura de identidad con el tiempo
- Una lista de posibles mejoras

Si realiza las acciones de mejora, puede:

- Mejorar su nivel de seguridad y su puntuación
- Aprovechar las características disponibles para su organización como parte de sus inversiones en identidad

¿Cómo se obtiene la puntuación segura?

La puntuación segura de identidad está disponible en todas las ediciones de Azure AD. Las organizaciones pueden acceder a su puntuación de seguridad de la identidad desde **Azure Portal > Azure Active Directory > Seguridad > Puntuación de seguridad de la identidad**.

¿Cómo funciona?

Cada 48 horas, Azure examina la configuración de seguridad y compara los valores con los procedimientos recomendados. En función del resultado de esta evaluación, se calcula una nueva puntuación para el directorio. Es posible que la configuración de seguridad no esté completamente alineada con la guía del procedimiento recomendado y que las acciones de mejora solo se cumplan parcialmente. En estos casos, solo se le premiará con una parte de la puntuación máxima disponible para el control.

Cada recomendación se mide según la configuración de Azure AD. Si usa productos de terceros para habilitar una recomendación del procedimiento recomendado, puede indicar esta configuración en las opciones de una acción de mejora. También tiene la opción de establecer que se ignoren las recomendaciones si no se aplican a su entorno. Las recomendaciones ignoradas no contribuyen al cálculo de la puntuación.

The screenshot shows the 'Improvement action' dialog box. At the top, it says 'Delete/block accounts not used in last 30 days'. Below that, 'SCORE IMPACT' is listed as '+0'. The 'CURRENT SCORE' is '1', and the 'MAX SCORE' is also '1'. A red box highlights the 'STATUS' section, which includes 'Default', 'Ignore', and 'Third party'. A note below states: 'Use of inactive accounts. These accounts can be targets for attackers who are looking to find ways to access your data without being noticed. You have 0 accounts that have not been used in the last 30 days.' Under 'USER IMPACT', it says 'Moderate'. Under 'IMPLEMENTATION COST', it says 'Secure score updates can take up to 48 hours.' At the bottom, there is a 'Save' button.

¿Cómo me ayuda?

La puntuación segura le ayuda a:

- Medir de forma objetiva su nivel de seguridad de la identidad
- Planear la realización de mejoras en la seguridad de la identidad
- Ver si las mejoras han logrado sus objetivos

Qué debería saber

¿Quién puede usar la puntuación segura de identidad?

La puntuación segura de identidad pueden usarla los roles siguientes:

- Administrador global
- Administrador de seguridad
- Lectores de seguridad

¿Cómo se puntúan los controles?

Los controles se pueden puntuar de dos maneras. Algunos se puntúan en forma binaria: obtiene el 100 % de la puntuación si tiene la característica o la opción configurada según nuestra recomendación. Otras puntuaciones se calculan como un porcentaje de la configuración total. Por ejemplo, si la recomendación de mejora indica que obtendrá 30 puntos si protege a todos los usuarios con MFA y solo tiene protegidos 5 usuarios de un total de 100, se le otorgará una puntuación parcial de aproximadamente 2 puntos ($5 \text{ protegidos}/100 \text{ totales} * 30 \text{ puntos máximos} = 2 \text{ puntos de puntuación parcial}$).

¿Qué significa [Not Scored]?

Las acciones con la etiqueta [Not Scored] (Sin puntuación) son las que puede realizar en su organización, pero que no se puntúan porque no están conectadas en la herramienta (aún). Por consiguiente, puede mejorar aún más la seguridad, pero no obtendrá ninguna puntuación por esas acciones ahora mismo.

¿Con qué frecuencia se actualiza la puntuación?

La puntuación se calcula una vez al día (aproximadamente a las 1:00 A.M., hora del Pacífico). Si realiza algún cambio en una acción medida, la puntuación se actualizará automáticamente al día siguiente. Cualquier cambio tarda hasta 48 horas en reflejarse en la puntuación.

Mi puntuación ha cambiado. ¿Cómo averiguo por qué?

Vaya al [Centro de seguridad de Microsoft 365](#), donde encontrará su puntuación segura de Microsoft completa. Puede ver fácilmente todos los cambios de la puntuación segura mediante la revisión de los cambios detallados en la pestaña Historial.

¿Mide la puntuación segura el riesgo de vulneración de la seguridad?

En pocas palabras, no. La puntuación segura no expresa una medida absoluta de la probabilidad de sufrir una vulneración de la seguridad. Expresa en qué medida ha adoptado características que pueden compensar el riesgo de vulneración de la seguridad. Ningún servicio puede garantizar que no va a sufrir una vulneración de la seguridad y la puntuación segura no se debe interpretar de ningún modo como una garantía.

¿Cómo debo interpretar la puntuación?

Se le dan puntos por configurar las características de seguridad recomendadas o por realizar tareas relacionadas con la seguridad (como la lectura de informes). Se puntúan algunas acciones por la finalización parcial, como por ejemplo, habilitar la autenticación multifactor (MFA) para los usuarios. Su puntuación segura representa directamente los servicios de seguridad de Microsoft que usa. Recuerde que debe existir un equilibrio entre seguridad y facilidad de uso. Todos los controles de seguridad tienen un componente de impacto en el usuario. Los controles que tienen un impacto bajo en el usuario deben tener poco o ningún efecto en las operaciones diarias de los usuarios.

Para ver el historial de puntuación, diríjase al [Centro de seguridad de Microsoft 365](#) y revise su puntuación segura

de Microsoft. Puede revisar los cambios de su puntuación segura general haciendo clic en Vista de historial. Elija una fecha concreta para ver los controles que se han habilitado para ese día y los puntos que ha logrado por cada uno de ellos.

¿Cómo se relaciona la puntuación segura de identidad con la puntuación segura de Office 365?

La [puntuación segura de Microsoft](#) contiene cinco categorías distintas de control y puntuación:

- Identidad
- data
- Dispositivos
- Infraestructura
- Aplicaciones

La puntuación segura de identidad representa la parte de la identidad de la puntuación segura de Microsoft, lo que significa que las recomendaciones de la puntuación segura de identidad y la puntuación de identidad en Microsoft son idénticas.

Pasos siguientes

[Obtener más información acerca de la puntuación segura de Microsoft](#)

Respuesta rápida para proteger identidades con Azure AD

22/07/2020 • 26 minutes to read • [Edit Online](#)

Tratar de proteger a sus trabajadores en el mundo actual puede parecer desalentador, especialmente cuando tiene que responder rápidamente y proporcionar acceso a muchos servicios con rapidez. Este artículo está pensado para proporcionar una lista concisa de todas las acciones que se deben llevar a cabo, lo que ayuda a identificar y priorizar el orden de implementación de las características de Azure AD en función del tipo de licencia que posea. Azure AD ofrece muchas características y proporciona muchos niveles de seguridad para las identidades, ya que determinar qué característica es relevante puede resultar abrumador en ocasiones. Muchas organizaciones ya están en la nube o están migrando rápidamente a la misma; este documento está diseñado para permitirle implementar servicios rápidamente, con la protección de las identidades como consideración principal.

Cada tabla proporciona una recomendación de seguridad coherente, que protege las identidades de usuario y administrador de los principales ataques de seguridad (la reproducción de infracciones, la suplantación de identidad [phishing] y la difusión de contraseñas), a la vez que minimiza el impacto del usuario y mejora su experiencia.

Las instrucciones también permitirán a los administradores configurar el acceso a las aplicaciones SaaS y locales de manera segura, se podrán aplicar a las identidades de nube o híbridas (sincronizadas) y se aplicarán a los usuarios que trabajan de forma remota o en la oficina.

Esta lista de comprobación le ayudará a implementar rápidamente las acciones críticas recomendadas para proteger su organización de inmediato; en ella se explica cómo:

- Reforzar las credenciales.
- Reducir el área de la superficie de ataque.
- Automatizar la respuesta frente a amenazas.
- Usar Cloud Intelligence.
- Habilitar el autoservicio del usuario final.

Prerrequisitos

En esta guía se da por supuesto que ya se han establecido en Azure AD las identidades híbridas o en la nube. Para obtener ayuda para elegir un tipo de identidad, consulte el artículo [Selección del método de autenticación adecuado para su solución de identidad híbrida de Azure Active Directory](#).

Resumen

Existen muchos aspectos en una infraestructura de identidad segura, pero esta lista de comprobación se centra en una que permite a los usuarios trabajar de forma remota. La protección de su identidad es solo una parte de la seguridad; también se debe tener en cuenta la protección de datos, las aplicaciones y los dispositivos.

Guía para clientes de Azure AD Free u Office 365

Hay una serie de recomendaciones que los clientes de la aplicación Azure AD Free u Office 365 deben seguir para proteger sus identidades de usuario. La tabla siguiente tiene como objetivo resaltar las acciones clave de las siguientes suscripciones de licencia:

- Office 365 (O365 E1, E3, E5, F1, A1, A3, A5)
- Office 365 Empresa (Essentials, Empresa, Empresa Premium)

- Microsoft 365 (M365 Empresa, A1)
- Azure AD Free (incluido con Azure, Dynamics 365, Intune y Power Platform)

ACCIÓN RECOMENDADA	DETALL
Habilitar los valores predeterminados de seguridad	Proteja todas las aplicaciones e identidades de usuario al habilitar MFA y bloquear la autenticación heredada.
Habilitar la sincronización de hash de contraseñas (si se usan identidades híbridas)	Proporcione redundancia para la autenticación y mejore la seguridad (incluido el bloqueo inteligente, el bloqueo de IP y la capacidad de detectar las credenciales filtradas).
Habilitar el bloqueo inteligente de ADFS (si procede)	Protege a los usuarios de los bloqueos de cuentas de extranet debido a actividades malintencionadas.
Habilitar el bloqueo inteligente de Azure Active Directory (si se usan identidades administradas)	El bloqueo inteligente ayuda a bloquear a los actores malintencionados que intentan adivinar las contraseñas de los usuarios o que usan métodos de fuerza bruta para obtenerlas.
Deshabilitar el consentimiento del usuario final a las aplicaciones	El flujo de trabajo de consentimiento del administrador proporciona a los administradores una manera segura de conceder acceso a las aplicaciones que requieren la aprobación del administrador, de modo que los usuarios finales no expongan los datos de la empresa. Microsoft recomienda deshabilitar las operaciones futuras de consentimiento del usuario para ayudar a reducir el área expuesta y a mitigar este riesgo.
Integrar aplicaciones SaaS compatibles de la galería con Azure AD y habilitar el inicio de sesión único	Azure AD incluye una galería que contiene miles de aplicaciones previamente integradas. Algunas de las aplicaciones que su organización usa probablemente estén en la galería y se pueda acceder a ellas desde Azure Portal. Proporcione acceso a las aplicaciones SaaS empresariales de forma remota y segura mediante una experiencia de usuario mejorada (SSO).
Automatizar el aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS (si procede)	Cree automáticamente roles e identidades de usuario en las aplicaciones en la nube (SaaS) a las que los usuarios necesitan acceder. Además de crear identidades de usuario, el aprovisionamiento automático incluye el mantenimiento y la eliminación de identidades de usuario a medida que el estado o los roles cambian, de modo que mejora la seguridad de su organización.
Habilitar el acceso híbrido seguro: Protección de aplicaciones heredadas con redes y controladores de entrega de aplicaciones existentes (si procede)	Publique y proteja sus aplicaciones de autenticación heredadas locales y en la nube conectándolas a Azure AD con su red o controlador de entrega de aplicaciones existentes.
Habilitar el autoservicio de restablecimiento de contraseña (aplicable solo a cuentas en la nube)	Esta capacidad reduce las llamadas al departamento de soporte técnico y la pérdida de productividad cuando un usuario no puede iniciar sesión en su dispositivo o en una aplicación.
Uso de roles de administrador no global siempre que sea posible	Asigne a los administradores solo el acceso que necesitan a las áreas a las que necesitan acceso. No todos los administradores necesitan ser administradores globales.

ACCIÓN RECOMENDADA	DETAIL
Habilitación de la guía de contraseñas de Microsoft	Olvídense de solicitar a los usuarios que cambien periódicamente la contraseña, deshabilite los requisitos de complejidad y a los usuarios les será más fácil recordar la contraseña y mantener una segura.

Instrucciones para los clientes del plan 1 de Azure AD Premium

La tabla siguiente tiene como objetivo resaltar las acciones clave de las siguientes suscripciones de licencia:

- Azure Active Directory Premium P1 (Azure AD P1)
- Enterprise Mobility + Security (EMS E3)
- Microsoft 365 (M365 E3, A3, F1, F3)

ACCIÓN RECOMENDADA	DETAIL
Habilitar la experiencia de registro combinada para Azure MFA y SSPR para simplificar la experiencia de registro del usuario	Permita que los usuarios se registren para una de las experiencias comunes: Azure Multi-Factor Authentication o el autoservicio de restablecimiento de contraseña.
Configurar MFA para su organización	Asegúrese de que las cuentas están protegidas frente a los riesgos de la autenticación multifactor.
Habilitar el autoservicio de restablecimiento de contraseña	Esta capacidad reduce las llamadas al departamento de soporte técnico y la pérdida de productividad cuando un usuario no puede iniciar sesión en su dispositivo o en una aplicación.
Implementar la escritura diferida de contraseñas (si usa identidades híbridas)	Permita la escritura diferida de los cambios de contraseña en la nube en un entorno de Windows Server Active Directory local.
Crear y habilitar directivas de acceso condicional	<p>MFA para que los administradores protejan las cuentas a las que se asignan derechos administrativos.</p> <p>Bloquear los protocolos de autenticación heredados debido al aumento de riesgo asociado a los protocolos de autenticación heredados.</p> <p>MFA para que todos los usuarios y las aplicaciones creen una directiva de MFA equilibrada para el entorno, protegiendo a los usuarios y las aplicaciones.</p> <p>Exigir que MFA para Azure Management proteja los recursos con privilegios al requerir la autenticación multifactor para cualquier usuario que tenga acceso a recursos de Azure.</p>
Habilitar la sincronización de hash de contraseñas (si se usan identidades híbridas)	Proporcione redundancia para la autenticación y mejore la seguridad (incluido el bloqueo inteligente, el bloqueo de IP y la capacidad de detectar las credenciales filtradas).
Habilitar el bloqueo inteligente de ADFS (si procede)	Protege a los usuarios de los bloqueos de cuentas de extranet debido a actividades malintencionadas.
Habilitar el bloqueo inteligente de Azure Active Directory (si se usan identidades administradas)	El bloqueo inteligente ayuda a bloquear a los actores malintencionados que intentan adivinar las contraseñas de los usuarios o que usan métodos de fuerza bruta para obtenerlas.

ACCIÓN RECOMENDADA	DETAIL
Deshabilitar el consentimiento del usuario final a las aplicaciones	El flujo de trabajo de consentimiento del administrador proporciona a los administradores una manera segura de conceder acceso a las aplicaciones que requieren la aprobación del administrador, de modo que los usuarios finales no expongan los datos de la empresa. Microsoft recomienda deshabilitar las operaciones futuras de consentimiento del usuario para ayudar a reducir el área expuesta y a mitigar este riesgo.
Habilitar el acceso remoto a las aplicaciones heredadas locales con Application Proxy	Habilite Azure AD Application Proxy e intégrela con aplicaciones heredadas para que los usuarios tengan acceso seguro a aplicaciones locales, iniciando sesión con su cuenta de Azure AD.
Habilitar el acceso híbrido seguro: Protección de aplicaciones heredadas con redes y controladores de entrega de aplicaciones existentes (si procede)	Publique y proteja sus aplicaciones de autenticación heredadas locales y en la nube conectándolas a Azure AD con su red o controlador de entrega de aplicaciones existentes.
Integrar aplicaciones SaaS compatibles de la galería con Azure AD y habilitar el inicio de sesión único	Azure AD incluye una galería que contiene miles de aplicaciones previamente integradas. Algunas de las aplicaciones que su organización usa probablemente estén en la galería y se pueda acceder a ellas desde Azure Portal. Proporcione acceso a las aplicaciones SaaS empresariales de forma remota y segura mediante una experiencia de usuario mejorada (SSO).
Automatizar el aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS (si procede)	Cree automáticamente roles e identidades de usuario en las aplicaciones en la nube (SaaS) a las que los usuarios necesitan acceder. Además de crear identidades de usuario, el aprovisionamiento automático incluye el mantenimiento y la eliminación de identidades de usuario a medida que el estado o los roles cambian, de modo que mejora la seguridad de su organización.
Habilitar el acceso condicional basado en dispositivos	Mejore la seguridad y las experiencias de usuario con el acceso condicional basado en dispositivos. Este paso garantiza que los usuarios solo pueden tener acceso desde dispositivos que cumplen los estándares de seguridad y cumplimiento. A estos dispositivos también se les conoce como dispositivos administrados. Los dispositivos administrados pueden ser conformes con Intune o dispositivos unidos a Azure AD híbrido.
Habilitar la protección con contraseña	Proteja a los usuarios del uso de contraseñas poco seguras y fáciles de adivinar.
Designación de más de un administrador global	Asigne al menos dos cuentas de administrador global permanentes solo en la nube para casos de emergencia. Estas cuentas no son para un uso diario y deben tener contraseña compleja y larga. Las cuentas de acceso de emergencia garantizan el acceso al servicio en situaciones de emergencia.
Uso de roles de administrador no global siempre que sea posible	Asigne a los administradores solo el acceso que necesitan a las áreas a las que necesitan acceso. No todos los administradores necesitan ser administradores globales.

ACCIÓN RECOMENDADA	DETAIL
Habilitación de la guía de contraseñas de Microsoft	Olvídense de solicitar a los usuarios que cambien periódicamente la contraseña, deshabilite los requisitos de complejidad y a los usuarios les será más fácil recordar la contraseña y mantener una segura.
Creación de un plan para el acceso de usuarios invitados	Colabore con los usuarios invitados y permítales iniciar sesión en sus aplicaciones y servicios con sus propias identidades profesionales, educativas o sociales.

Instrucciones para los clientes del plan 2 de Azure AD Premium

La tabla siguiente tiene como objetivo resaltar las acciones clave de las siguientes suscripciones de licencia:

- Azure Active Directory Premium P2 (Azure AD P2)
- Enterprise Mobility + Security (EMS E5)
- Microsoft 365 (M365 E5, A5)

ACCIÓN RECOMENDADA	DETAIL
Habilitar la experiencia de registro combinada para Azure MFA y SSPR para simplificar la experiencia de registro del usuario	Permita que los usuarios se registren para una de las experiencias comunes: Azure Multi-Factor Authentication o el autoservicio de restablecimiento de contraseña.
Configurar MFA para su organización	Asegúrese de que las cuentas están protegidas frente a los riesgos de la autenticación multifactor.
Habilitar el autoservicio de restablecimiento de contraseña	Esta capacidad reduce las llamadas al departamento de soporte técnico y la pérdida de productividad cuando un usuario no puede iniciar sesión en su dispositivo o en una aplicación.
Implementar la escritura diferida de contraseñas (si usa identidades híbridas)	Permita la escritura diferida de los cambios de contraseña en la nube en un entorno de Windows Server Active Directory local.
Habilitar las directivas de Identity Protection para aplicar el registro de MFA	Administre la implementación de Azure Multi-Factor Authentication (MFA).
Habilitar las directivas de riesgo de inicio de sesión y de usuario de Identity Protection	Habilite las directivas de inicio de sesión y de usuario de Identity Protection. La directiva de inicio de sesión recomendada está dirigida a los inicios de sesión de riesgo medio y requiere de MFA. En el caso de las directivas de usuario, deben dirigirse a los usuarios de alto riesgo que necesitan la acción de cambio de contraseña.
Crear y habilitar directivas de acceso condicional	<p>MFA para que los administradores protejan las cuentas a las que se asignan derechos administrativos.</p> <p>Bloquear los protocolos de autenticación heredados debido al aumento de riesgo asociado a los protocolos de autenticación heredados.</p> <p>Exigir que MFA para Azure Management proteja los recursos con privilegios al requerir la autenticación multifactor para cualquier usuario que tenga acceso a recursos de Azure.</p>

ACCIÓN RECOMENDADA	DETAIL
Habilitar la sincronización de hash de contraseñas (si se usan identidades híbridas)	Proporcione redundancia para la autenticación y mejore la seguridad (incluido el bloqueo inteligente, el bloqueo de IP y la capacidad de detectar las credenciales filtradas).
Habilitar el bloqueo inteligente de ADFS (si procede)	Protege a los usuarios de los bloqueos de cuentas de extranet debido a actividades malintencionadas.
Habilitar el bloqueo inteligente de Azure Active Directory (si se usan identidades administradas)	El bloqueo inteligente ayuda a bloquear a los actores malintencionados que intentan adivinar las contraseñas de los usuarios o que usan métodos de fuerza bruta para obtenerlas.
Deshabilitar el consentimiento del usuario final a las aplicaciones	El flujo de trabajo de consentimiento del administrador proporciona a los administradores una manera segura de conceder acceso a las aplicaciones que requieren la aprobación del administrador, de modo que los usuarios finales no expongan los datos de la empresa. Microsoft recomienda deshabilitar las operaciones futuras de consentimiento del usuario para ayudar a reducir el área expuesta y a mitigar este riesgo.
Habilitar el acceso remoto a las aplicaciones heredadas locales con Application Proxy	Habilite Azure Active Directory Application Proxy e intégrala con aplicaciones heredadas para que los usuarios tengan acceso seguro a aplicaciones locales, iniciando sesión con su cuenta de Azure AD.
Habilitar el acceso híbrido seguro: Protección de aplicaciones heredadas con redes y controladores de entrega de aplicaciones existentes (si procede)	Publique y proteja sus aplicaciones de autenticación heredadas locales y en la nube conectándolas a Azure AD con su red o controlador de entrega de aplicaciones existentes.
Integrar aplicaciones SaaS compatibles de la galería con Azure AD y habilitar el inicio de sesión único	Azure AD incluye una galería que contiene miles de aplicaciones previamente integradas. Algunas de las aplicaciones que su organización usa probablemente estén en la galería y se pueda acceder a ellas desde Azure Portal. Proporcione acceso a las aplicaciones SaaS empresariales de forma remota y segura mediante una experiencia de usuario mejorada (SSO).
Automatizar el aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS (si procede)	Cree automáticamente roles e identidades de usuario en las aplicaciones en la nube (SaaS) a las que los usuarios necesitan acceder. Además de crear identidades de usuario, el aprovisionamiento automático incluye el mantenimiento y la eliminación de identidades de usuario a medida que el estado o los roles cambian, de modo que mejora la seguridad de su organización.
Habilitar el acceso condicional basado en dispositivos	Mejore la seguridad y las experiencias de usuario con el acceso condicional basado en dispositivos. Este paso garantiza que los usuarios solo pueden tener acceso desde dispositivos que cumplen los estándares de seguridad y cumplimiento. A estos dispositivos también se les conoce como dispositivos administrados. Los dispositivos administrados pueden ser conformes con Intune o dispositivos unidos a Azure AD híbrido.
Habilitar la protección con contraseña	Proteja a los usuarios del uso de contraseñas poco seguras y fáciles de adivinar.

ACCIÓN RECOMENDADA	DETAIL
Designación de más de un administrador global	Asigne al menos dos cuentas de administrador global permanentes solo en la nube para casos de emergencia. Estas cuentas no son para un uso diario y deben tener contraseña compleja y larga. Las cuentas de acceso de emergencia garantizan el acceso al servicio en situaciones de emergencia.
Uso de roles de administrador no global siempre que sea posible	Asigne a los administradores solo el acceso que necesitan a las áreas a las que necesitan acceso. No todos los administradores necesitan ser administradores globales.
Habilitación de la guía de contraseñas de Microsoft	Olvídense de solicitar a los usuarios que cambien periódicamente la contraseña, deshabilite los requisitos de complejidad y a los usuarios les será más fácil recordar la contraseña y mantener una segura.
Creación de un plan para el acceso de usuarios invitados	Colabore con los usuarios invitados y permítales iniciar sesión en sus aplicaciones y servicios con sus propias identidades profesionales, educativas o sociales.
Habilitar Privileged Identity Management	Permite administrar, controlar y supervisar el acceso a recursos importantes de la organización, lo que garantiza que los administradores tengan acceso solo cuando sea necesario y reciban aprobación.

Pasos siguientes

- Para obtener instrucciones detalladas sobre la implementación de las características individuales de Azure AD, revise los [planes de implementación del proyecto de Azure AD](#).
- Para obtener una lista de comprobación detallada de la implementación de Azure AD, consulte el artículo [Guía de implementación de la característica Azure Active Directory](#).

Evaluación continua de acceso

22/07/2020 • 12 minutes to read • [Edit Online](#)

Los servicios de Microsoft, como Azure Active Directory (Azure AD) y Office 365, usan estándares y protocolos abiertos para maximizar la interoperabilidad. Uno de los más importantes es Open ID Connect (OIDC). Cuando una aplicación cliente como Outlook se conecta a un servicio como Exchange Online, las solicitudes de API se autorizan mediante tokens de acceso de OAuth 2.0. De manera predeterminada, los tokens de acceso son válidos durante una hora. Cuando expiran, el cliente se redirige de nuevo a Azure AD para actualizarlos. Esto también proporciona la oportunidad de volver a evaluar las directivas de acceso de los usuarios, por lo que podríamos optar por no actualizar el token debido a una directiva de acceso condicional, o bien porque el usuario se ha deshabilitado en el directorio.

La expiración y actualización de los tokens es un mecanismo estándar del sector. Dicho esto, los clientes han manifestado dudas sobre el lapso de tiempo entre que cambian las condiciones de riesgo para el usuario (por ejemplo, moverse de la oficina corporativa a la cafetería local, o credenciales de usuario detectadas en el mercado negro) y se pueden aplicar directivas relacionadas con ese cambio. Aunque hemos experimentado con el enfoque directo de duraciones de tokens reducidas, hemos descubierto que pueden degradar las experiencias de usuario y la confiabilidad y no eliminan los riesgos.

La respuesta oportuna a las infracciones de las directivas o a los problemas de seguridad requiere realmente una "conversación" entre el emisor del token, como Azure AD, y el usuario de confianza, como Exchange Online. Esta conversación bidireccional nos proporciona dos funcionalidades importantes. El usuario de confianza puede advertir cuándo han cambiado las cosas, como un cliente que procede de una nueva ubicación, e indicárselo al emisor del token. También proporciona al emisor del token una manera de indicar al usuario de confianza que deje de respetar los tokens de un usuario determinado debido a que la cuenta esté en peligro, se haya deshabilitado u otros problemas. El mecanismo para esta conversación es la Evaluación continua de acceso (CAE).

Microsoft ha sido un participante pionero en la iniciativa del Protocolo de evaluación continua de acceso (CAEP), como parte del grupo de trabajo [Señales y eventos compartidos](#) en OpenID Foundation. Los proveedores de identidades y las entidades de confianza podrán aprovechar las señales y los eventos de seguridad definidos por el grupo de trabajo para volver a autorizar o finalizar el acceso. Es un trabajo fascinante y mejorará la seguridad en muchas plataformas y aplicaciones.

Dado que las ventajas de seguridad son tan buenas, vamos a lanzar una implementación inicial específica de Microsoft en paralelo a nuestro trabajo continuo dentro de los organismos de estándares. A medida que trabajamos para implementar estas capacidades de evaluación continua de acceso (CAE) en los servicios de Microsoft, hemos aprendido mucho y estamos compartiendo esta información con la comunidad de estándares. Esperamos que nuestra experiencia en la implementación pueda ayudar a afianzar un estándar del sector aún mejor y nos comprometemos a implementar ese estándar una vez ratificado, lo que permitirá que todos los servicios participantes se beneficien.

¿Cómo funciona CAE en los servicios de Microsoft?

Nos centramos en la implementación inicial de la evaluación continua de acceso para Exchange y Teams. Esperamos ampliar la compatibilidad con otros servicios de Microsoft en el futuro. Comenzaremos a habilitar la evaluación continua de acceso solo para los inquilinos sin directivas de acceso condicional. Usaremos nuestros aprendizajes en esta fase de CAE para informar del lanzamiento continuo de CAE.

Requisitos del servicio

La evaluación continua de acceso se implementa mediante la habilitación de servicios (proveedores de recursos)

para suscribirse a eventos críticos en Azure AD de modo que dichos eventos se puedan evaluar y aplicar casi en tiempo real. Los siguientes eventos se aplicarán en este lanzamiento inicial de CAE:

- La cuenta de usuario se ha eliminado o deshabilitado.
- La contraseña de un usuario ha cambiado o se ha restablecido.
- MFA está habilitado para el usuario.
- El administrador revoca explícitamente todos los tokens de actualización de un usuario.
- Azure AD Identity Protection ha detectado un riesgo de usuario elevado.

En el futuro esperamos agregar más eventos, como los cambios de estado de dispositivo y ubicación. **Aunque nuestro objetivo es que el cumplimiento sea instantáneo, en algunos casos se puede observar una latencia de hasta 15 minutos debido al tiempo de propagación de eventos.**

Desafío de notificaciones del lado cliente

Antes de la evaluación continua de acceso, los clientes siempre intentaban reproducir el token de acceso desde su memoria caché, siempre y cuando no haya expirado. Con CAE, presentamos un nuevo caso en el que un proveedor de recursos puede rechazar un token aunque no haya expirado. Para informar a los clientes de que omitan su memoria caché aunque los tokens almacenados en caché no hayan expirado, presentamos un mecanismo denominado **desafío de notificaciones**. CAE requiere una actualización de cliente para comprender el desafío de notificaciones. La versión más reciente de las siguientes aplicaciones es compatible con el desafío de notificaciones:

- Outlook para Windows
- Outlook para iOS
- Outlook para Android
- Outlook para Mac
- Teams para Windows
- Teams para iOS
- Teams para Android
- Teams para Mac

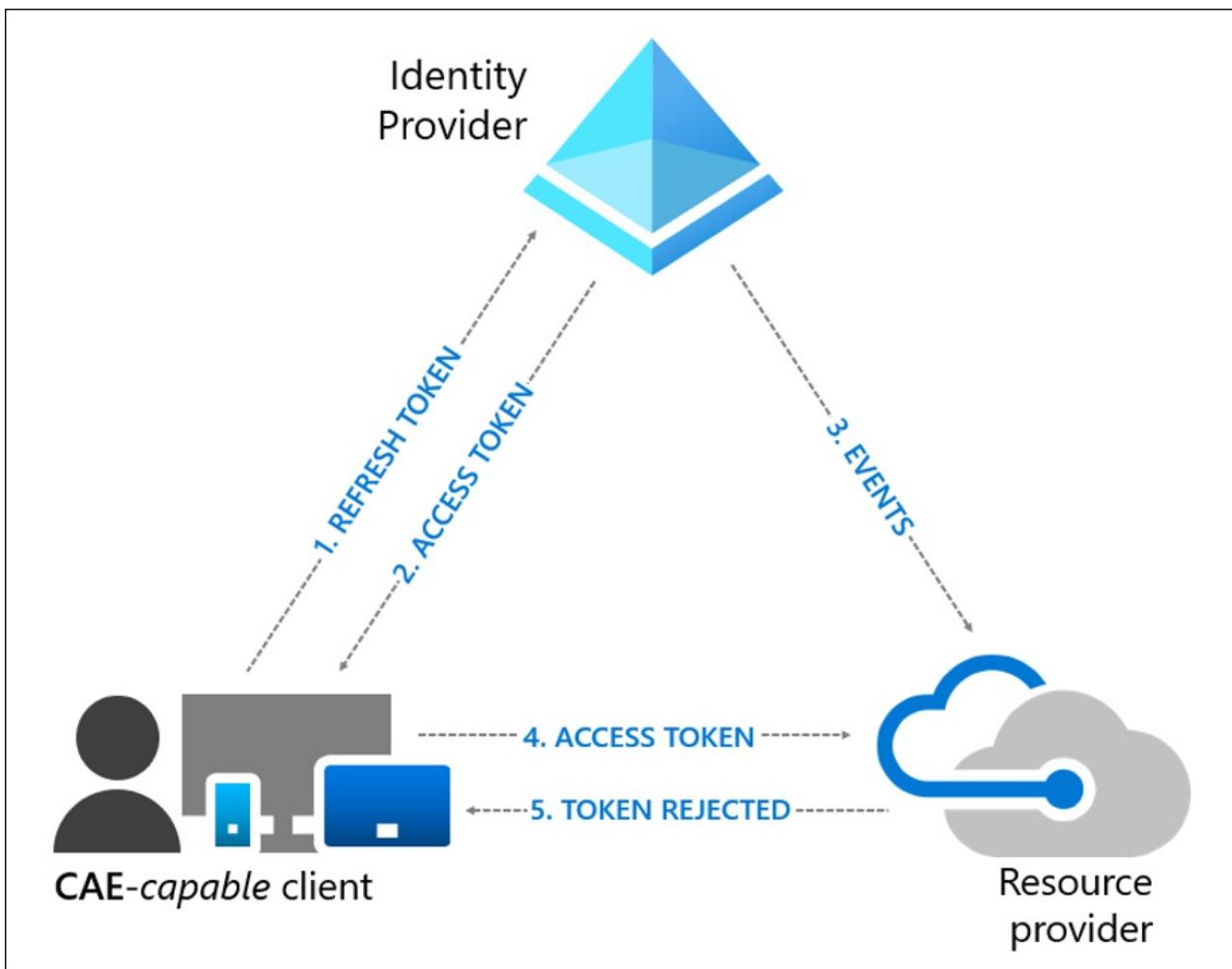
Vigencia del token

Dado que el riesgo y la directiva se evalúan en tiempo real, los clientes que negocien sesiones con reconocimiento de evaluación continua de acceso confiarán en CAE en lugar de en las directivas de vigencia del token de acceso estático existente, lo que significa que la directiva de vigencia del token configurable ya no se respetará en los clientes compatibles con CAE que negocien las sesiones con reconocimiento de CAE.

Aumentaremos la vigencia del token de acceso a 24 horas en las sesiones de CAE. La revocación se basa en eventos críticos y en la evaluación de directivas, no en un período de tiempo arbitrario. Este cambio aumenta la estabilidad de las aplicaciones sin afectar a su postura de seguridad.

Flujos de ejemplo

Flujo de eventos de revocación de usuario:



1. Un cliente compatible con CAE presenta credenciales o un token de actualización a AAD para solicitar un token de acceso para algún recurso.
2. Se devuelve un token de acceso junto con otros artefactos al cliente.
3. El administrador [revoca explícitamente todos los tokens de actualización de un usuario](#). Se enviará un evento de revocación al proveedor de recursos desde Azure AD.
4. Se presenta un token de acceso al proveedor de recursos. El proveedor de recursos evalúa la validez del token y comprueba si hay algún evento de revocación para el usuario. El proveedor de recursos utiliza esta información para decidir si se concede acceso al recurso.
5. En este caso, el proveedor de recursos deniega el acceso y envía un desafío de notificaciones 401+ al cliente.
6. El cliente compatible con CAE comprende el desafío de notificaciones 401+. Omite las cachés y vuelve al paso 1, enviando su token de actualización junto con el desafío de notificaciones de vuelta a Azure AD. A continuación, Azure AD volverá a evaluar todas las condiciones y solicitará al usuario que vuelva a autenticarse en este caso.

Preguntas más frecuentes

¿Cuál es la vigencia de mi token de acceso?

Si no usa clientes compatibles con CAE, la vigencia del token de acceso predeterminada seguirá siendo de una hora, a menos que haya configurado la vigencia del token de acceso con la característica en vista previa (GB) de [vigencia de token configurable \(CTL\)](#).

Si usa clientes compatibles con CAE que negocian sesiones con reconocimiento de CAE, se sobrescribirá la configuración de CTL de la vigencia del token de acceso, que será de 24 horas.

¿Qué rapidez tiene el cumplimiento?

Aunque nuestro objetivo es que el cumplimiento sea instantáneo, en algunos casos se puede observar una latencia de hasta 15 minutos debido al tiempo de propagación de eventos.

¿Cómo funcionará CAE con la frecuencia de inicio de sesión?

La frecuencia de inicio de sesión se respetará con o sin CAE.

Pasos siguientes

[Anuncio de evaluación continua de acceso](#)

Administración del acceso a recursos y aplicaciones con grupos en Azure Active Directory

22/07/2020 • 7 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) le permite usar grupos para administrar el acceso a las aplicaciones en la nube, las aplicaciones locales y los recursos. Sus recursos pueden formar parte de la organización de Azure AD, como los permisos para administrar objetos a través de los roles en Azure AD, o pueden estar fuera de la organización, como las aplicaciones SaaS (software como servicio), los servicios de Azure, los sitios de SharePoint y los recursos locales.

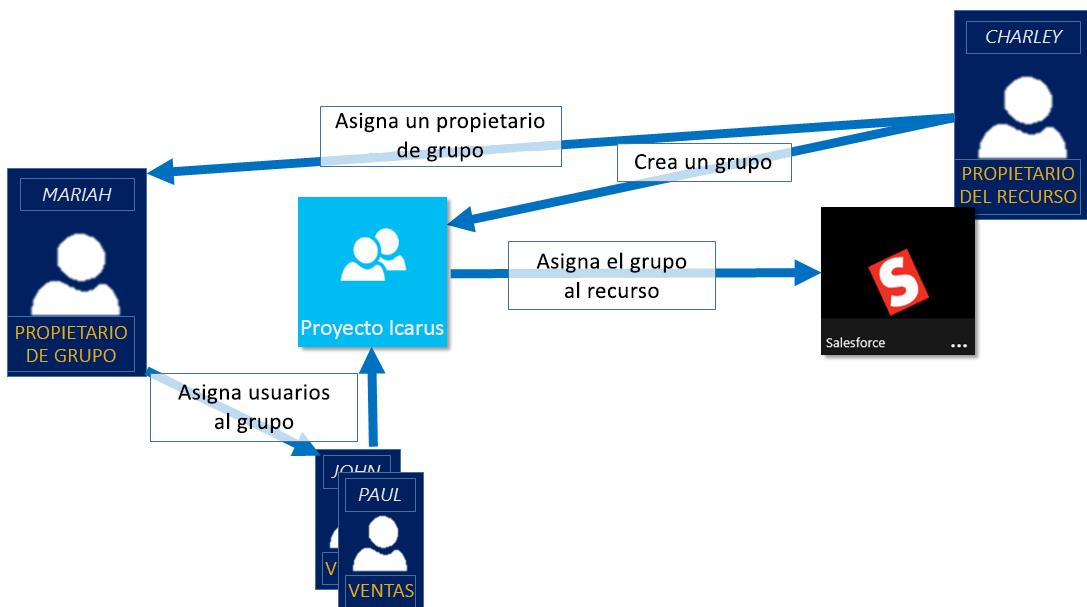
NOTE

En Azure Portal, puede ver algunos grupos cuyos miembros y detalles de grupo no se pueden administrar en el portal:

- Los grupos sincronizados desde Active Directory local solo se pueden administrar en Active Directory local.
- Otros tipos de grupos, como 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.

Funcionamiento de la administración de acceso en Azure AD

Azure AD le ayuda a proporcionar acceso a los recursos de su organización, ya que proporciona derechos de acceso a un usuario individual o a todo un grupo de Azure AD. El uso de grupos permite al propietario de los recursos (o al propietario del directorio de Azure AD) asignar un conjunto de permisos de acceso a todos los miembros del grupo, en lugar de tener que proporcionar los derechos uno por uno. El propietario del recurso o del directorio también puede conceder derechos de administrador para la lista de miembros a otra persona, como por ejemplo, a un director de departamento o a un administrador del departamento de soporte técnico, y dejar que dicha persona agregue y quite miembros, según sea necesario. Para más información acerca de cómo administrar propietarios de grupos, consulte [Administración de propietarios de grupos](#)



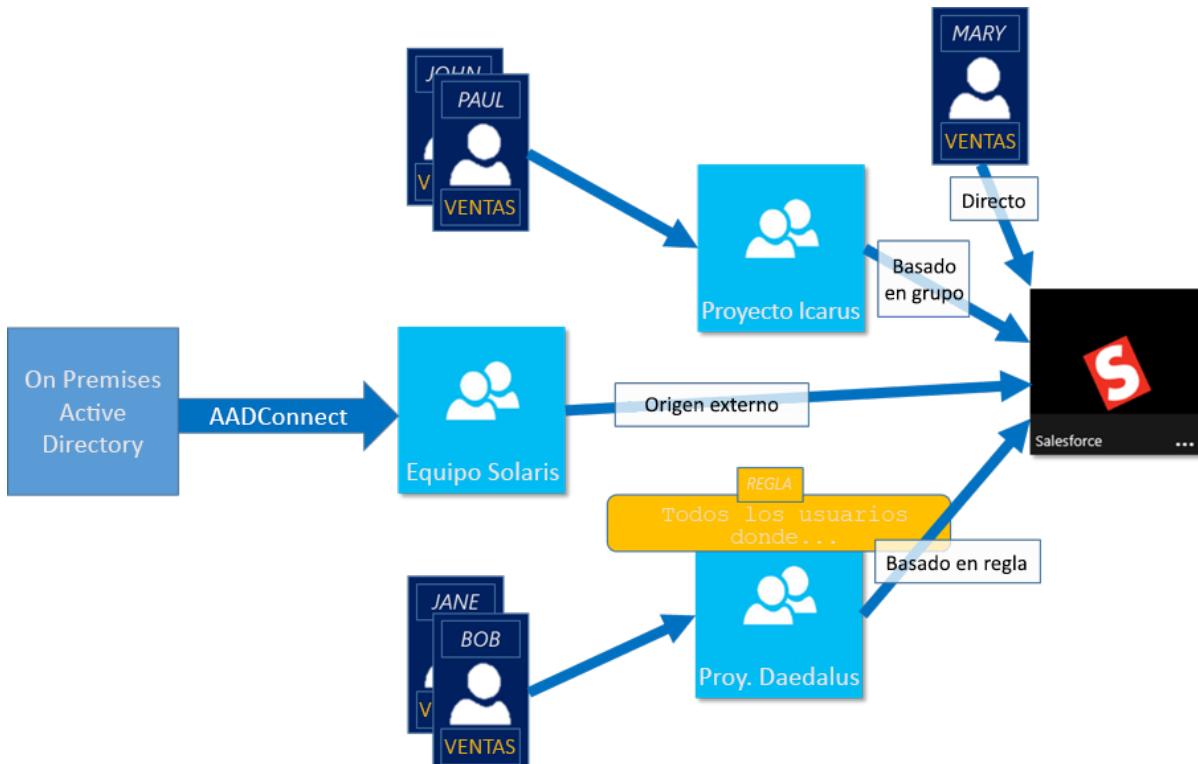
Formas de asignar derechos de acceso

Hay cuatro maneras de asignar derechos de acceso a los recursos a los usuarios:

- **Asignación directa.** El propietario del recurso asigna directamente el usuario al recurso.
- **Asignación de un grupo.** El propietario del recurso asigna un grupo de Azure AD al recurso, que automáticamente concede a todos sus miembros acceso al recurso. La pertenencia a un grupo la administran el propietario del grupo y el propietario del recurso, lo que permite a ambos propietarios agregar o quitar miembros del grupo. Para más información acerca de cómo agregar o eliminar miembros del grupo, consulte [Procedimiento para cómo agregar o quitar un grupo de otro grupo con Azure Active Directory](#).
- **Asignación basada en reglas.** El propietario del recurso crea un grupo y usa una regla para definir qué usuarios están asignados a un recurso concreto. La regla se basa en atributos que se asignan a usuarios individuales. El propietario del recurso administra la regla, lo que determina los atributos y valores que son necesarios para permitir el acceso al recurso. Para más información, consulte [Creación de un grupo dinámico y comprobación de su estado](#).

También puede ver este breve vídeo, donde encontrará para obtener una explicación rápida sobre cómo crear y usar grupos dinámicos:

- **Asignación de una autoridad externa.** El acceso procede de un origen externo, como un directorio local o una aplicación SaaS. En esta situación, el propietario del recurso asigna al grupo para proporcionar acceso al recurso y, después, el origen externo administra los miembros del grupo.



¿Pueden los usuarios unirse a grupos sin que se les asigne?

El propietario del grupo puede permitir a los usuarios buscar los grupos a los que se van a unir, en lugar de asignarlos. El propietario también puede configurar el grupo para que acepte todos los usuarios que se unan a él para que exija aprobación.

Cuando un usuario solicita unirse a un grupo, la solicitud se reenvía al propietario del mismo. Si es necesario, el

propietario puede aprobar la solicitud y se notifica al usuario de la pertenencia al grupo. Sin embargo, si tiene varios propietarios y uno de ellos la rechaza, el usuario recibe una notificación, pero no se agrega al grupo. Para más información e instrucciones acerca de cómo permitir a los usuarios solicitar su unión a grupos, consulte [Configuración de Azure AD para que los usuarios puedan solicitar unirse a grupos](#)

Pasos siguientes

Tras esta introducción a la administración de acceso mediante grupos, empiece a administrar los recursos y aplicaciones.

- [Creación de un grupo y adición de miembros en Azure Active Directory](#) o [Creación y administración de grupos mediante los cmdlets de PowerShell](#)
- [Uso de grupos para asignar acceso a una aplicación SaaS integrada](#)
- [Sincronización de un grupo local con Azure mediante Azure AD Connect](#)

¿En qué consisten las licencias basadas en grupos de Azure Active Directory?

22/07/2020 • 8 minutes to read • [Edit Online](#)

Los servicios en la nube de pago de Microsoft, como Office 365, Enterprise Mobility + Security, Dynamics 365 y otros productos similares, requieren licencias. Estas licencias se asignan a cada usuario que necesita acceso a estos servicios. Para administrar las licencias, los administradores usan uno de los portales de administración (ya sea Office o Azure) y los cmdlets de PowerShell. Azure Active Directory (Azure AD) es la infraestructura subyacente que admite la administración de identidades para todos los servicios en la nube de Microsoft. Azure AD almacena información sobre los estados de asignación de licencias para los usuarios.

Hasta ahora, las licencias solo podían asignarse a nivel de cada usuario, lo que puede dificultar la administración a gran escala. Por ejemplo, para agregar o quitar licencias de usuario en función de los cambios que se producen en la organización, por ejemplo, la incorporación o la baja de un usuario en la organización o en un departamento, un administrador a menudo debe escribir un script de PowerShell complejo. Este script hace llamadas individuales al servicio en la nube.

Para abordar esos desafíos, Azure AD incluye ahora las licencias basadas en grupo. Puede asignar una o varias licencias de producto a un grupo. Azure AD garantiza que las licencias se asignen a todos los miembros del grupo. A todos los miembros nuevos que se unan al grupo se les asignarán las licencias correspondientes. Cuando salen del grupo, se quitan esas licencias. La administración de licencias elimina la necesidad de automatizar la administración de licencias a través de PowerShell para reflejar los cambios que se producen en la organización y en la estructura de departamento por cada usuario.

Requisitos de concesión de licencia

Para usar licencias basadas en grupos, debe tener una de las siguientes licencias:

- Suscripción de pago o de prueba de Azure AD Premium P1 y versiones posteriores
- Edición de pago o de prueba de Office 365 Enterprise E3, Office 365 A3, Office 365 GCC G3, Office 365 E3 para GCCH u Office 365 E3 para DOD y superior

Número necesario de licencias

Para cualquier grupo al que se le asigne una licencia, también debe tener una licencia para cada miembro exclusivo. Si bien no tiene que asignar una licencia a cada miembro del grupo, debe tener al menos suficientes licencias para incluir a todos los miembros. Por ejemplo, si tiene 1000 miembros exclusivos que forman parte de grupos con licencia en su inquilino, debe tener al menos 1000 licencias para cumplir el contrato de licencia.

Características

A continuación se indican las características principales de las licencias basadas en grupos:

- Se pueden asignar licencias a todos los grupos de seguridad en Azure AD. Los grupos de seguridad se pueden sincronizar desde el entorno local mediante Azure AD Connect. También puede crear grupos de seguridad directamente en Azure AD (también denominados grupos solo de nube) o de forma automática, a través de la característica de grupo dinámico de Azure AD.
- Cuando se asigna una licencia de producto a un grupo, el administrador puede deshabilitar uno o varios planes de servicio del producto. Habitualmente, esta asignación se hace cuando la organización todavía no está preparada para comenzar a usar un servicio incluido en un producto. Por ejemplo, el administrador

podría asignar Office 365 a un departamento y deshabilitar temporalmente el servicio Yammer.

- Se admiten todos los Servicios en la nube de Microsoft que requieren licencias a nivel de usuario. Esta compatibilidad incluye todos los productos de Office 365, Enterprise Mobility + Security y Dynamics 365.
- Las licencias basadas en grupos actualmente solo están disponibles mediante [Azure Portal](#). Si usa principalmente otros portales de administración para la administración de usuarios y grupos, como [Centro de administración de Microsoft 365](#), puede seguir haciéndolo. Sin embargo, debe usar Azure Portal para administrar las licencias en el nivel de grupo.
- Azure AD administra automáticamente las modificaciones de licencia resultantes de los cambios de pertenencia a grupos. Habitualmente, las modificaciones de licencia entran en vigor minutos después de un cambio en la pertenencia.
- Un usuario puede ser miembro de varios grupos con directivas de licencia especificadas. Un usuario también puede tener algunas licencias que se asignaron directamente, fuera de cualquier grupo. El estado de usuario resultante es una combinación de todas las licencias de producto y servicio asignadas. Si se le asigna a un usuario la misma licencia desde varios orígenes, la licencia solo se usará una vez.
- En algunos casos, las licencias no se pueden asignar a un usuario. Por ejemplo, es posible que no haya licencias disponibles suficientes en el inquilino o puede que se hayan asignado servicios en conflicto al mismo tiempo. Los administradores tienen acceso a información sobre usuarios para los que Azure AD no pudo procesar íntegramente las licencias de grupo. Pueden realizar acciones correctivas según esa información.

Agradecemos sus comentarios.

Si tiene comentarios o solicitudes de características, compártalos con nosotros a través del [foro de administradores de Azure AD](#).

Pasos siguientes

Para más información sobre otros escenarios de administración de licencias basadas en grupos, consulte:

- [Asignación de licencias a un grupo en Azure Active Directory](#)
- [Identificación y resolución de problemas de licencias de un grupo en Azure Active Directory](#)
- [Migración de usuarios individuales con licencia a licencias basadas en grupos en Azure Active Directory](#)
- [Cómo migrar usuarios entre diferentes licencias de productos con licencias basadas en grupos de Azure Active Directory](#)
- [Azure Active Directory group-based licensing additional scenarios](#) (Escenarios adicionales de licencias basadas en grupos de Azure Active Directory)
- [Ejemplos de PowerShell para licencias basadas en grupos de Azure AD](#)

¿Cuáles son los permisos de usuario predeterminados en Azure Active Directory?

22/07/2020 • 18 minutes to read • [Edit Online](#)

En Azure Active Directory (Azure AD), a todos los usuarios se les otorga un conjunto de permisos predeterminados. El acceso de un usuario consta del tipo de usuario, sus [asignaciones de roles](#) y su propiedad de objetos individuales. En este artículo se describen dichos permisos predeterminados y contiene una comparación de los valores predeterminados de los usuarios miembros e invitados. Los permisos de usuario predeterminados solo se pueden cambiar en la configuración de usuario de Azure AD.

Usuarios miembros e invitados

El conjunto de permisos predeterminados recibido depende de si el usuario es miembro nativo del inquilino (usuario miembro) o si el usuario se incorpora desde otro directorio como un invitado de la colaboración B2B (usuario invitado). Vea [¿Qué es el acceso de usuarios invitados de B2B?](#) para más información sobre la adición de usuarios invitados.

- Los usuarios miembro pueden registrar aplicaciones, administrar el número de teléfono móvil y la fotografía de su propio perfil, cambiar su contraseña e invitar a los invitados de B2B. Además, los usuarios pueden leer toda la información del directorio (con algunas excepciones).
- Los usuarios invitados tienen permisos de directorio restringidos. Por ejemplo, los usuarios invitados no pueden buscar la información del inquilino más allá de su propia información de perfil. Sin embargo, un usuario invitado puede recuperar información acerca de otro usuario si proporciona el nombre principal de usuario u objectId. Un usuario invitado puede leer las propiedades de los grupos a los que pertenece, incluida la pertenencia a grupos, con independencia del valor **Guest users permissions are limited** (Los permisos de los usuarios invitados están limitados). Un invitado no puede ver información sobre cualquier otro objeto de inquilino.

De forma predeterminada, los permisos predeterminados de los invitados son restrictivos. Los invitados se pueden agregar a los roles de administrador, que les conceden permisos completos de lectura y escritura incluidos en el rol. Hay una restricción adicional disponible, la capacidad que tienen los invitados para invitar a otros. Si **Los invitados pueden invitar** se establece en **No** se evita que los invitados puedan invitar a otros. Consulte [Delegación de invitaciones de la colaboración B2B de Azure Active Directory](#) para aprender a hacerlo. Para conceder a los usuarios invitados los mismos permisos que a los usuarios miembros de forma predeterminada, establezca **Los permisos de los usuarios invitados están limitados** en **No**. Esta configuración concede a todos los miembros permisos de usuario para usuarios invitados de forma predeterminada y permite que se agreguen invitados a los roles administrativos.

Comparación de los permisos predeterminados de miembros e invitados

ÁMBITO

PERMISOS DE USUARIOS MIEMBROS

PERMISOS DE USUARIOS INVITADOS

ÁMBITO	PERMISOS DE USUARIOS MIEMBROS	PERMISOS DE USUARIOS INVITADOS
Usuarios y contactos	Leer todas las propiedades públicas de usuarios y contactos Invitar a los invitados Cambiar la contraseña propia Administrar el número de teléfono móvil propio Administrar la fotografía propia Invalidar tokens de actualización propios	Leer las propiedades propias Leer el nombre para mostrar, el correo electrónico, el nombre de inicio de sesión, la fotografía, el nombre principal de usuario y las propiedades de tipo de usuario de otros usuarios y contactos Cambiar la contraseña propia
Grupos	Crear grupos de seguridad Crear grupos de Office 365 Leer todas las propiedades de los grupos Leer las pertenencias a grupos no ocultos Leer las pertenencias a grupos de Office 365 ocultos para los grupos a los que se ha unido Administrar las propiedades, la propiedad y la pertenencia de los grupos propiedad del usuario Agregar invitados a los grupos que se poseen Administrar la configuración de pertenencia dinámica Eliminar los grupos que se poseen Restaurar los grupos de Office 365 que se poseen	Leer todas las propiedades de los grupos Leer las pertenencias a grupos no ocultos Leer las pertenencias a grupos de Office 365 ocultos para los grupos a los que se ha unido Administrar los grupos que se poseen Agregar invitados a los grupos que se poseen (si se permite) Eliminar los grupos que se poseen Restaurar los grupos de Office 365 que se poseen Leer las propiedades de los grupos a los que pertenecen, incluida la pertenencia.
APLICACIONES	Registrar aplicaciones nuevas Leer las propiedades de las aplicaciones registradas y empresariales Administrar las propiedades, asignaciones y credenciales de las aplicaciones que se poseen Crear o eliminar contraseña de la aplicación para el usuario Eliminar las aplicaciones que se poseen Restaurar las aplicaciones que se poseen	Leer las propiedades de las aplicaciones registradas y empresariales Administrar las propiedades, asignaciones y credenciales de las aplicaciones que se poseen Eliminar las aplicaciones que se poseen Restaurar las aplicaciones que se poseen
Dispositivos	Leer todas las propiedades de los dispositivos Administrar todas las propiedades de los dispositivos que se poseen	Sin permisos Eliminar los dispositivos que se poseen
Directorio	Leer toda la información de la compañía Leer todos los dominios Leer todos los contratos de los asociados	Leer el nombre para mostrar y los dominios comprobados
Roles y ámbitos	Leer todos los roles y las pertenencias administrativas Leer todas las propiedades y la pertenencia de las unidades administrativas	Sin permisos
Suscripciones	Leer todas las suscripciones Habilitar a miembro del plan de servicio	Sin permisos

ÁMBITO	PERMISOS DE USUARIOS MIEMBROS	PERMISOS DE USUARIOS INVITADOS
Directivas	Leer todas las propiedades de las directivas Administrar todas las propiedades de las directivas que se poseen	Sin permisos

Restricción de los permisos predeterminados de los usuarios miembros

Los permisos predeterminados de los usuarios miembros se pueden restringir de las siguientes maneras.

PERMISO	EXPLICACIÓN DEL VALOR
Los usuarios pueden registrar aplicaciones	Si se selecciona No en esta opción, se impide que los usuarios creen registros de aplicaciones. La capacidad puede ser devuelta a individuos específicos agregándolos al rol Desarrollador de aplicaciones.
Permitir a los usuarios conectar su cuenta profesional o educativa con LinkedIn	Si se selecciona No en esta opción, se impide que los usuarios conecten su cuenta profesional o educativa con su cuenta de LinkedIn. Para más información, consulte Consentimiento y uso compartido de datos de conexiones de cuentas de LinkedIn .
Capacidad para crear grupos de seguridad	Si se selecciona No en esta opción, se impide que los usuarios creen grupos de seguridad. Tanto los administradores globales como los administradores de tipo usuario pueden seguir creando grupos de seguridad. Para aprender a hacerlo, consulte Cmdlets de Azure Active Directory para configurar las opciones de grupo .
Capacidad para crear grupos de Office 365	Si se selecciona No en esta opción, se impide que los usuarios creen grupos de Office 365. Si se selecciona algunos en esta opción, se permite que un conjunto de usuarios creen grupos de Office 365. Tanto los administradores globales como los administradores de tipo usuario pueden seguir creando grupos de Office 365. Para aprender a hacerlo, consulte Cmdlets de Azure Active Directory para configurar las opciones de grupo .
Restringir el acceso al portal de administración de Azure AD	Si esta opción se establece en No, los usuarios que no son administradores pueden usar el portal de administración de Azure AD para leer y administrar recursos de Azure AD. Si se elige Sí, los usuarios que no son administradores no podrán acceder a ningún dato de Azure AD en el portal de administración. Importante: esta configuración no restringe el acceso a los datos de Azure AD usando PowerShell u otros clientes, como Visual Studio. Cuando se establece en Sí, para conceder a un usuario específico que no es administrador la capacidad de usar el portal de administración de Azure AD, asígnale cualquier rol administrativo, como el rol Lectores de directorio. Este rol permite leer información básica del directorio, que los usuarios miembros tienen de forma predeterminada (los invitados y las entidades de servicio, no).

PERMISO	EXPLICACIÓN DEL VALOR
Capacidad para leer otros usuarios	Esta configuración solo está disponible en PowerShell. Si establece esta marca en \$false, se impide que quienes no son administradores lean la información de los usuarios desde el directorio. Esta marca no impide que puedan leer la información de los usuarios en otros servicios de Microsoft, como Exchange Online. Esta configuración está pensada para circunstancias especiales y no se recomienda establecer esta marca en \$false.

Propiedad del objeto

Permisos de propietario del registro de una aplicación

Cuando un usuario registra una aplicación, se agrega automáticamente como propietario de la misma. Como propietario, puede administrar los metadatos de la aplicación, como el nombre y los permisos que solicita la aplicación. También pueden administrar la configuración específica del inquilino de la aplicación, como la configuración de SSO y las asignaciones de usuarios. Un propietario también puede agregar o quitar otros propietarios. A diferencia de los administradores globales, los propietarios solo pueden administrar las aplicaciones que poseen.

Permisos de propietario de las aplicaciones empresariales

Cuando un usuario agrega una aplicación empresarial, se agrega automáticamente como propietario. Como propietario, también puede administrar la configuración específica del inquilino de la aplicación, como la configuración de SSO, el aprovisionamiento y las asignaciones de usuarios. Un propietario también puede agregar o quitar otros propietarios. A diferencia de los administradores globales, los propietarios solo pueden administrar las aplicaciones que poseen.

Permisos de propietario de grupo

Cuando un usuario crea un grupo, se agrega automáticamente como propietario de dicho grupo. Como propietario, puede administrar las propiedades del grupo, como el nombre, así como administrar la pertenencia al grupo. Un propietario también puede agregar o quitar otros propietarios. A diferencia de los administradores globales y los administradores de tipo usuario, los propietarios solo pueden administrar los grupos que poseen. Para asignar un propietario de grupo, consulte [Administración de propietarios de un grupo](#).

Permisos de propiedad

En las tablas siguientes se describen los permisos específicos de Azure Active Directory que los usuarios miembro tienen sobre los objetivos que poseen. El usuario solamente tiene estos permisos en objetos que posee.

Registros de aplicación que se poseen

Los usuarios pueden realizar las siguientes acciones en los registros de aplicación que poseen.

ACCIONES	DESCRIPCIÓN
microsoft.directory/applications/audience/update	Actualiza la propiedad applications.audience en Azure Active Directory.
microsoft.directory/applications/authentication/update	Actualiza la propiedad applications.authentication en Azure Active Directory.
microsoft.directory/applications/basic/update	Actualiza las propiedades básicas de las aplicaciones en Azure Active Directory.

ACCIONES	DESCRIPCIÓN
microsoft.directory/applications/credentials/update	Actualiza la propiedad applications.credentials en Azure Active Directory.
microsoft.directory/applications/delete	Elimina aplicaciones en Azure Active Directory.
microsoft.directory/applications/owners/update	Actualiza la propiedad applications.owners en Azure Active Directory.
microsoft.directory/applications/permissions/update	Actualiza la propiedad applications.permissions en Azure Active Directory.
microsoft.directory/applications/policies/update	Actualiza la propiedad applications.policies en Azure Active Directory.
microsoft.directory/applications/restore	Restaura aplicaciones en Azure Active Directory.

Aplicaciones empresariales que se poseen

Los usuarios pueden realizar las siguientes acciones en las aplicaciones empresariales que poseen. Una aplicación empresarial se compone de la entidad de servicio, una o varias directivas de aplicación y, a veces, un objeto de aplicación en el mismo inquilino que la entidad de servicio.

ACCIONES	DESCRIPCIÓN
microsoft.directory/auditLogs/allProperties/read	Lee todas las propiedades (incluidas las propiedades con privilegios) en auditLogs en Azure Active Directory.
microsoft.directory/policies/basic/update	Actualiza las propiedades básicas en las directivas de Azure Active Directory.
microsoft.directory/policies/delete	Elimina directivas en Azure Active Directory.
microsoft.directory/policies/owners/update	Actualiza la propiedad policies.owners en Azure Active Directory.
microsoft.directory/servicePrincipals/appRoleAssignedTo/update	Actualiza la propiedad servicePrincipals.appRoleAssignedTo en Azure Active Directory.
microsoft.directory/servicePrincipals/appRoleAssignments/update	Actualiza la propiedad users.appRoleAssignments en Azure Active Directory.
microsoft.directory/servicePrincipals/audience/update	Actualiza la propiedad servicePrincipals.audience en Azure Active Directory.
microsoft.directory/servicePrincipals/authentication/update	Actualiza la propiedad servicePrincipals.authentication en Azure Active Directory.
microsoft.directory/servicePrincipals/basic/update	Actualiza las propiedades básicas de servicePrincipals en Azure Active Directory.
microsoft.directory/servicePrincipals/credentials/update	Actualiza la propiedad servicePrincipals.credentials en Azure Active Directory.
microsoft.directory/servicePrincipals/delete	Elimina servicePrincipals en Azure Active Directory.

ACCIONES	DESCRIPCIÓN
microsoft.directory/servicePrincipals/owners/update	Actualiza la propiedad servicePrincipals.owners en Azure Active Directory.
microsoft.directory/servicePrincipals/permissions/update	Actualiza la propiedad servicePrincipals.permissions en Azure Active Directory.
microsoft.directory/servicePrincipals/policies/update	Actualiza la propiedad servicePrincipals.policies en Azure Active Directory.
microsoft.directory/signInReports/allProperties/read	Lee todas las propiedades (incluidas las propiedades con privilegios) en signInReports en Azure Active Directory.

Dispositivos que se poseen

Los usuarios pueden realizar las siguientes acciones en los dispositivos que poseen.

ACCIONES	DESCRIPCIÓN
microsoft.directory/devices/bitLockerRecoveryKeys/read	Lee la propiedad devices.bitLockerRecoveryKeys en Azure Active Directory.
microsoft.directory/devices/disable	Deshabilita dispositivos en Azure Active Directory.

Grupos que se poseen

Los usuarios pueden realizar las siguientes acciones en los grupos que poseen.

ACCIONES	DESCRIPCIÓN
microsoft.directory/groups/appRoleAssignments/update	Actualiza la propiedad groups.appRoleAssignments en Azure Active Directory.
microsoft.directory/groups/basic/update	Actualiza las propiedades básicas de los grupos en Azure Active Directory.
microsoft.directory/groups/delete	Elimina grupos en Azure Active Directory.
microsoft.directory/groups/dynamicMembershipRule/update	Actualiza la propiedad groups.dynamicMembershipRule en Azure Active Directory.
microsoft.directory/groups/members/update	Actualiza la propiedad groups.members en Azure Active Directory.
microsoft.directory/groups/owners/update	Actualiza la propiedad groups.owners en Azure Active Directory.
microsoft.directory/groups/restore	Restaura grupos en Azure Active Directory.
microsoft.directory/groups/settings/update	Actualiza la propiedad groups.settings en Azure Active Directory.

Pasos siguientes

- Para obtener más información sobre cómo asignar roles de administrador de Azure AD, vea [Asignación de roles de administrador a un usuario en Azure Active Directory](#)

- Para más información acerca de cómo se controla el acceso a los recursos en Microsoft Azure, consulte [Descripción de acceso a los recursos de Azure](#)
- Para más información acerca de cómo se relaciona Azure Active Directory con la suscripción de Azure, consulte [Asociación de las suscripciones de Azure con Azure Active Directory](#)
- [Administrar usuarios](#)

¿Qué es la arquitectura de Azure Active Directory?

22/07/2020 • 15 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) le permite administrar el acceso a los servicios y recursos de Azure para los usuarios de forma segura. Con Azure AD se incluye un conjunto completo de funcionalidades de administración de identidades. Para más información sobre las características de Azure AD, consulte [¿Qué es Azure Active Directory?](#)

Con Azure AD, puede crear y administrar usuarios y grupos, y utilizar permisos para permitir o denegar el acceso a los recursos empresariales. Para más información sobre la administración de identidades, consulte [Aspectos básicos de la administración de identidades de Azure](#).

Arquitectura de Azure AD

La arquitectura distribuida geográficamente de Azure AD combina las funcionalidades de una amplia supervisión, el reenrutamiento automatizado, la conmutación por error y la recuperación, que ofrecen disponibilidad y rendimiento en toda la empresa a nuestros clientes.

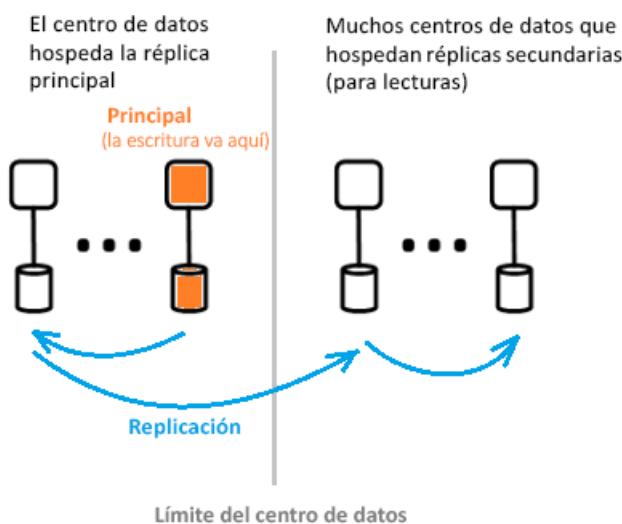
En este artículo se tratan los siguientes elementos de la arquitectura:

- Diseño de la arquitectura del servicio
- Escalabilidad
- Disponibilidad continua
- Centros de datos

Diseño de la arquitectura del servicio

La manera más común de compilar un sistema con datos enriquecidos que sea accesible y pueda usarse es con bloques de creación independientes o unidades de escalado. Para la capa de datos de Azure AD, a las unidades de escalado se les llama *particiones*.

El nivel de datos tiene varios servicios front-end que proporcionan la funcionalidad de lectura y escritura. En el diagrama siguiente se muestra cómo se entregan los componentes de una partición de directorio único a lo largo de centros de datos geográficamente distribuidos.



Los componentes de la arquitectura de Azure AD incluyen una réplica principal y réplicas secundarias.

Réplica principal

La *réplica principal* recibe todas las *operaciones de escritura* para la partición a la que pertenece. Esta operación de

escritura se replica inmediatamente en una réplica secundaria de otro centro de datos antes volver correctamente al que llama, lo que garantiza la durabilidad de las operaciones de escritura con redundancia geográfica.

Réplicas secundarias

Todas las *lecturas* de los directorios son atendidas desde las *réplicas secundarias*, que se encuentran en centros de datos ubicados físicamente en regiones geográficas diferentes. Existen muchas réplicas secundarias, ya que los datos se replican de forma asincrónica. Las lecturas de directorio, como las solicitudes de autenticación, se procesan en los centros de datos que están cerca de los clientes. Las réplicas secundarias son responsables de la escalabilidad de lectura.

Escalabilidad

La escalabilidad es la capacidad de un servicio de expandirse para satisfacer la creciente demanda de rendimiento. La escalabilidad de la operación de escritura se consigue mediante la creación de particiones de los datos. La escalabilidad de lectura se logra al replicar datos de una partición en varias réplicas secundarias que se distribuyen en todo el mundo.

Las solicitudes de las aplicaciones de directorio se enrutan al centro de datos que se encuentre físicamente más cerca. Las escrituras son redirigidas de forma transparente a la réplica principal para proporcionar coherencia de lectura y escritura. Las réplicas secundarias extienden significativamente la escala de las particiones porque los directorios suelen estar atendiendo a las lecturas la mayoría del tiempo.

Las aplicaciones de directorio se conectan a los centros de datos más cercanos. Esta conexión mejora el rendimiento y, por tanto, es posible el escalado horizontal. Como una partición de directorio puede tener varias réplicas secundarias, estas se pueden colocar más cerca a los clientes de directorio. Solo los componentes del servicio de directorio internos que requieren una gran cantidad de operaciones de escritura se dirigen directamente a la réplica principal activa.

Disponibilidad continua

La disponibilidad (o tiempo de actividad) define la capacidad de un sistema de ejecutarse sin interrupciones. La clave para la alta disponibilidad de Azure AD es que los servicios pueden cambiar rápidamente el tráfico entre varios centros de datos distribuidos geográficamente. Cada centro de datos es independiente, lo que permite anular la correlación de los modos con error. En este diseño de alta disponibilidad, Azure AD no requiere ningún tiempo de inactividad para las actividades de mantenimiento.

El diseño de la partición de Azure AD se ha simplificado en comparación con el diseño empresarial de AD, mediante un diseño maestro único que incluye un proceso de conmutación por error de la réplica principal determinista y cuidadosamente organizado.

Tolerancia a errores

Un sistema está más disponible si es tolerante a errores de hardware, de red y de software. Para cada partición en el directorio, existe una réplica de alta disponibilidad: la réplica principal. Solo se realizan en esta réplica las operaciones de escritura en la partición. Esta réplica se supervisa constante y estrechamente, y las operaciones de escritura pueden desplazarse inmediatamente a otra réplica (que se convierte en la nueva réplica principal) si se detecta un error. Durante la conmutación por error, podría haber una pérdida de disponibilidad de escritura de 1 a 2 minutos. La disponibilidad de lectura no se ve afectada durante este tiempo.

Las operaciones de lectura (que superan a las de escritura en muchos órdenes de magnitud) solo van a las réplicas secundarias. Como las réplicas secundarias son idempotentes, la pérdida de alguna réplica en una en una partición determinada se compensa fácilmente dirigiendo las lecturas a otra réplica, normalmente en el mismo centro de datos.

Durabilidad de los datos

Una operación de escritura está confirmada de forma duradera en al menos dos centros de datos antes de su reconocimiento. Esto ocurre al confirmar por primera vez la operación de escritura en el servidor principal y, después, replicar inmediatamente esta operación en al menos otro centro de datos. Esta acción de escritura garantiza que una potencial pérdida grave del centro de datos que hospeda la réplica principal no tenga como

resultado una pérdida de datos.

Azure AD mantiene un [tiempo objetivo de recuperación \(RTO\)](#) de cero para no perder datos en las conmutaciones por error. Esto incluye:

- Emisión de tokens y lecturas de directorio
- Permite únicamente un RTO de 5 minutos para la escritura en directorios

Centros de datos

Las réplicas de Azure AD se almacenan en centros de datos ubicados en todo el mundo. Para más información, consulte [Infraestructura global de Azure](#).

Azure AD funciona entre centros de datos con las siguientes características:

- Autenticación, Graph y otros servicios de AD residen detrás del servicio de puerta de enlace. La puerta de enlace administra el equilibrio de carga de estos servicios. Se conmutará por error automáticamente si se detecta algún servidor incorrecto mediante el sondeo de estado transaccional. En función de estos sondeos de estado, la puerta de enlace enruta dinámicamente el tráfico a centros de datos correctos.
- Para las operaciones de *lectura*, el directorio tiene réplicas secundarias y servicios front-end correspondientes en una configuración activa-activa que funciona en varios centros de datos. En caso de error en todo un centro de datos, el tráfico se redirigirá automáticamente a otro. Para las operaciones de *escritura*, el directorio continuará por error la réplica principal en los centros de datos mediante procedimientos de conmutación por error planeados (el nuevo elemento principal se sincroniza con el antiguo) o de emergencia. La durabilidad de los datos se logra al replicar cualquier confirmación en al menos dos centros de datos.

Coherencia de datos

El modelo de directorio es uno de coherencias finales. Uno de los problemas típicos con los sistemas de replicación distribuidos de forma asincrónica es que los datos devueltos de una réplica "determinada" pueden no estar actualizados.

Azure AD proporciona coherencia de lectura y escritura para las aplicaciones dirigidas a una réplica secundaria mediante el enrutamiento de sus operaciones de escritura a la réplica principal y la recuperación de forma sincrónica de las operaciones de escritura a la réplica secundaria.

Las operaciones de escritura de la aplicación que utilizan Microsoft Graph API de Azure AD se extraen de la afinidad de mantenimiento a una réplica de directorio para la coherencia de lectura y escritura. El servicio Microsoft Graph API mantiene una sesión lógica, que tiene afinidad con una réplica secundaria que se utiliza para las lecturas; la afinidad se captura en un "token de réplica" que el servicio almacena en caché mediante una memoria caché distribuida en el centro de datos de la réplica secundaria. Este token se usa entonces para las siguientes operaciones de la misma sesión lógica. Para seguir usando la misma sesión lógica, las solicitudes posteriores deben enrutarse al mismo centro de datos de Azure AD. No es posible continuar una sesión lógica si las solicitudes del cliente del directorio se enrutan a varios centros de datos de Azure Ad. Si esto ocurre, el cliente tiene varias sesiones lógicas con coherencias de lectura-escritura independientes.

NOTE

Las operaciones de escritura se replican inmediatamente a la réplica secundaria en la que se emitieron las operaciones de lectura de la sesión lógica.

Protección de copia de seguridad

El directorio implementa eliminaciones temporales, en lugar de eliminaciones permanentes, para usuarios e inquilinos para una recuperación fácil en el caso de eliminaciones accidentales realizadas por un cliente. Si el administrador de inquilinos elimina accidentalmente usuarios, pueden deshacer esta operación con facilidad y restaurar a los usuarios eliminados.

Azure AD implementa copias de seguridad diarias de todos los datos y, por tanto, puede restaurar de forma

autoritativa los datos en el caso de eliminaciones lógicas o daños. La capa de datos emplea códigos de corrección de errores, por lo que se puede comprobar si hay errores y corregir automáticamente determinados tipos de errores de disco.

Métricas y supervisiones

Ejecutar un servicio de alta disponibilidad requiere métricas y funcionalidades de supervisión de primer nivel. Azure AD analiza continuamente e informa de métricas de estado de servicio clave y de criterios de éxito para cada uno de sus servicios. Además, continuamente desarrollamos y optimizamos las métricas, las capacidades de supervisión y las alertas para cada escenario, dentro de cada servicio de Azure AD y en todos los servicios.

Si algún servicio de Azure AD no funciona según lo previsto, nos encargamos inmediatamente para restaurar la funcionalidad lo antes posible. La métrica más importante que sigue Azure AD es la rapidez con la que podemos detectar y mitigar los problemas en el sitio activo para los clientes. Estamos realizando grandes inversiones en la supervisión y alertas para minimizar el tiempo de detección (TTD objetivo:<5 minutos) y la preparación operativa para minimizar el tiempo de mitigación (TTM objetivo: <30 minutos).

Operaciones seguras

Mediante el uso de controles operativos, como Multi-Factor Authentication (MFA) para cualquier operación, así como la auditoría de todas las operaciones. Además, se usa un sistema de elevación just-in-time para conceder el acceso temporal necesario a cualquier tarea operativa a petición de forma continuada. Para más información, consulte [La nube de confianza](#).

Pasos siguientes

[Guía del desarrollador de Azure Active Directory](#)

Guía de implementación de la característica Azure Active Directory

22/07/2020 • 14 minutes to read • [Edit Online](#)

Puede parecer muy complicado implementar Azure Active Directory (Azure AD) para su organización y mantener la seguridad. En este artículo se identifican las tareas comunes que los clientes encuentran útiles para completar en fases, a lo largo de 30, 60, 90 días o más, para mejorar su posición de seguridad. Incluso las organizaciones que ya han implementado Azure AD pueden usar esta guía para asegurarse de que sacan el máximo partido de su inversión.

Una infraestructura de identidades bien planeada y ejecutada prepara el terreno para que únicamente los usuarios y los dispositivos conocidos puedan acceder de forma segura a los datos y a las cargas de trabajo de productividad.

Además, los clientes pueden consultar su [puntuación segura de identidad](#) para ver hasta qué punto siguen los procedimientos recomendados de Microsoft. Compruebe su puntuación segura antes y después de implementar estas recomendaciones para ver qué tal va en comparación con otros usuarios del sector y otras organizaciones de su tamaño.

Prerrequisitos

Muchas de las recomendaciones de esta guía se pueden implementar con Azure AD Free o sin licencia. Cuando se requiera licencia, indicaremos cuál es necesaria como mínimo para completar la tarea.

En las páginas siguientes encontrará información adicional sobre las licencias:

- [Licencias de Azure AD](#)
- [Microsoft 365 Enterprise](#)
- [Enterprise Mobility + Security](#)
- [Guía de concesión de licencias B2B de Azure AD](#)

Fase 1: Creación de una base de seguridad

En esta fase, los administradores habilitan unas características de seguridad como base de referencia para crear una base más segura y fácil de usar en Azure AD antes de importar o crear cuentas de usuario normales. Esta base fundamental garantiza un estado inicial seguro y que a los usuarios finales solo hay que presentarles los conceptos nuevos una vez.

TAREA	DETAL	LICENCIA NECESARIA
Designación de más de un administrador global	Asigne al menos dos cuentas de administrador global permanentes solo en la nube para casos de emergencia. Estas cuentas no son para un uso diario y deben tener contraseña compleja y larga.	Azure AD Free

TAREA	DETAL	LICENCIA NECESARIA
Uso de roles de administrador no global siempre que sea posible	Asigne a los administradores solo el acceso que necesitan a las áreas a las que necesitan acceso. No todos los administradores necesitan ser administradores globales.	Azure AD Free
Habilitación de Privileged Identity Management para el seguimiento del uso del rol de administrador	Habilite Privileged Identity Management para empezar el seguimiento del uso del rol de administrador.	Azure AD Premium P2
Implementación del autoservicio de restablecimiento de contraseña	Reduzca las llamadas al departamento de soporte técnico para el restablecimiento de contraseña al permitir a los empleados restablecerlas ellos mismos mediante directivas que controle usted como administrador.	
Creación de una lista de contraseñas prohibidas personalizada específica de la organización	Evite que los usuarios creen contraseñas que incluyan palabras o frases comunes de su organización o zona.	
Habilitación de la integración local con la protección de contraseñas de Azure AD	Amplíe la lista de contraseñas prohibidas al directorio local para garantizar que las contraseñas locales también cumplen los requisitos de las listas de contraseñas prohibidas globales y específicas del inquilino.	Azure AD Premium P1
Habilitación de la guía de contraseñas de Microsoft	Olvídese de solicitar a los usuarios que cambien periódicamente la contraseña, deshabilite los requisitos de complejidad y a los usuarios les será más fácil recordar la contraseña y mantener una segura.	Azure AD Free
Deshabilitación de los restablecimientos de contraseña periódicos para las cuentas de usuario en la nube	Los restablecimientos de contraseña periódicos promueven un aumento de las contraseñas existentes para los usuarios. Sírvase de la documentación de guía de las directrices de Microsoft sobre las contraseñas y copie la directiva local con los usuarios únicamente de la nube.	Azure AD Free
Personalización del bloqueo inteligente de Azure Active Directory	Deje de tener bloqueos de los usuarios de la nube al replicarlos a usuarios de Active Directory locales.	
Habilitación del bloqueo inteligente de la extranet para AD FS	El bloqueo de la extranet de AD FS protege contra los ataques de adivinación de contraseñas por fuerza bruta al tiempo que permite a los usuarios de AD FS válidos continuar usando sus cuentas.	

TAREA	DETAIL	LICENCIA NECESARIA
Implementación de Azure AD Multi-Factor Authentication mediante directivas de acceso condicional	Haga que los usuarios realicen la verificación en dos pasos al acceder a aplicaciones confidenciales mediante directivas de acceso condicional.	Azure AD Premium P1
Habilitación de Azure Active Directory Identity Protection	Habilite el seguimiento de los inicios de sesión de riesgo y de las credenciales en riesgo para los usuarios de su organización.	Azure AD Premium P2
Uso de detecciones de riesgos para desencadenar Multi-Factor Authentication y cambios de contraseñas	Habilite la automatización que desencadene eventos como la autenticación multifactor, el restablecimiento de contraseña y el bloqueo del inicio de sesión en caso de riesgo.	Azure AD Premium P2
Habilitación del registro convergente para autoservicio de restablecimiento de contraseña y Azure AD Multi-Factor Authentication (versión preliminar)	Permita que los usuarios se registren para una de las experiencias comunes: Azure Multi-Factor Authentication o el autoservicio de restablecimiento de contraseña.	Azure AD Premium P1

Fase 2: Importación de usuarios, habilitación de la sincronización y administración de dispositivos

A continuación agregaremos la base de la fase 1 mediante la importación de nuestros usuarios y la habilitación de la sincronización, la planeación del acceso de invitados y la preparación de la compatibilidad con otras funcionalidades.

TAREA	DETAIL	LICENCIA NECESARIA
Instalación de Azure AD Connect	Prepárese para sincronizar usuarios de su directorio local existente con la nube.	Azure AD Free
Implementación de la sincronización de hash de contraseñas	Sincronice los hash de contraseña para permitir que se repliquen los cambios de contraseña, la detección y la solución de problemas con la contraseña y los informes de revelación de credenciales.	Azure AD Free
Implementación de la escritura diferida de contraseñas	Permita la escritura diferida de los cambios de contraseña en la nube en un entorno de Windows Server Active Directory local.	Azure AD Premium P1
Implementación de Azure AD Connect Health	Habilite la supervisión de estadísticas de las claves de estado para los servidores de Azure AD Connect y de AD FS, y los controladores de dominio.	Azure AD Premium P1

TAREA	DETAL	LICENCIA NECESARIA
Asignación de licencias a usuarios según su pertenencia a un grupo en Azure Active Directory	Ahorre tiempo y esfuerzo mediante la creación de grupos de licencias que habiliten o deshabiliten características por grupo en lugar de la configuración por usuario.	
Creación de un plan para el acceso de usuarios invitados	Colabore con los usuarios invitados y permítales iniciar sesión en las aplicaciones y los servicios con sus propias identidades profesionales, educativas o sociales.	Guía de concesión de licencias B2B de Azure AD
Decisión acerca de la estrategia de administración de dispositivos	Decida lo que permite su organización con respecto a los dispositivos. Registro o unión, dispositivos propios o proporcionados por la empresa, etc.	
Implementación de Windows Hello para empresas en su organización	Prepárese para la autenticación sin contraseña con Windows Hello.	
Implementar métodos de autenticación sin contraseña para los usuarios	Proporcione a los usuarios métodos cómodos de autenticación sin contraseñas.	Azure AD Premium P1

Fase 3: Administración de aplicaciones

Siguiendo con la compilación de las fases anteriores, identificaremos aplicaciones candidatas para la migración y la integración con Azure AD y completaremos la configuración de esas aplicaciones.

TAREA	DETAL	LICENCIA NECESARIA
Identificación de las aplicaciones	Identifique las aplicaciones que se usan en la organización: locales, SaaS en la nube y otras de línea de negocio. Determinar si estas aplicaciones pueden y deben administrarse con Azure AD.	Sin necesidad de licencia
Integración de aplicaciones SaaS compatibles en la galería	Azure AD incluye una galería que contiene miles de aplicaciones previamente integradas. Algunas de las aplicaciones que su organización usa probablemente estén en la galería y se pueda acceder a ellas desde Azure Portal.	Azure AD Free
Uso de un proxy de aplicación para integrar las aplicaciones locales	Un proxy de aplicación permite a los usuarios acceder a aplicaciones locales mediante el sesión con su cuenta de Azure AD.	

Fase 4: Auditoría de las identidades con permisos, revisión del acceso y administración del ciclo de vida de los usuarios

En la fase 4 los administradores deben aplicar los últimos principios de los permisos de administración, completar sus primeras revisiones de acceso y permitir la automatización de las tareas comunes del ciclo de vida de los

usuarios.

TAREA	DETAIL	LICENCIA NECESARIA
Inicio del uso de Privileged Identity Management	Elimine los roles de administrador de las cuentas de usuario diarias normales. Haga que los usuarios administradores puedan usar su rol tras la comprobación de la autenticación multifactor para proporcionar una justificación de negocios o solicitar la autorización de los aprobadores designados.	Azure AD Premium P2
Completar una revisión de acceso para los roles de directorio de Azure AD en PIM	Trabaje con los equipos de seguridad y dirección para crear una directiva de revisión de acceso para revisar el acceso de los administradores de conformidad con las directivas de la organización.	Azure AD Premium P2
Implementación de directivas de pertenencia dinámica a grupos	Use grupos dinámicos para asignar automáticamente usuarios a grupos en función de sus atributos de RR. HH. (o su origen fiable), como el departamento, el puesto, la región y otros atributos.	
Implementación del aprovisionamiento de aplicaciones basado en grupos	Use el aprovisionamiento de administración del acceso basado en grupos para aprovisionar usuarios automáticamente para las aplicaciones SaaS.	
Automatización del aprovisionamiento y desaprovisionamiento de usuarios	Elimine los pasos manuales del ciclo de vida de la cuenta del empleado para evitar el acceso no autorizado. Sincronización de identidades desde un origen fiable (sistema de RR. HH.) en Azure AD.	

Pasos siguientes

[Detalles de precios y licencias de Azure AD](#)

[Configuraciones de acceso de dispositivos e identidades](#)

[Directivas comunes de acceso a dispositivos e identidades](#)

Planes de implementación de Azure Active Directory

22/07/2020 • 12 minutes to read • [Edit Online](#)

¿Busca una guía de un extremo a otro sobre cómo implementar las funcionalidades de Azure Active Directory (Azure AD)? Los planes de implementación de Azure AD le guían por el valor de negocio, las consideraciones de planeamiento y los procedimientos operativos necesarios para implementar correctamente las funcionalidades comunes de Azure AD.

Desde cualquiera de las páginas del plan, use la funcionalidad Imprimir en PDF del explorador para crear una versión sin conexión actualizada de la documentación.

Inclusión de la parte interesada correcta

Cuando comience a planear la implementación de una nueva funcionalidad, es importante incluir a las partes interesadas que son clave en la organización. Es recomendable identificar y documentar a la persona o personas que cumplen cada uno de los siguientes roles y trabajar con ellas para determinar su participación en el proyecto.

Entre los roles, se incluyen los siguientes:

ROLE	DESCRIPCIÓN
Usuario final	Un grupo representativo de usuarios para el que se implementará la funcionalidad. A menudo previsualiza los cambios en un programa piloto.
Administrador de soporte técnico de TI	Un representante de la organización de soporte técnico de TI que puede proporcionar información sobre la compatibilidad de este cambio desde una perspectiva del departamento de soporte técnico.
Arquitecto de identidades o administrador global de Azure	Un representante del equipo de administración de identidades responsable de definir cómo este cambio se alinea con la infraestructura de administración de identidades principal de su organización.
Propietario empresarial de la aplicación	El propietario empresarial global de las aplicaciones afectadas, que pueden incluir la administración del acceso. También puede proporcionar información sobre la experiencia del usuario y la utilidad de este cambio desde la perspectiva del usuario final.
Propietario de seguridad	Un representante del equipo de seguridad que puede aprobar que el plan cumplirá los requisitos de seguridad de la organización.
Administrador de cumplimiento	La persona de la organización responsable de garantizar el cumplimiento con requisitos corporativos, del sector o gubernamentales.

Los niveles de implicación podrían incluir:

- Responsable para implementar el plan del proyecto y el resultado
- Aprobación del plan del proyecto y el resultado

- Colaborador con el plan del proyecto y el resultado
- Informado del plan del proyecto y el resultado

Procedimientos recomendados para un piloto

Un piloto le permite probar con un grupo pequeño antes de activar una funcionalidad para todos. Asegúrese de que, como parte de sus pruebas, cada caso de uso de su organización se prueba de forma exhaustiva. Es mejor dirigirse a un grupo específico de usuarios piloto antes de implementar esto en su organización como un todo.

En su primera oleada, TI de destino, facilidad de uso y otros usuarios adecuados que pueden probar y proporcionar comentarios. Estos comentarios deben usarse para desarrollar aún más las comunicaciones e instrucciones que envía a sus usuarios y proporcionarles información sobre los tipos de problemas que puede ver su personal de soporte técnico.

La ampliación de la implementación en grupos de usuarios más grandes debe llevarse a cabo aumentando el ámbito de los grupos objetivo. Esto puede hacerse a través de la [pertenencia dinámica a grupos](#) o agregando usuarios manualmente a los grupos objetivo.

Implementación de la autenticación

CAPACIDAD	DESCRIPCIÓN
Multi-Factor Authentication	Azure Multi-Factor Authentication (MFA) es la solución de Microsoft de comprobación de dos pasos. El uso de métodos de autenticación aprobados por un administrador permite a Azure MFA ayudar a proteger el acceso a sus datos y aplicaciones, además de satisfacer la exigencia de un proceso de inicio de sesión simple.
Acceso condicional	Con Acceso condicional, puede implementar decisiones de control de acceso automatizado sobre quién puede acceder a las aplicaciones en nube, en función de condiciones.
Restablecimiento de la contraseña de autoservicio	El autoservicio de restablecimiento de contraseñas proporciona a los usuarios la capacidad de restablecer sus contraseñas, sin intervención de ningún administrador, en el momento y el lugar donde se precisa.
Inicio de sesión sin contraseña	Implementación de la autenticación sin contraseña mediante la aplicación Microsoft Authenticator o las claves de seguridad de FIDO2 de su organización

Implementación de la administración de aplicaciones y dispositivos

CAPACIDAD	DESCRIPCIÓN
Inicio de sesión único	El inicio de sesión único ayuda a los usuarios a acceder a las aplicaciones y los recursos que necesitan para hacer negocios, iniciando sesión una sola vez. Una vez iniciada la sesión, pueden ir de Microsoft Office a SalesForce, a Box y a aplicaciones internas sin necesidad de escribir credenciales una segunda vez.

CAPACIDAD	DESCRIPCIÓN
Panel de acceso	Proporcione a sus usuarios un lugar centralizado y sencillo desde el que puedan acceder a todas las aplicaciones. Favorezca la productividad con funcionalidades de autoservicio, como la solicitud de acceso a aplicaciones y grupos, o la administración del acceso a recursos en nombre de otros usuarios.
Dispositivos	Este artículo le ayuda a evaluar los métodos para integrar el dispositivo con Azure AD, elegir el plan de implementación y proporciona vínculos clave a las herramientas de administración de dispositivos compatibles.

Implementación de escenarios híbridos

CAPACIDAD	DESCRIPCIÓN
ADFS para sincronización de hash de contraseña	Con la sincronización de hash de contraseña, los valores de hash de las contraseñas de usuario se sincronizan desde Active Directory local a Azure AD, lo que permite a Azure AD autenticar a los usuarios sin interacción con Active Directory local.
Autenticación de ADFS para paso a través	La autenticación de paso a través de Azure AD ayuda a los usuarios a iniciar sesión en aplicaciones basadas en la nube y locales con las mismas contraseñas. Esta característica proporciona a los usuarios una mejor experiencia (una contraseña menos que recordar) y reduce los costos del departamento de soporte técnico de TI dado que es menos probable que olviden cómo iniciar sesión. Cuando los usuarios inician sesión con Azure AD, esta característica valida sus contraseñas directamente con la instancia de Active Directory local.
Azure AD Application Proxy	Hoy en día, los empleados desean ser productivos en cualquier lugar, en cualquier momento y con cualquier dispositivo. Tienen que acceder a aplicaciones SaaS en la nube y a aplicaciones corporativas locales. El proxy de aplicación de Azure AD permite este acceso sólido sin redes privadas virtuales (VPN) costosas y complejas ni zonas desmilitarizadas (DMZ).
SSO de conexión directa	El inicio de sesión único de conexión directa de Azure Active Directory (SSO de conexión directa de Azure AD) permite iniciar sesión automáticamente a los usuarios en dispositivos corporativos conectados a la red de la empresa. Con esta característica, los usuarios no tendrán que escribir la contraseña para iniciar sesión en Azure AD ni en general el nombre de usuario. Esta característica proporciona a los usuarios autorizados un acceso sencillo a las aplicaciones en la nube sin necesidad de componentes locales adicionales.

Implementación del aprovisionamiento de usuarios

CAPACIDAD	DESCRIPCIÓN
Aprovisionamiento de usuarios	Azure AD le ayuda a automatizar la creación, el mantenimiento y la eliminación de identidades de usuario en aplicaciones en la nube (SaaS) como Dropbox, Salesforce y muchas otras.
Aprovisionamiento de usuarios de RR. HH. en la nube	El aprovisionamiento de usuarios de RR. HH. en la nube para Active Directory establece las bases de una gobernanza continua de identidades y mejora la calidad de los procesos de negocio que se basan en datos de identidades fidedignos. Si usa esta característica con el producto de RR. HH. en la nube, como Workday o SuccessFactors, puede administrar fácilmente el ciclo de vida de las identidades de los empleados y los trabajadores temporales configurando reglas que asignen procesos de tipo alta, baja o traslado (como Nueva contratación, Fin de contrato y Traslado) a las acciones de aprovisionamiento de TI (como Crear, Habilitar y Deshabilitar).

Implementación de la gobernanza y los informes

CAPACIDAD	DESCRIPCIÓN
Privileged Identity Management	Azure AD Privileged Identity Management (PIM) le permite administrar roles con privilegios administrativos en Azure AD, los recursos de Azure y otros servicios de Microsoft Online Services. Asimismo, PIM ofrece soluciones como acceso de tipo Just-In-Time, flujos de trabajo de aprobación de solicitudes y revisiones de acceso completamente integradas para que pueda identificar, detectar y evitar en tiempo real las actividades malintencionadas de roles con privilegios.
Creación de informes y supervisión	El diseño de la solución de creación de informes y supervisión de Azure AD depende de sus requisitos legales, de seguridad y operativos, así como del entorno y los procesos existentes. En este artículo se presentan las distintas opciones de diseño y se le guía para que elija la estrategia de implementación adecuada.

Almacenamiento de datos de identidad para los clientes Europeos en Azure Active Directory

22/07/2020 • 5 minutes to read • [Edit Online](#)

Azure AD almacena los datos de identidad en una ubicación geográfica en función de la dirección que proporcione la organización al suscribirse a un servicio de Microsoft Online, como Office 365 y Azure. Para obtener información sobre dónde se almacenan los datos de identidad, puede consultar la sección [Where is your data located?](#) (Dónde se encuentran sus datos) de Microsoft Trust Center.

Para los clientes que proporcionaron una dirección en Europa, Azure AD conserva la mayoría de los datos de identidad en centros de datos europeos. En este documento se proporciona información sobre los datos que los servicios de Azure AD almacenan fuera de Europa.

Microsoft Azure Multi-Factor Authentication (MFA)

- La autenticación en dos fases que use llamadas telefónicas o mensajes de texto proceden de los centros de datos de EE. UU. y también se enruta mediante proveedores internacionales.
- Las notificaciones de inserción que usan la aplicación Microsoft Authenticator proceden de los centros de datos de EE. UU. Además, es posible que se usen servicios específicos del proveedor del dispositivo y estos servicios podrían encontrarse fuera de Europa.
- Los códigos OATH se validan siempre en EE. UU.

Para más información sobre qué información de usuario recopila el Servidor Microsoft Azure Multi-Factor Authentication (Servidor MFA) y Azure MFA basada en la nube, consulte [Recopilación de datos de usuario de Azure Multi-Factor Authentication](#).

Microsoft Azure Active Directory B2C (Azure AD B2C)

Los datos de configuración de directivas y contenedores de claves de Azure AD B2C se almacenan en los centros de datos de EE. UU. Estos no contienen datos personales de los usuarios. Para obtener más información sobre las configuraciones de directivas, consulte el artículo [Azure Active Directory B2C: directivas integradas](#).

Microsoft Azure Active Directory B2B (Azure AD B2B)

Azure AD B2B almacena las invitaciones con vínculos de canje y la información sobre la dirección URL de redirección en centros de datos de EE. UU. Además, la dirección de correo electrónico de los usuarios que cancelan la suscripción a invitaciones B2B también se almacena en centros de datos de EE. UU.

Microsoft Azure Active Directory Domain Services (Azure AD DS)

Azure AD DS almacena los datos de usuario en la misma ubicación que la instancia de Azure Virtual Network que seleccionó el cliente. Por lo tanto, si la red está fuera de Europa, los datos se replican y almacenan fuera de Europa.

Federación en Microsoft Exchange Server 2013

- Identificador de la aplicación (AppID): un número único que genera el sistema de autenticación de Azure Active Directory para identificar las organizaciones de Exchange.
- Lista de dominios federados aprobados para la aplicación
- Clave pública de firma de tokens de la aplicación

Para más información acerca de la federación en Microsoft Exchange Server, consulte el artículo [Federación: Ayuda de Exchange 2013](#).

Otras consideraciones

Los servicios y las aplicaciones que se integran en Azure AD tienen acceso a datos de identidad. Evalúe cada servicio y aplicación que use para determinar la manera en que cada servicio y aplicación específico procesa los datos de identidad, y si cumple los requisitos de almacenamiento de datos de la empresa.

Para obtener más información sobre la residencia de los datos de los servicios de Microsoft, consulte la sección [Where is your data located? \(Dónde se encuentran sus datos\)](#) de Microsoft Trust Center.

Pasos siguientes

Para más información sobre cualquiera de las características y funcionalidades que se han descrito anteriormente, consulte estos artículos:

- [¿Qué es Multi-Factor Authentication?](#)
- [Autoservicio de restablecimiento de contraseña de Azure AD](#)
- [¿Qué es Azure Active Directory B2C?](#)
- [¿Qué es la colaboración B2B de Azure AD?](#)
- [Azure Active Directory \(AD\) Domain Services](#)

Almacenamiento de datos de identidad para clientes australianos y neozelandeses en Azure Active Directory

22/07/2020 • 2 minutes to read • [Edit Online](#)

Azure AD almacena los datos de identidad en una ubicación geográfica en función de la dirección que proporcione la organización al suscribirse a un servicio de Microsoft Online, como Office 365 y Azure. Para más información sobre dónde se almacenan los datos de identidad del cliente, puede consultar la sección [Dónde se encuentran tus datos](#) del Centro de confianza de Microsoft.

NOTE

Los servicios y las aplicaciones que se integran en Azure AD tienen acceso a datos de identidad del cliente. Evalúe cada servicio y aplicación que use para determinar la manera en que cada servicio y aplicación específico procesa los datos de identidad del cliente, y si cumple los requisitos de almacenamiento de datos de la empresa. Para obtener más información sobre la residencia de los datos de los servicios de Microsoft, consulte la sección [Dónde se encuentran sus datos](#) del Centro de confianza de Microsoft.

En el caso de los clientes que han proporcionado direcciones de Australia y Nueva Zelanda y utilizan la edición gratuita de Azure AD, Azure AD mantiene la información de identificación personal en reposo en centros de datos australianos.

Todos los demás servicios de Azure AD premium almacenan los datos del cliente en centros de datos globales. Para localizar el centro de datos de un servicio, consulte [Azure Active Directory: Dónde se encuentran sus datos](#).

Microsoft Azure Multi-Factor Authentication (MFA)

El servicio MFA de Azure AD almacena datos de identidad del cliente en centros de datos globales en reposo. Para más información sobre los datos del usuario que Azure MFA basado en la nube recopila y almacena, consulte [Recopilación de datos de usuario de Azure Multi-Factor Authentication](#). Si los clientes usan MFA, sus datos se almacenarán fuera de los centros de datos en reposo de Australia.

Pasos siguientes

Para más información sobre cualquiera de las características y funcionalidades que se han descrito anteriormente, consulte estos artículos:

- [¿Qué es Multi-Factor Authentication?](#)

Guía de referencia de operaciones de Azure Active Directory

22/07/2020 • 3 minutes to read • [Edit Online](#)

Esta guía de referencia de operaciones describe las comprobaciones y las acciones que debe realizar para proteger y mantener las áreas siguientes:

- **La administración de identidades y accesos**: capacidad de administrar el ciclo de vida de las identidades y sus derechos.
- **Administración de autenticación**: capacidad de administrar las credenciales, definir la experiencia de autenticación, delegar la asignación, medir el uso y definir directivas de acceso basadas en la postura de seguridad de la empresa.
- **Gobernanza**: capacidad para evaluar y confirmar el acceso concedido a las identidades sin privilegios y con privilegios, así como auditar y controlar los cambios en el entorno.
- **Operaciones**: optimizar las operaciones de Azure Active Directory (Azure AD).

Algunas de estas recomendaciones podrían no aplicarse al entorno de todos los clientes; por ejemplo, podrían no aplicarse los procedimientos recomendados de AD FS si la organización usara la sincronización de hash de contraseñas.

NOTE

Estas recomendaciones están actualizadas hasta la fecha de publicación, pero pueden cambiar con el tiempo. Las organizaciones deben evaluar continuamente sus prácticas de identidad a medida que los productos y servicios de Microsoft evolucionen. Las recomendaciones pueden cambiar cuando las organizaciones se suscriben a una licencia de Azure AD Premium diferente. Por ejemplo, Azure AD Premium P2 incluirá más recomendaciones de gobernanza.

Partes interesadas

Cada sección de esta guía de referencia recomienda asignar las partes interesadas para planear e implementar correctamente las tareas clave. En la tabla siguiente se describe la lista de todas las partes interesadas de esta guía:

PARTES INTERESADAS	DESCRIPCIÓN
Equipo de operaciones IAM	Este equipo controla la administración de las operaciones diarias del sistema de Administración de identidades y acceso
Equipo de productividad	Este equipo posee y administra las aplicaciones de productividad como el correo electrónico, el uso compartido de archivos y la colaboración, la mensajería instantánea y las conferencias.
Application Owner	Este equipo es el propietario de la aplicación específica de una empresa y, normalmente, una perspectiva técnica de una organización.
Equipo de arquitectura de InfoSec	Este equipo planea y diseña las prácticas de seguridad de la información de una organización.

PARTES INTERESADAS	DESCRIPCIÓN
Equipo de operaciones de InfoSec	Este equipo ejecuta y supervisa los procedimientos de seguridad de la información implementados del equipo de arquitectura de InfoSec.

Pasos siguientes

Empiece con las [comprobaciones y las acciones de administración de la autenticación](#).

Guía de referencia de operaciones de administración de identidad y acceso de Azure Active Directory

22/07/2020 • 24 minutes to read • [Edit Online](#)

En esta sección de la [guía de referencia de operaciones de Azure AD](#) se describen las comprobaciones y las acciones que debe tener en cuenta para proteger y administrar el ciclo de vida de las identidades y sus asignaciones.

NOTE

Estas recomendaciones están actualizadas hasta la fecha de publicación, pero pueden cambiar con el tiempo. Las organizaciones deben evaluar continuamente sus prácticas de identidad a medida que los productos y servicios de Microsoft evolucionen.

Procesos operativos clave

Asignación de propietarios a las tareas clave

La administración de Azure Active Directory requiere la ejecución continua de tareas y procesos operativos clave que pueden no formar parte de un proyecto de implementación. Aun así, es importante que configure estas tareas con miras al mantenimiento de su entorno. Entre las tareas clave y sus propietarios recomendados se incluyen:

TAREA	PROPIETARIO
Definir el proceso de creación de suscripciones de Azure	Varía según la organización
Decidir quién obtiene licencias de Enterprise Mobility + Security	Equipo de operaciones IAM
Decidir quién obtiene licencias de Office 365	Equipo de productividad
Decidir quién obtiene otras licencias, por ejemplo, Dynamics, VSO	Application Owner
Asignación de licencias	Equipo de operaciones IAM
Solución de problemas y corrección de errores de asignación de licencias	Equipo de operaciones IAM
Aprovisionar identidades para aplicaciones en Azure AD	Equipo de operaciones IAM

A medida que revise la lista, es posible que tenga que asignar un propietario a las tareas que no tienen uno o ajustar la propiedad de aquellas tareas cuyos propietarios no se ajustan a las recomendaciones anteriores.

Lectura recomendada sobre la asignación de propietarios

- [Asignación de roles de administrador en Azure Active Directory](#)
- [Gobernanza en Azure](#)

Sincronización de identidades local

Identificación y solución de problemas de sincronización

Microsoft recomienda tener una buena línea de base y comprensión de los problemas de su entorno local que pueden derivar en problemas de sincronización en la nube. Dado que las herramientas automatizadas como [IdFix](#) y [Azure AD Connect Health](#) pueden generar un gran volumen de falsos positivos, se recomienda que identifique los errores de sincronización que se han dejado sin solucionar durante más de 100 días limpiando esos objetos con error. Los errores de sincronización sin resolver a largo plazo pueden generar incidentes de soporte técnico. En [Solución de errores durante la sincronización](#) se proporciona información general sobre los distintos tipos de errores de sincronización, algunos de los posibles escenarios que provocan dichos errores y las posibles maneras de corregirlos.

Configuración de la sincronización de Azure AD Connect

Para habilitar todas las experiencias híbridas, la postura de seguridad basada en dispositivos y la integración con Azure AD, es necesario sincronizar las cuentas de usuario que los empleados usan para iniciar sesión en sus equipos de escritorio.

Si no sincroniza los bosques en que los usuarios inician sesión, debe cambiar la sincronización para que provenga del bosque adecuado.

Ámbito de sincronización y filtrado de objetos

La supresión de cubos de objetos conocidos que no requieren sincronización tiene los siguientes beneficios operativos:

- Menos orígenes de errores de sincronización
- Ciclos de sincronización más rápidos
- Habrá menos elementos inútiles para transferir desde el entorno local; por ejemplo, la contaminación de la lista global de direcciones de las cuentas de servicios locales que no son pertinentes en la nube

NOTE

Si se da cuenta de que está importando muchos objetos que no se están exportando a la nube, debe filtrar por unidad organizativa o atributos específicos.

Algunos ejemplos de objetos que se deben excluir son:

- Cuentas de servicio que no se usan con aplicaciones en la nube.
- Grupos que no están diseñados para usarse en escenarios en la nube, como los que se usan para conceder acceso a los recursos.
- Usuarios o contactos que son identidades externas pensados para representarse con Colaboración B2B de Azure AD.
- Cuentas de equipo en las que no está previsto que los empleados accedan a aplicaciones en la nube desde, por ejemplo, servidores.

NOTE

Si una única identidad humana tiene varias cuentas aprovisionadas a partir de un suceso como una migración de dominio heredada, una fusión o una adquisición, solo debe sincronizar la cuenta utilizada por el usuario de forma cotidiana, por ejemplo, la que usa para iniciar sesión en su equipo.

Idealmente, querrá alcanzar un equilibrio entre la reducción del número de objetos que se van a sincronizar y la complejidad de las reglas. Por lo general, una combinación entre el [filtrado](#) de unidad organizativa/contenedor más una asignación de atributo simple para el atributo cloudFiltered resulta eficaz.

IMPORTANT

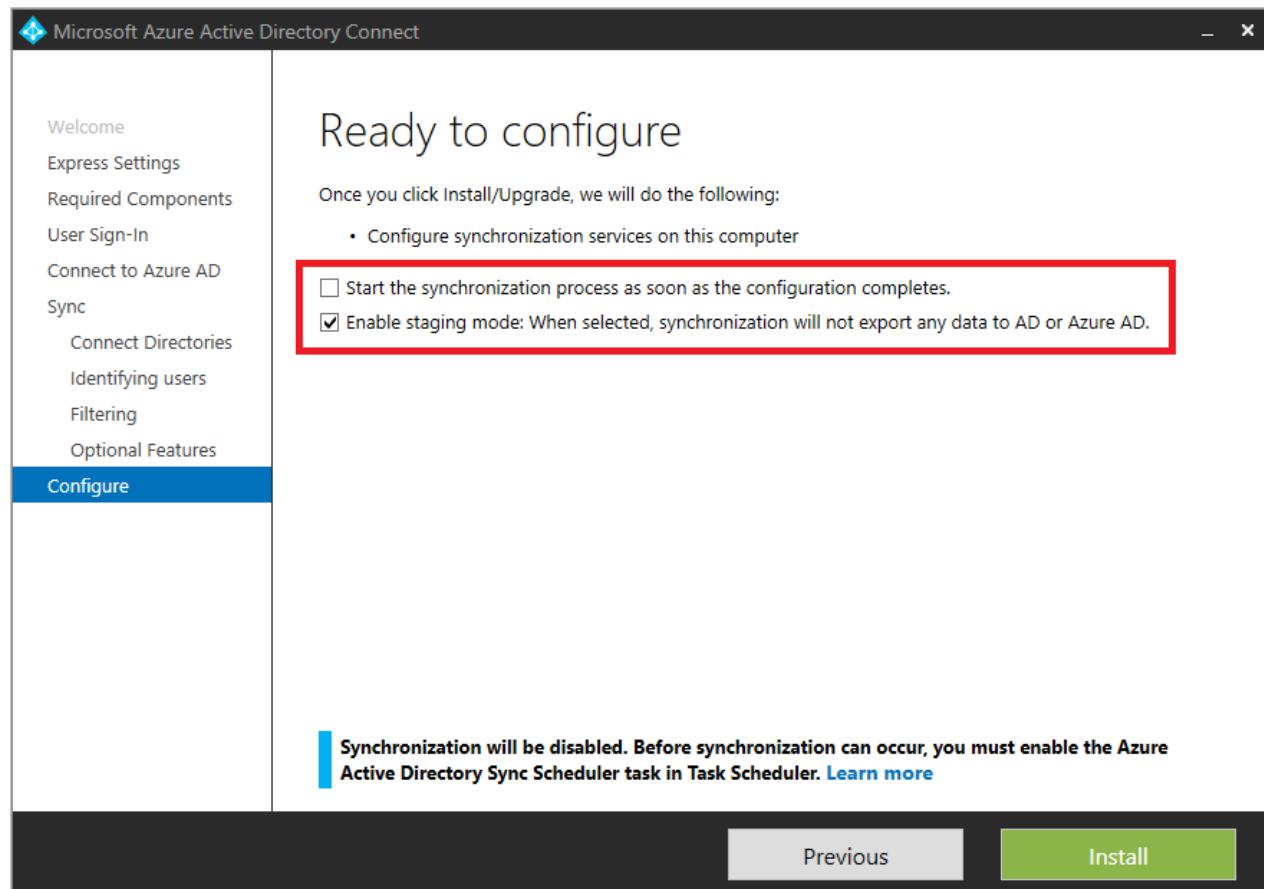
Si usa el filtrado de grupos en producción, debe contemplar la adopción de otro tipo de filtrado.

Conmutación por error o recuperación ante desastres para la sincronización

Azure AD Connect desempeña un papel clave en el proceso de aprovisionamiento. Si por algún motivo el servidor de sincronización se queda sin conexión, los cambios en el entorno local no se actualizan en la nube y se pueden producir problemas de acceso para los usuarios. Por lo tanto, es importante definir una estrategia de conmutación por error que permita a los administradores reanudar rápidamente la sincronización después de que el servidor de sincronización se queda sin conexión. Estas estrategias se dividen en una de las siguientes categorías:

- **Implementación de los servidores de Azure AD Connect en modo de ensayo:** permite al administrador "promover" el servidor de ensayo a producción mediante un sencillo cambio de configuración.
- **Uso de virtualización:** si la conexión de Azure AD se implementa en una máquina virtual (VM), los administradores pueden aprovechar su pila de virtualización para migrar en vivo o volver a implementar rápidamente la máquina virtual y, de este modo, reanudar la sincronización.

Si su organización no dispone de una estrategia de recuperación ante desastres y conmutación por error para la sincronización, no dude en implementar Azure AD Connect en modo de ensayo. Del mismo modo, si hay una discrepancia entre la configuración de producción y de ensayo, debe volver a configurar el modo de ensayo de la línea de base de Azure AD Connect para que coincida con la configuración de producción, incluidas las versiones y las configuraciones de software.



Mantenerse al día

Microsoft actualiza Azure AD Connect con regularidad. Manténgase al día para aprovechar las mejoras de rendimiento, las correcciones de errores y las nuevas capacidades que proporciona cada nueva versión.

Si la versión de Azure AD Connect tiene más de seis meses, debe actualizar a la versión más reciente.

Delimitador de origen

El uso de **ms-DS-consistencyguid** como **delimitador de origen** permite una migración más sencilla de objetos

entre bosques y dominios, tarea habitual en procesos de consolidación y limpieza, fusiones, adquisiciones y desinversiones en AD Domain.

Si actualmente está usando **ObjectGuid** como delimitador de origen, se recomienda empezar a utilizar **ms-DS-ConsistencyGuid**.

Reglas personalizadas

Las reglas personalizadas de Azure AD Connect proporcionan la capacidad de controlar el flujo de atributos entre los objetos locales y los objetos en la nube. Sin embargo, la sobreutilización o el uso indebido de reglas personalizadas pueden presentar los siguientes riesgos:

- Complejidad de la solución de problemas
- Degrado del rendimiento al realizar operaciones complejas en objetos
- Mayor probabilidad de divergencias de configuración entre el servidor de producción y el servidor de ensayo
- Sobrecarga adicional al actualizar Azure AD Connect si se crean reglas personalizadas en una precedencia mayor a 100 (usada por las reglas integradas)

Si usa reglas excesivamente complejas, debe investigar las causas de la complejidad y buscar oportunidades de simplificación. Del mismo modo, si ha creado reglas personalizadas con un valor de precedencia superior a 100, debe corregir las reglas para que no estén en riesgo ni entren en conflicto con el conjunto predeterminado.

Entre los ejemplos de reglas personalizadas de uso incorrecto se incluyen:

- **Compensar los datos sucios en el directorio:** en este caso, se recomienda trabajar con los propietarios del equipo de AD y limpiar los datos en el directorio como una tarea de corrección, así como ajustar los procesos para evitar la reintroducción de datos incorrectos.
- **Corrección única de usuarios individuales:** es habitual encontrar reglas que se correlacionan con los valores atípicos de casos especiales, normalmente debido a un problema con un usuario específico.
- **"CloudFiltering" excesivamente complicado:** aunque se recomienda reducir el número de objetos, existe el riesgo de crear y complicar en exceso el ámbito de sincronización mediante el uso de muchas reglas de sincronización. Si hay una lógica compleja para incluir o excluir objetos más allá del filtrado de la unidad organizativa, se recomienda tratar esta lógica fuera de la sincronización y etiquetar los objetos con un simple atributo "cloudFiltered" que pueda fluir con una regla de sincronización simple.

Documentador de configuración de Azure AD Connect

El [documentador de configuración de Azure AD Connect](#) es una herramienta que puede usar para generar documentación de una instalación de Azure AD Connect a fin de permitir una mejor comprensión de la configuración de sincronización, generar confianza para hacer las cosas bien y saber qué ha cambiado cuando aplicó una nueva compilación o configuración de Azure AD Connect o agregó o actualizó reglas de sincronización personalizadas. Las funcionalidades actuales de la herramienta incluyen:

- Documentación de la configuración completa de la sincronización de Azure AD Connect.
- Documentación de los cambios en la configuración de dos servidores de sincronización de Azure AD Connect o cambios de una línea de base de configuración determinada.
- Generación de un script de implementación de PowerShell para migrar las diferencias o personalizaciones de la regla de sincronización de un servidor a otro.

Asignación a aplicaciones y recursos

Concesión de licencias basada en grupo para servicios en la nube de Microsoft

Azure Active Directory simplifica la administración de licencias a través de la [concesión de licencias basada en grupos](#) para los servicios en la nube de Microsoft. De este modo, la administración de identidad y acceso proporciona la infraestructura de grupo y la administración delegada de esos grupos a los equipos adecuados en las organizaciones. Hay varias maneras de configurar la pertenencia a grupos en Azure AD, entre las que se incluyen:

- **Sincronización desde el entorno local:** los grupos pueden provenir de directorios locales, lo que podría ser una buena opción para las organizaciones que han establecido procesos de administración de grupos que se pueden ampliar para asignar licencias en Office 365.
- **Base en atributos/dinámica:** los grupos se pueden crear en la nube en función de una expresión basada en atributos de usuario, por ejemplo, Departamento igual a "ventas". Azure AD mantiene los miembros del grupo, manteniendo la coherencia con la expresión definida. El uso de este tipo de grupo para la asignación de licencias posibilita una asignación de licencias basada en atributos, que es una buena opción para las organizaciones que tienen una calidad de datos alta en su directorio.
- **Propiedad delegada:** los grupos se pueden crear en la nube y pueden ser propietarios designados. De este modo, puede permitir que los propietarios de empresas, por ejemplo, el equipo de colaboración o el equipo de BI, puedan definir quién debe tener acceso.

Si actualmente está usando un proceso manual para asignar licencias y componentes a los usuarios, se recomienda implementar las licencias basadas en grupos. Si el proceso actual no supervisa los errores de licencia o lo que está asignado frente a lo que está disponible, debe definir mejoras en el proceso para solucionar los errores relativos a las licencias y supervisar su asignación.

Otro aspecto de la administración de licencias es la definición de los planes de servicio (componentes de la licencia) que deben habilitarse en función de las funciones de trabajo de la organización. Otorgar acceso a planes de servicio que no son necesarios puede hacer que los usuarios vean herramientas en el portal de Office para las que no se han preparado o que no deberían utilizar. Puede generar un volumen adicional para el departamento de soporte técnico y un aprovisionamiento innecesario, además de poner en riesgo el cumplimiento y la gobernanza, por ejemplo, al aprovisionar OneDrive para la Empresa para individuos que podrían no tener permiso para compartir contenido.

Utilice las siguientes directrices para definir planes de servicio para los usuarios:

- Los administradores deben definir "agrupaciones" de los planes de servicio que se van a ofrecer a los usuarios en función de su rol, por ejemplo, trabajador de cuello blanco o de cuello azul.
- Cree grupos de este modo y asigne la licencia con el plan de servicio.
- Opcionalmente, se puede definir un atributo que contenga los paquetes para los usuarios.

IMPORTANT

Las concesión de licencias basada en grupos de Azure AD incorpora el concepto de usuarios en estado de error de licencias. En caso de que se produzcan errores relativos a las licencias, debe [detectar y resolver](#) de inmediato cualquier problema de asignación de licencias.

PRODUCTS	STATE	ENABLED SERVICES
Office 365 Enterprise E1	Active	11/12

Si actualmente usa una herramienta, como [Microsoft Identity Manager](#) o un sistema de terceros, que se base en una infraestructura local, se recomienda descargar la asignación de la herramienta existente, implementar licencias basadas en grupos y definir una administración del ciclo de vida de los grupos basada en [grupos](#). Del mismo modo, si el proceso existente no tiene en cuenta los nuevos empleados o los empleados que abandonan la organización, debe implementar licencias basadas en grupos dinámicos y definir un ciclo de vida de pertenencia a grupos. Por último, si implementa la concesión de licencias basada en grupo sobre grupos locales que carecen de administración del ciclo de vida, considere la posibilidad de usar grupos en la nube para habilitar funcionalidades como la propiedad delegada o la pertenencia dinámica basada en atributos.

Asignación de aplicaciones con el grupo "Todos los usuarios"

Los propietarios de recursos pueden creer que el grupo **Todos los usuarios** solo contiene **Empleados de la empresa**, cuando puede que realmente contengan tanto **Empleados de la empresa** como **Invitados**. Como resultado, debe tener especial cuidado al usar el grupo **Todos los usuarios** para la asignación de aplicaciones y conceder acceso a recursos como aplicaciones o contenido de SharePoint.

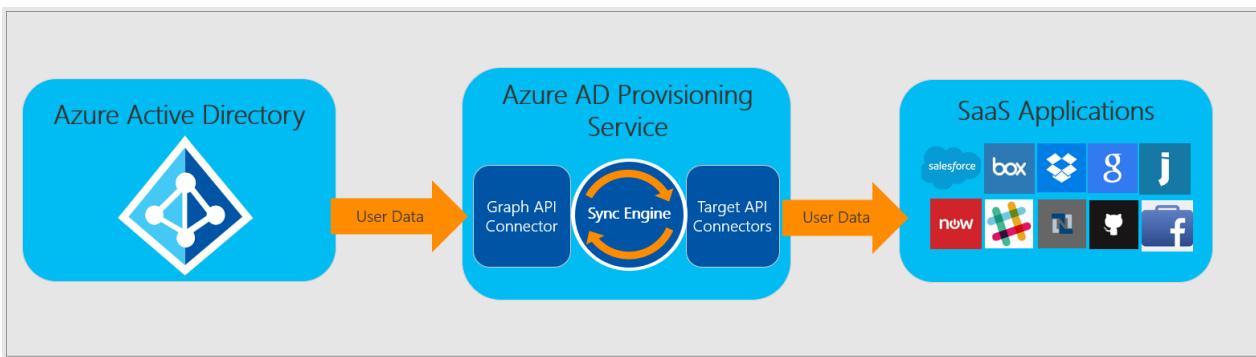
IMPORTANT

Si el grupo **Todos los usuarios** está habilitado y se usa para las directivas de acceso condicional o la asignación de recursos o aplicaciones, asegúrese de [proteger el grupo](#) si no desea que incluya a los usuarios invitados. Además, debe corregir las asignaciones de licencias creando y asignando grupos que contengan solo a los **Empleados de la empresa**. Por otro lado, si observa que el grupo **Todos los usuarios** está habilitado pero no se usa para conceder acceso a los recursos, asegúrese de que la directriz operativa de su organización sea usar intencionadamente ese grupo (que incluye tanto a los **empleados de la empresa** como a los **invitados**).

Aprovisionamiento de usuarios automático a aplicaciones

El [aprovisionamiento de usuarios automático](#) para aplicaciones es la mejor manera de crear un aprovisionamiento, desaprovisionamiento y ciclo de vida de identidades coherente entre varios sistemas.

Si actualmente está aprovisionando aplicaciones ad hoc o usa elementos como archivos CSV, JIT o una solución local que no se encargue de administrar el ciclo de vida, le recomendamos que [implemente el aprovisionamiento de aplicaciones](#) con Azure AD con las aplicaciones compatibles y que defina un patrón coherente para las aplicaciones que aún no son compatibles con Azure AD.



Línea de base del ciclo de sincronización diferencial de Azure AD Connect

Es importante comprender el volumen de cambios de la organización y no tardar demasiado en tener un tiempo de sincronización predecible.

La frecuencia de [sincronización diferencial predeterminada](#) es de 30 minutos. Si la sincronización diferencial tarda más de 30 minutos de manera recurrente, o hay discrepancias significativas entre el rendimiento de la sincronización diferencial de ensayo y producción, debe investigar y revisar los [factores que influyen en el rendimiento de Azure AD Connect](#).

Lectura recomendada para la solución de problemas de Azure AD Connect

- Preparación de los atributos del directorio para sincronizarlos con Office 365 mediante la herramienta IdFix:

- [Azure AD Connect: Solución de errores durante la sincronización](#)

Resumen

Una infraestructura de identidad segura está conformada por cinco aspectos. Esta lista le ayudará a encontrar y adoptar rápidamente las acciones necesarias para proteger y administrar el ciclo de vida de las identidades y sus derechos en su organización.

- Asignar propietarios a las tareas principales.
- Buscar y resolver problemas de sincronización.
- Definir una estrategia de conmutación por error para la recuperación ante desastres.
- Optimizar la administración de licencias y la asignación de aplicaciones.
- Automatizar el aprovisionamiento de usuarios a las aplicaciones.

Pasos siguientes

Empiece con las [comprobaciones y las acciones de administración de la autenticación](#).

Guía de referencia de operaciones de administración de autenticación de Azure Active Directory

22/07/2020 • 45 minutes to read • [Edit Online](#)

En esta sección de la [guía de referencia de operaciones de Azure AD](#) se describen las comprobaciones y las acciones que debe realizar para proteger y administrar las credenciales, definir la experiencia de autenticación, delegar la asignación, medir el uso y definir directivas de acceso basadas en la posición de seguridad de la empresa.

NOTE

Estas recomendaciones están actualizadas hasta la fecha de publicación, pero pueden cambiar con el tiempo. Las organizaciones deben evaluar continuamente sus prácticas de identidad a medida que los productos y servicios de Microsoft evolucionen.

Procesos operativos clave

Asignación de propietarios a las tareas clave

La administración de Azure Active Directory requiere la ejecución continua de tareas y procesos operativos clave que pueden no formar parte de un proyecto de lanzamiento. Aun así, es importante que configure estas tareas con miras a optimizar su entorno. Entre las tareas clave y sus propietarios recomendados se incluyen:

TAREA	PROPIETARIO
Administrar el ciclo de vida de la configuración de inicio de sesión único (SSO) en Azure AD	Equipo de operaciones IAM
Diseñar directivas de acceso condicional para aplicaciones de Azure AD	Equipo de arquitectura de InfoSec
Archivar la actividad de inicio de sesión en un sistema SIEM	Equipo de operaciones de InfoSec
Archivar eventos de riesgo en un sistema SIEM	Equipo de operaciones de InfoSec
Evaluar las propiedades e investigar las alertas de seguridad	Equipo de operaciones de InfoSec
Evaluar las propiedades e investigar los eventos de seguridad	Equipo de operaciones de InfoSec
Evaluar las propiedades e investigar los usuarios marcados en informes de vulnerabilidades y riesgos desde Azure AD Identity Protection	Equipo de operaciones de InfoSec

NOTE

Azure AD Identity Protection requiere una licencia de Azure AD Premium P2. Para obtener la licencia correcta para sus requisitos, consulte [Comparación de las características con disponibilidad general de las ediciones Azure AD Free y Azure AD Premium](#).

A medida que revise la lista, es posible que tenga que asignar un propietario a las tareas que no tienen uno o ajustar la propiedad de aquellas tareas cuyos propietarios no se ajustan a las recomendaciones anteriores.

Lecturas recomendadas para propietarios

- [Asignación de roles de administrador en Azure Active Directory](#)
- [Gobernanza en Azure](#)

Administración de credenciales

Directivas de contraseña

Administrar contraseñas de forma segura es una de las partes más destacadas de la administración de identidades y acceso y, a menudo, el objetivo más importante de los ataques. Azure AD admite varias características que pueden ayudarle a evitar que un ataque tenga éxito.

Use la tabla siguiente para encontrar la solución recomendada para mitigar el problema que debe abordarse:

PROBLEMA	RECOMENDACIÓN
No hay ningún mecanismo que le proteja contra contraseñas poco seguras	Habilite el autoservicio de restablecimiento de contraseña (SSPR) y la protección con contraseña de Azure AD.
No hay ningún mecanismo para detectar contraseñas filtradas	Habilite la sincronización de hash de contraseñas (PHS) para obtener más detalles.
Se está usando AD FS y no es posible ir a la autenticación administrada	Habilite el bloqueo inteligente de la extranet de AD FS o el bloqueo inteligente de Azure AD .
La directiva de contraseñas usa reglas basadas en la complejidad, como la longitud, los conjuntos de varios caracteres o la caducidad	Reconsidere usar los procedimientos recomendados de Microsoft , cambie su enfoque a la administración de contraseñas e implemente la protección con contraseñas de Azure AD .
Los usuarios no están registrados para usar la autenticación multifactor (MFA)	Registre toda la información de seguridad del usuario de modo que se pueda usar como mecanismo para comprobar la identidad del usuario junto con su contraseña.
No hay ninguna revocación de contraseñas en función del riesgo del usuario	Implemente directivas de riesgo de usuario de Azure AD Identity Protection para forzar cambios de contraseña en credenciales perdidas mediante SSPR.
No hay ningún mecanismo de bloqueo inteligente para proteger la autenticación malintencionada de actores no válidos procedentes de direcciones IP identificadas	Implemente la autenticación administrada mediante la nube con la sincronización de hash de contraseñas o mediante la autenticación de paso a través (PTA) .

Lectura recomendada de directivas de contraseñas

- [Procedimientos recomendados de Azure AD y AD FS: defensa contra ataques de difusión de contraseña: Enterprise Mobility + Security](#)

Habilitar el autoservicio de restablecimiento de contraseña y la protección con contraseña

Los usuarios que necesitan cambiar o restablecer sus contraseñas son uno de los principales orígenes de volumen y costo debido a las llamadas que realizan al departamento de soporte técnico. Además del costo, cambiar la contraseña como una herramienta para mitigar el riesgo de un usuario es un paso fundamental para mejorar la posición de seguridad de su organización.

Como mínimo, se recomienda implementar el [autoservicio de restablecimiento de contraseña \(SSPR\)](#) de Azure AD y la [protección de contraseñas](#) local para realizar lo siguiente:

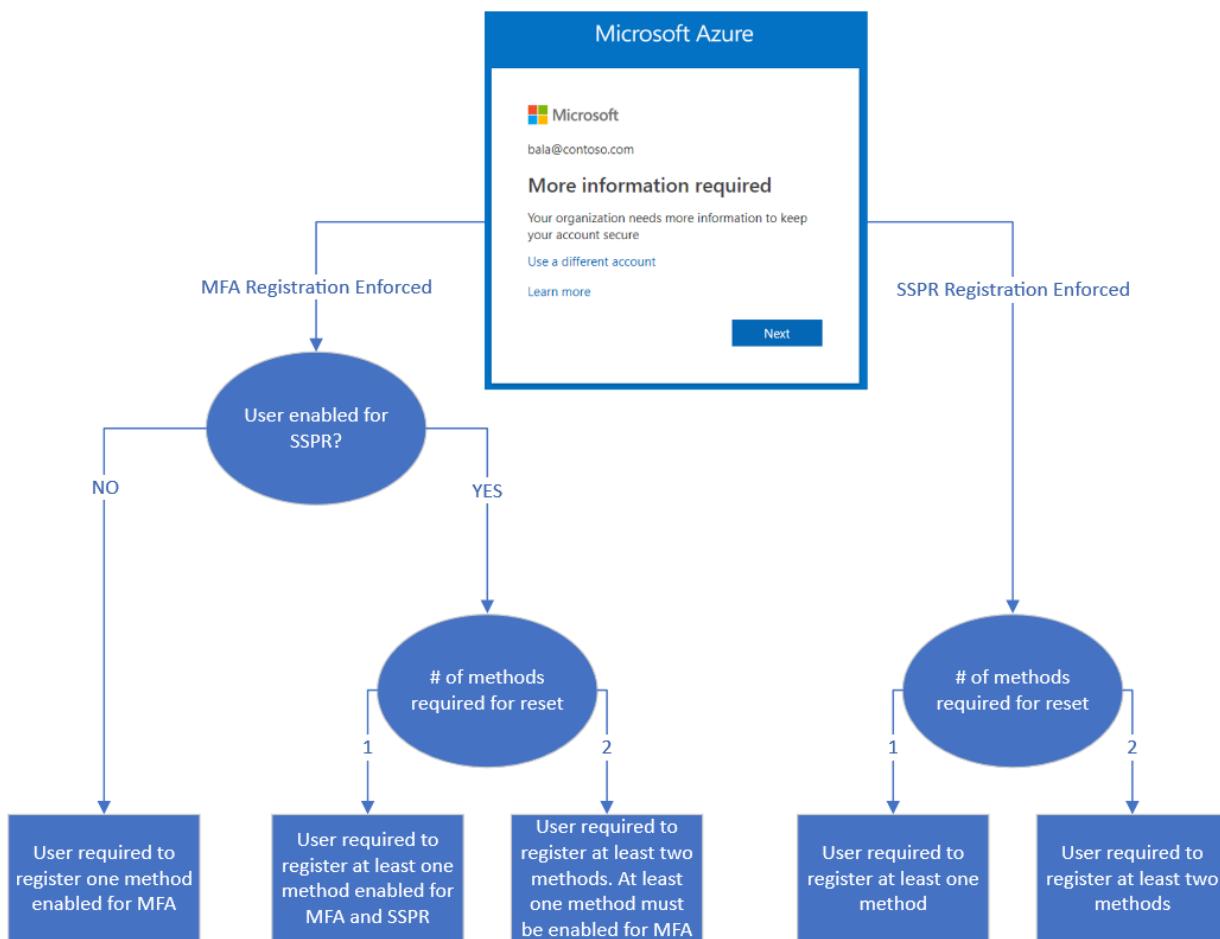
- Desviar las llamadas del departamento de soporte técnico.
- Reemplazar el uso de contraseñas temporales.
- Reemplazar cualquier solución de autoservicio de administración de contraseñas existente que se base en una solución local.
- **Eliminar las contraseñas no seguras** de su organización.

NOTE

En el caso de las organizaciones con una suscripción de Azure AD Premium P2, se recomienda implementar SSPR y usarlo como parte de una [directiva de riesgo de usuario de Identity Protection](#).

Administración segura de credenciales

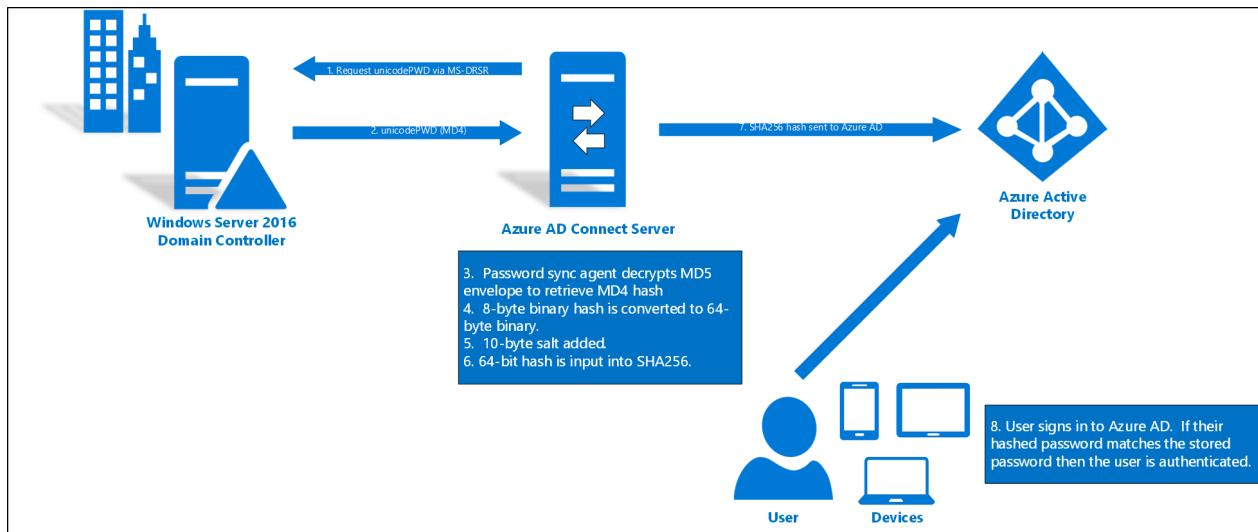
Las contraseñas por sí mismas no son lo suficientemente seguras para evitar que los actores no válidos obtengan acceso a su entorno. Como mínimo, cualquier usuario con una cuenta con privilegios debe estar habilitado para poder realizar la autenticación multifactor (MFA). Idealmente, debe habilitar el [registro combinado](#) y requerir que todos los usuarios se registren en MFA y SSPR mediante la [experiencia de registro combinada](#). Asimismo, se recomienda adoptar una estrategia para [proporcionar resistencia](#) y así reducir el riesgo de bloqueo debido a circunstancias imprevistas.



Resistencia de la autenticación a las interrupciones locales

Además de las ventajas de la simplicidad y la posibilidad de habilitar la detección de credenciales filtradas, la sincronización de hash de contraseñas (PHS) de Azure AD y Azure MFA permiten a los usuarios obtener acceso a las aplicaciones SaaS y a Office 365 a pesar de las interrupciones locales debido a ciberataques, como [NotPetya](#). También es posible habilitar PHS mientras esté usando la federación. Si habilita PHS, podrá realizar una reserva de autenticación cuando los servicios de federación no estén disponibles.

Si la organización local no tiene una estrategia de resistencia frente a interrupciones o tiene una que no está integrada con Azure AD, debe implementar PHS de Azure AD y definir un plan de recuperación ante desastres que incluya PHS. Si habilita PHS de Azure AD, los usuarios podrán autenticarse en Azure AD si su instancia de Active Directory local no está disponible.



Para comprender mejor las opciones de autenticación, consulte [Elegir el método de autenticación adecuado para la solución de identidad híbrida de Azure Active Directory](#).

Uso de credenciales mediante programación

Los scripts de Azure AD que utilizan PowerShell o las aplicaciones que usan Microsoft Graph API requieren una autenticación segura. La mala administración de credenciales que ejecutan esos scripts y herramientas aumenta el riesgo de robo de credenciales. Si usa scripts o aplicaciones que se basan en contraseñas codificadas de forma rígida o en mensajes de contraseñas, primero debe revisar las contraseñas de los archivos de configuración o el código fuente y, a continuación, reemplazar esas dependencias y usar las identidades administradas de Azure, la autenticación integrada de Windows o los [certificados](#) siempre que sea posible. En cuanto a aplicaciones donde no se puedan aplicar las soluciones anteriores, use [Azure Key Vault](#).

Si ve que hay entidades de servicio con credenciales de contraseña y no está seguro de cómo los scripts o las aplicaciones protegen esas credenciales de contraseña, póngase en contacto con el propietario de la aplicación para comprender mejor los patrones de uso.

Microsoft también le recomienda que se ponga en contacto con los propietarios de las aplicaciones para comprender los patrones de uso, si es que existen entidades de servicio con credenciales de contraseña.

Experiencia de autenticación

Autenticación local

La autenticación federada con la Autenticación integrada de Windows (IWA) o la autenticación administrada de inicio de sesión único (SSO) de conexión directa con la sincronización de hash de contraseña o la autenticación de paso a través, es la mejor experiencia de usuario cuando use la red corporativa relacionada con los controladores de dominio locales. Gracias a ello, se minimiza la fatiga de la petición de credenciales y reduce el riesgo de que los usuarios caigan en ataques de suplantación de identidad. Si ya usa la autenticación administrada en la nube con PHS o PTA, pero los usuarios todavía tienen que escribir su contraseña al autenticarse de forma local, debe implementar de inmediato el [SSO de conexión directa](#). Por otro lado, si está federado con planes para migrar definitivamente a la autenticación administrada en la nube, debe implementar el SSO de conexión directa como parte del proyecto de migración.

Directivas de acceso de confianza de dispositivos

Al igual que un usuario de su organización, un dispositivo es una identidad principal que desea proteger. Puede usar una identidad de dispositivo para proteger los recursos en cualquier momento y ubicación. La autenticación

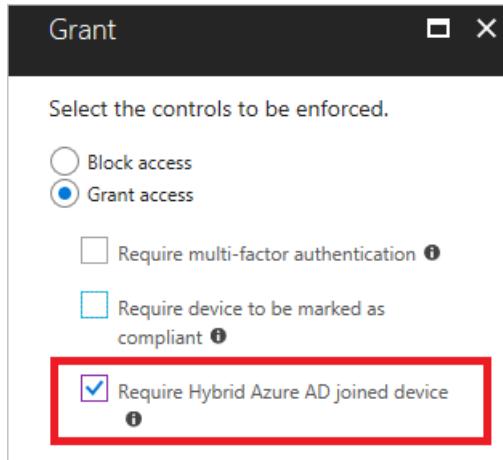
del dispositivo y tener en cuenta su tipo de confianza mejoran la seguridad y facilidad de uso, ya que:

- Se evita la fricción, por ejemplo, con MFA, cuando el dispositivo es de confianza.
- Se bloquea el acceso desde dispositivos que no son de confianza.
- En el caso de los dispositivos Windows 10, es posible usar el [inicio de sesión único en los recursos locales sin problemas](#).

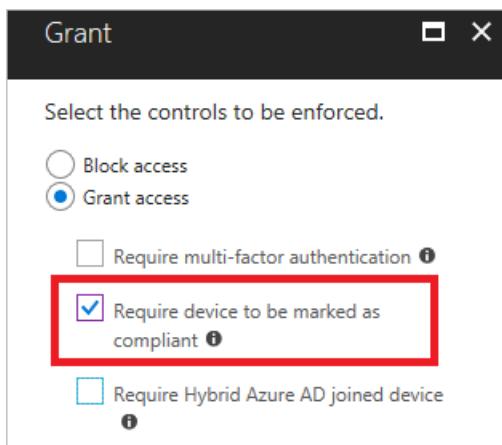
Puede llevar a cabo este objetivo mediante la incorporación de identidades de dispositivo, y administrarlas en Azure AD mediante uno de los métodos siguientes:

- Las organizaciones pueden usar [Microsoft Intune](#) para administrar el dispositivo y aplicar las directivas de cumplimiento, atestar el estado del dispositivo y establecer directivas de acceso condicional en función de si el dispositivo es compatible. Microsoft Intune puede administrar dispositivos iOS, dispositivos de escritorio Mac (a través de la integración JAMF), dispositivos de escritorio de Windows (de modo nativo mediante la administración de dispositivos móviles para Windows 10 y la administración conjunta con Microsoft Endpoint Configuration Manager) y dispositivos móviles Android.
- La [combinación de Azure AD híbrido](#) proporciona la opción de administrar contenido con directivas de grupo o Microsoft Endpoint Configuration Manager en un entorno con equipos unidos a un dominio de Active Directory. Las organizaciones pueden implementar un entorno administrado a través de PHS o PTA con un SSO de conexión directa. Si lleva sus dispositivos a Azure AD, podrá maximizar la productividad de los usuarios a través de SSO en los recursos locales y en la nube, a la vez que protegerá el acceso a los recursos en la nube y locales con la opción de [acceso condicional](#) al mismo tiempo.

Si tiene dispositivos Windows unidos a un dominio que no están registrados en la nube, o dispositivos Windows unidos a un dominio que sí están registrados en la nube, pero sin directivas de acceso condicional, debe registrar los dispositivos no registrados y, en cualquier caso, [usar la combinación de Azure AD híbrido como control](#) de las directivas de acceso condicional.



Si está administrando dispositivos con MDM o Microsoft Intune, pero no usa controles de dispositivo en las directivas de acceso condicional, se recomienda usar la opción [Requerir que el dispositivo esté marcado como compatible](#) como control en esas directivas.



Lectura recomendada de directivas de acceso de confianza al dispositivo

- [Cómo: Planificar la implementación de la combinación a Azure Active Directory híbrido](#)
- [Configuraciones de acceso de dispositivos e identidades](#)

Windows Hello para empresas

En Windows 10, [Windows Hello para empresas](#) reemplaza las contraseñas por la autenticación en dos fases segura en equipos. Windows Hello para empresas permite obtener una experiencia de MFA más simplificada para los usuarios y reduce la dependencia de las contraseñas. Si no ha comenzado a implementar dispositivos con Windows 10 o solo los ha implementado parcialmente, se recomienda actualizar a Windows 10 y [habilitar Windows Hello para empresas](#) en todos los dispositivos.

Si quiere obtener más información sobre la autenticación sin contraseñas, consulte [Un mundo sin contraseñas con Azure Active Directory](#).

Asignación y autenticación de la aplicación

Inicio de sesión único para aplicaciones

Proporcionar un mecanismo estándar de inicio de sesión único para toda la empresa es fundamental para mejorar la experiencia del usuario, reducir el riesgo, generar informes y facilitar el gobierno. Si usa aplicaciones que admiten SSO con Azure AD pero actualmente están configuradas para usar cuentas locales, debe volver a configurar esas aplicaciones para poder usar SSO con Azure AD. Del mismo modo, si usa cualquier aplicación que admite SSO con Azure AD pero usa otro proveedor de identidades, debe volver a configurar esas aplicaciones para usar SSO con Azure AD también. En el caso de las aplicaciones que no admiten protocolos de federación, pero que admiten la autenticación basada en formularios, se recomienda que configure la aplicación para usar el [almacenamiento de contraseñas](#) con Azure AD Application Proxy.

Mode: Password-based Sign-on

Sign-on URL: https://expenses-f128.msappproxy.net/ExpenseReporting ✓

NOTE

Si no tiene un mecanismo para detectar aplicaciones no administradas en su organización, le recomendamos que implemente un proceso de detección mediante una solución de agente de seguridad de acceso a la nube (CASB), como Microsoft Cloud App Security.

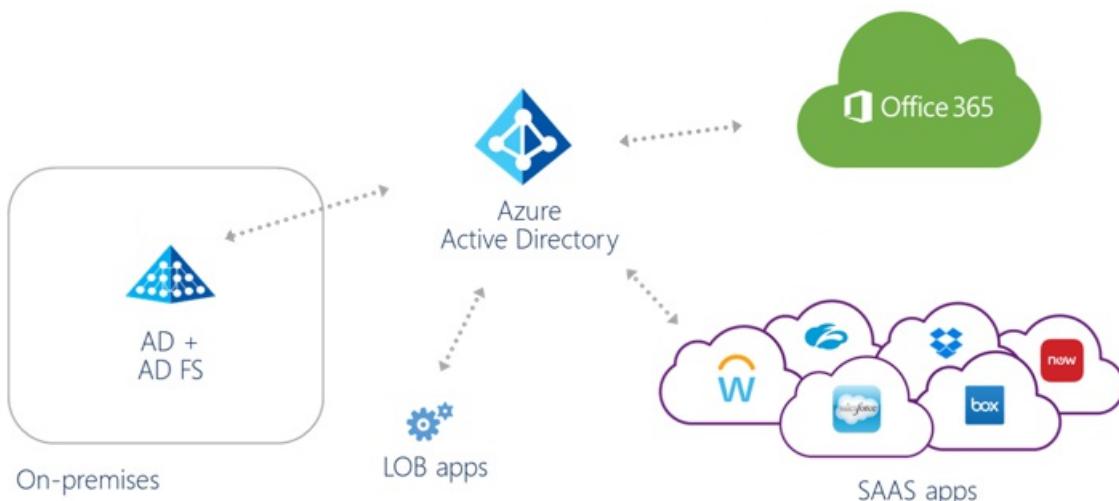
Por último, si tiene una galería de aplicaciones de Azure AD y usa aplicaciones que admiten SSO con Azure AD, es recomendable [enumerar la aplicación en la galería de aplicaciones](#).

Lectura recomendada del inicio de sesión único

- [¿Qué es el acceso a aplicaciones y el inicio de sesión único con Azure Active Directory?](#)

Migración de aplicaciones de AD FS a Azure AD

La [migración de aplicaciones desde AD FS a Azure AD](#) habilita funcionalidades adicionales en cuanto a seguridad, capacidad de administración más coherente y una mejor experiencia de colaboración. Si tiene aplicaciones configuradas en AD FS que admiten SSO con Azure AD, debe volver a configurar esas aplicaciones para que usen SSO con Azure AD. Si tiene aplicaciones configuradas en AD FS con configuraciones poco comunes y que no admite Azure AD, debe ponerse en contacto con los propietarios de la aplicación para saber si la configuración especial es un requisito absoluto de la aplicación. Si no es necesario, debe volver a configurar la aplicación para usar SSO con Azure AD.



NOTE

Azure AD Connect Health para ADFS se puede usar para recopilar los detalles de configuración de cada aplicación que se pueda migrar a Azure AD.

Asignar usuarios a aplicaciones

La [asignación de usuarios a las aplicaciones](#) se realiza mejor cuando se usan grupos, porque permiten una gran flexibilidad y la posibilidad de administrarlos a escala. Las ventajas de usar grupos incluyen las opciones de [pertенencia dinámica a grupos basada en atributos](#) y de [delegación a los propietarios de las aplicaciones](#). Por lo tanto, si ya usa y administra grupos, es recomendable realizar las siguientes acciones para mejorar la administración a escala:

- Delegar la administración y la gobernanza de grupos a los propietarios de la aplicación.
- Permitir el acceso de autoservicio a la aplicación.
- Definir grupos dinámicos si los atributos de usuario pueden determinar de forma coherente el acceso a las aplicaciones.
- Implementar la atestación en los grupos que se usan para obtener acceso a las aplicaciones mediante la

srevisiones de acceso de Azure AD.

Por otro lado, si encuentra aplicaciones que tienen una asignación a usuarios individuales, asegúrese de implementar la [gobernanza](#) en esas aplicaciones.

Lectura recomendada para asignar usuarios a aplicaciones

- [Asignación de usuarios y grupos en una aplicación de Azure Active Directory](#)
- [Delegación de permisos de registro de aplicaciones en Azure Active Directory](#)
- [Reglas de pertenencia dinámica a grupos de Azure Active Directory](#)

Directivas de acceso

Ubicaciones con nombre

Gracias a las [ubicaciones con nombre](#) en Azure AD, puede etiquetar intervalos de direcciones IP de confianza en su organización. Azure AD usa las ubicaciones con nombre para:

- Prevenir falsos positivos en eventos de riesgo. Si se inicia sesión desde una ubicación de confianza se reduce el riesgo en el inicio de sesión del usuario.
- Configurar el [acceso condicional basado en la ubicación](#).

The screenshot shows the 'Conditional access - Named locations' page in the Azure Active Directory portal. On the left, there's a sidebar with 'Policies' and sections for 'MANAGE' (including 'Named locations', which is highlighted with a red box), 'Custom controls (preview)', 'Terms of use', 'VPN connectivity', 'Classic policies', and 'TROUBLESHOOTING + SUPPORT' (with 'Troubleshoot' and 'New support request'). At the top right, there are buttons for '+ New location' and 'Configure MFA trusted IPs'. Below these buttons, a note states: 'Named locations are used by Azure AD security reports to reduce false positives and Azure AD conditional access policies.' A 'Search locations...' input field is also present. The main area displays a table with one row: 'No networks' under the 'NAME' column and 'TRUSTED' under the 'TRUSTED' column.

Según la prioridad, use la tabla siguiente para encontrar la solución recomendada que mejor se adapte a las necesidades de su organización:

PRIORIDAD	ESCENARIO	RECOMENDACIÓN
1	Si usa PHS o PTA y no se han definido las ubicaciones con nombre	Defina las ubicaciones con nombre para mejorar la detección de eventos de riesgo.
2	Si está federado y no usa la notificaciones de tipo "insideCorporateNetwork" y si no se han definido las ubicaciones con nombre	Defina las ubicaciones con nombre para mejorar la detección de eventos de riesgo.

PRIORIDAD	ESCENARIO	RECOMENDACIÓN
3	Si no usa ubicaciones con nombre en las directivas de acceso condicional y no hay ningún riesgo ni controles de dispositivo en las directivas de acceso condicional	Configure la directiva de acceso condicional para incluir ubicaciones con nombre.
4	Si está federado y usa la notificación de tipo "insideCorporateNetwork" y no se han definido las ubicaciones con nombre	Defina las ubicaciones con nombre para mejorar la detección de eventos de riesgo.
5	Si usa direcciones IP de confianza con MFA en lugar de ubicaciones con nombre y las marca como de confianza	Defina ubicaciones con nombre y márquelas como de confianza para mejorar la detección de eventos de riesgo.

Directivas de acceso basadas en riesgos

Azure AD puede calcular el riesgo de todos los inicios de sesión y de todos los usuarios. El uso del riesgo como criterio en las directivas de acceso puede proporcionar una experiencia de usuario mejor (por ejemplo, recibirá menos mensajes de autenticación y la seguridad será superior); solo debe preguntar a los usuarios cuando sea necesario y automatizar la respuesta y la corrección.



Si ya posee licencias de Azure AD Premium P2 que admiten el uso del riesgo en las directivas de acceso, pero no se usan estas directivas, le recomendamos encarecidamente agregar riesgo a su posición de seguridad.

Lectura recomendada de directivas de acceso basadas en riesgos

- [Cómo: configurar la directiva de riesgo de inicio de sesión](#)
- [Cómo: configurar la directiva de riesgo de usuario](#)

Directivas de acceso de aplicaciones cliente

La administración de aplicaciones de Microsoft Intune (MAM) ofrece la posibilidad de incorporar controles de protección de datos como el cifrado de almacenamiento, el PIN o la limpieza remota del almacenamiento a aplicaciones móviles cliente compatibles, como Outlook Mobile. Además, se pueden crear directivas de acceso condicional para [restringir el acceso](#) a servicios en la nube, como Exchange Online, desde aplicaciones aprobadas o compatibles.

Si los empleados instalan aplicaciones compatibles con MAM, como aplicaciones móviles de Office, para obtener acceso a recursos corporativos como Exchange Online o SharePoint Online, y si también admite la opción BYOD (traiga su propio dispositivo), es recomendable implementar las directivas de MAM de la aplicación para administrar la configuración de la aplicación en dispositivos de su propiedad sin tener que realizar la inscripción de MDM; a continuación, solo debe actualizar las directivas de acceso condicional para permitir el acceso solo desde clientes compatibles con MAM.



Si los empleados instalan aplicaciones compatibles con MAM en recursos corporativos y el acceso está restringido en los dispositivos que administra Intune, debe considerar la posibilidad de implementar directivas MAM de aplicaciones, para así poder administrar la configuración de la aplicación en dispositivos personales. Actualice las directivas de acceso condicional para permitir el acceso solo desde clientes compatibles con MAM.

Implementación del acceso condicional

El acceso condicional es una herramienta esencial para mejorar la posición de seguridad de su organización. Por lo tanto, es importante que siga estos procedimientos recomendados:

- Asegúrese de que todas las aplicaciones SaaS tienen al menos una directiva aplicada.
- Evite combinar el filtro **Todas las aplicaciones** con el control de **bloqueo**, para evitar el riesgo de bloqueo.
- Evite usar la opción **Todos los usuarios** como filtro y agregar sin querer **Invitados**.
- **Migre todas las directivas "heredadas" a Azure Portal**
- Recopile todos los criterios de los usuarios, los dispositivos y las aplicaciones.
- Use las directivas de acceso condicional para **implementar MFA**, en lugar de usar un **MFA por usuario**.
- Conserve un pequeño conjunto de directivas básicas que se puedan aplicar a varias aplicaciones.
- Defina grupos de excepciones vacíos y agréguelos a las directivas para tener una estrategia de excepción.
- Planifique las cuentas de **emergencia** sin controles MFA.
- Asegúrese de que proporciona una experiencia coherente entre las aplicaciones cliente de Office 365 (por ejemplo, Teams, OneDrive para la Empresa o Outlook) al implementar el mismo conjunto de controles para servicios como Exchange Online y SharePoint Online.
- Recuerde que la asignación a directivas debe implementarse a través de grupos, no de personas.
- Realice revisiones periódicas de los grupos de excepciones que se usan en las directivas para limitar el tiempo que los usuarios no usan la posición de seguridad. Si tiene Azure AD P2, puede usar las revisiones de acceso para automatizar el proceso.

- [Procedimientos recomendados para el acceso condicional en Azure Active Directory](#)
- [Configuraciones de acceso de dispositivos e identidades](#)
- [Referencia de configuración del acceso condicional de Azure Active Directory](#)
- [Directivas de acceso condicional habituales](#)

Área expuesta de acceso

Autenticación heredada

Las credenciales seguras, como MFA, no pueden proteger las aplicaciones que usan protocolos de autenticación heredados, por lo que se convierten en el objetivo de ataque preferido de los actores malintencionados. Bloquear la autenticación heredada es fundamental para mejorar la posición de seguridad de acceso.

La autenticación heredada es un término que hace referencia a los protocolos de autenticación que usan aplicaciones como:

- Clientes de Office antiguos que no usan la autenticación moderna (por ejemplo, un cliente de Office 2010).
- Clientes que usan protocolos de correo electrónico como IMAP/SMTP/POP.

Los atacantes prefieren estos protocolos; de hecho, casi el [100 % de los ataques de difusión de contraseñas](#) usan protocolos de autenticación heredados. Los hackers usan protocolos de autenticación heredados, ya que no admiten el inicio de sesión interactivo, que es necesario para superar otros desafíos de seguridad como la autenticación multifactor y la autenticación de dispositivos.

Si la autenticación heredada se usa ampliamente en su entorno, debe planear la migración de los clientes heredados a clientes que admitan una [autenticación moderna](#) lo antes posible. En el mismo token, si tiene algunos usuarios que ya usan la autenticación moderna, pero otros que siguen usando la autenticación heredada, debe realizar los siguientes pasos para bloquear a los clientes de autenticación heredada:

1. Use los [informes de actividad de inicio de sesión](#) para identificar a los usuarios que siguen usando la autenticación heredada y la corrección de planes:
 - a. Actualice los clientes con capacidad de autenticación moderna a los usuarios afectados.
 - b. Planifique un período de tiempo de transición para realizar un bloqueo según los pasos siguientes.
 - c. Identifique las aplicaciones heredadas que tengan una dependencia permanente en la autenticación heredada. Consulte el paso 3 que tiene a continuación.
2. Deshabilite los protocolos heredados en el origen (por ejemplo, el buzón de correo de Exchange) para los usuarios que no usen la autenticación heredada para así evitar una mayor exposición.
3. En el caso de las cuentas restantes (idealmente, son las identidades no humanas, como las cuentas de servicio), use el [acceso condicional para restringir los protocolos heredados](#) después de la autenticación.

Lectura recomendada de la autenticación heredada

- [Habilitar o deshabilitar el acceso POP3 o IMAP4 a los buzones de Exchange Server](#)

Otorgar consentimientos

En un ataque para otorgar consentimientos ilícito, el atacante crea una aplicación registrada en Azure AD que solicita acceso a ciertos datos, como la información de contacto, el correo electrónico o los documentos. Los usuarios pueden otorgar su consentimiento a aplicaciones malintencionadas a través de ataques de suplantación de identidad (phishing) al acceder a sitios web malintencionados.

A continuación se muestra una lista de aplicaciones con permisos que es posible quiera examinar para los servicios en la nube de Microsoft:

- Aplicaciones con permisos *.ReadWrite delegados o de aplicación

- Aplicaciones con permisos delegados que pueden leer, enviar o administrar el correo electrónico en nombre del usuario
- Aplicaciones a las que se concede el uso de los siguientes permisos:

RESOURCE	PERMISO
Office 365 Exchange Online	EAS.AccessAsUser.All
	EWS.AccessAsUser.All
	Mail.Read
Microsoft Graph API	Mail.Read
	Mail.Read.Shared
	Mail.ReadWrite

- Aplicaciones a las que se le concede la suplantación completa del usuario que inició sesión. Por ejemplo:

RESOURCE	PERMISO
Microsoft Graph API	Directory.AccessAsUser.All
API REST de Azure	user_impersonation

Para evitar este escenario, consulte [Detectar y solucionar la concesión de consentimiento ilegal en Office 365](#) para identificar y corregir cualquier aplicación con concesiones ilícitas o aplicaciones que tengan más concesiones de las necesarias. A continuación, [quite el autoservicio por completo](#) y [establezca los procedimientos de gobernanza](#). Por último, programe revisiones periódicas de los permisos de la aplicación y quítelos cuando no sean necesarios.

Lectura recomendada para otorgar consentimientos

- [Permisos para Microsoft Graph API](#)

Configuración de usuario y de grupo

A continuación, se muestra la configuración de usuario y de grupo que se puede bloquear si no existe una necesidad empresarial explícita:

Configuración de usuario

- **Usuarios externos:** la colaboración externa puede producirse de forma orgánica en la empresa mediante servicios como Teams, Power BI, SharePoint Online y Azure Information Protection. Si tiene restricciones explícitas para controlar cualquier colaboración externa que inicie el usuario, es recomendable que habilite usuarios externos mediante la [administración de derechos de Azure AD](#) o con una operación controlada como, por ejemplo, a través del departamento de soporte técnico. Si no quiere permitir la colaboración externa orgánica en los servicios, puede [impedir totalmente que los miembros inviten a usuarios externos](#). Como alternativa, también puede [permitir o bloquear dominios específicos](#) en invitaciones de usuarios externos.
- **Registros de aplicaciones:** cuando la característica Registros de aplicaciones está habilitada, los usuarios finales pueden incorporar aplicaciones y conceder acceso a sus datos. Un ejemplo típico de la característica Registro de aplicaciones, son los usuarios que habilitan los complementos de Outlook o los asistentes de voz como Alexa y Siri que se usan para leer los correos electrónicos y el calendario, o para enviar correos electrónicos en su nombre. Si el cliente decide desactivar Registro de aplicaciones, los equipos de InfoSec e IAM deben participar en la administración de excepciones (esto es, registros de aplicaciones que son necesarios según los requisitos empresariales), ya que tendrán que registrar las aplicaciones con una cuenta de administrador, y lo más probable es que necesite diseñar un proceso para poner en marcha esta operación.

- **Portal de administración:** las organizaciones pueden bloquear la hoja de Azure AD en Azure Portal para que los usuarios que no sean administradores no puedan obtener acceso a la administración de Azure AD en Azure Portal y se confundan debido a ello. Vaya a la configuración de usuario en el portal de administración de Azure AD para restringir el acceso:

The screenshot shows the 'Enterprise applications' section of the Azure Portal. At the top, there is a header with the title 'Enterprise applications' and a sub-header 'Manage how end users launch and view their applications'. Below this, there is a section titled 'App registrations' with the sub-header 'Users can register applications'. Underneath this, there is a button with two options: 'Yes' (highlighted in blue) and 'No'. A red rectangular box highlights a section titled 'Administration portal' with the sub-header 'Restrict access to Azure AD administration portal'. This section also has a button with 'Yes' (highlighted in blue) and 'No'.

NOTE

Los usuarios que no son administradores todavía pueden obtener acceso a las interfaces de administración de Azure AD a través de la línea de comandos u otras interfaces de programación.

Configuración de grupo

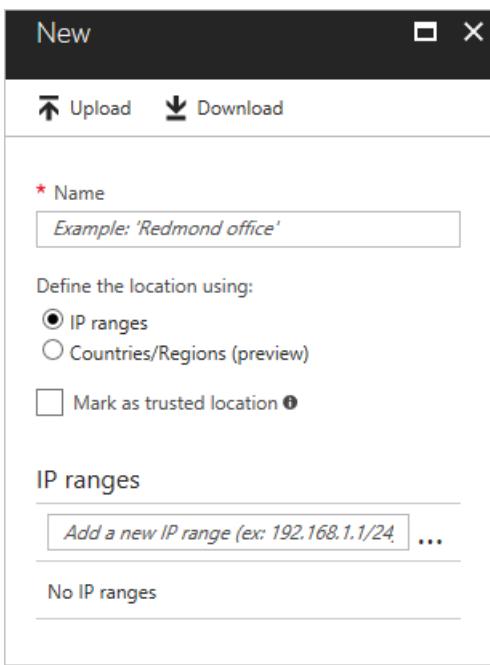
Administración de grupos de autoservicio: los usuarios pueden crear grupos de seguridad o grupos de O365. Si no hay ninguna iniciativa de autoservicio actual para los grupos en la nube, los clientes pueden decidir desactivarla hasta que estén listos para usar esta funcionalidad.

Lectura recomendada de grupos

- [¿Qué es la colaboración B2B de Azure Active Directory?](#)
- [Integración de aplicaciones con Azure Active Directory](#)
- [Aplicaciones, permisos y consentimiento en Azure Active Directory](#)
- [Uso de grupos para administrar el acceso a recursos en Azure Active Directory](#)
- [Configuración de la administración del acceso a aplicaciones de autoservicio en Azure Active Directory](#)

Tráfico desde ubicaciones inesperadas

Los atacantes son de varias partes del mundo. Administre este riesgo mediante el uso de directivas de acceso condicional con la ubicación establecida como condición. La [condición de ubicación](#) de una directiva de acceso condicional le permite bloquear el acceso a ubicaciones donde no haya ningún motivo empresarial debido al cual se deba iniciar sesión.



Si está disponible, use una solución de Administración de eventos e información de seguridad (SIEM) para analizar y buscar patrones de acceso entre regiones. Si no usa un producto SIEM o no ingiere información de autenticación de Azure AD, se recomienda usar [Azure Monitor](#) para identificar patrones de acceso entre regiones.

Uso de acceso

Registros de Azure AD archivados e integrados con planes de respuesta a incidentes

Tener acceso a la actividad de inicio de sesión, las auditorías y los eventos de riesgo de Azure AD es fundamental para la solución de problemas, el análisis de uso y las investigaciones de análisis forense. Azure AD proporciona acceso a estos orígenes a través de las API de REST que tienen un período de retención limitado. Un sistema de Administración de eventos e información de seguridad (SIEM) o una tecnología de archivo equivalente, es fundamental para el almacenamiento a largo plazo de auditorías y compatibilidad. Para habilitar el almacenamiento a largo plazo de los registros de Azure AD, debe agregarlos a la solución SIEM existente o usar [Azure Monitor](#). Archive los registros que se puedan usar como parte de las investigaciones y los planes de respuesta a incidentes.

Lectura recomendada de registros

- [Referencia de la API de auditoría de Azure Active Directory](#)
- [Referencia de la API de informes de actividad de inicio de sesión de Azure Active Directory](#)
- [Obtención de datos mediante la API de informes de Azure AD con certificados](#)
- [Microsoft Graph para Azure Active Directory Identity Protection](#)
- [Referencia de la API de actividad de administración de Office 365](#)
- [Uso del paquete de contenido de Power BI de Azure Active Directory](#)

Resumen

Existen 12 aspectos en una infraestructura de identidades segura. Esta lista le permitirá administrar y asegurar las credenciales, definir la experiencia de autenticación, delegar la asignación, medir el uso y definir las directivas de acceso basadas en la postura de seguridad de la empresa.

- Asignar propietarios a las tareas principales.
- Implementar soluciones para detectar contraseñas débiles o filtradas, mejore la protección y la administración de contraseñas y proteja aún más el acceso de los usuarios a los recursos.
- Administrar la identidad de los dispositivos para proteger los recursos en cualquier momento y desde cualquier ubicación.

- Implementar la autenticación con contraseña.
- Proporcionar un mecanismo de inicio de sesión único estandarizado en toda la organización.
- Migrar aplicaciones desde AD FS a Azure AD para obtener una seguridad mejor y una capacidad de administración más coherente.
- Asignar usuarios a las aplicaciones mediante el uso de grupos para permitir una mayor flexibilidad y capacidad administrativa a escala.
- Configurar directivas de acceso basadas en riesgos.
- Bloquear los protocolos de autenticación heredados.
- Detectar y corrija las opciones ilícitas para otorgar consentimiento.
- Bloquear la configuración de usuario y de grupo.
- Habilitar el almacenamiento a largo plazo de registros de Azure AD para la solución de problemas, el análisis de uso y las investigaciones de análisis forense.

Pasos siguientes

Comience a trabajar con las [comprobaciones y las acciones operativas de gobernanza de identidad](#).

Guía de referencia de operaciones de gobernanza de Azure Active Directory

22/07/2020 • 17 minutes to read • [Edit Online](#)

En esta sección de la [guía de referencia de operaciones de Azure AD](#) se describen las comprobaciones y las acciones que debe realizar para evaluar y confirmar el acceso concedido a las identidades sin privilegios y con privilegios, así como auditar y controlar los cambios en el entorno.

NOTE

Estas recomendaciones están actualizadas hasta la fecha de publicación, pero pueden cambiar con el tiempo. Las organizaciones deben evaluar continuamente sus prácticas de gobernanza a medida que los productos y servicios de Microsoft evolucionen con el tiempo.

Procesos operativos clave

Asignación de propietarios a las tareas clave

La administración de Azure Active Directory requiere la ejecución continua de tareas y procesos operativos clave que pueden no formar parte de un proyecto de lanzamiento. Aun así, es importante que configure estas tareas con miras a optimizar su entorno. Entre las tareas clave y sus propietarios recomendados se incluyen:

TAREA	PROPIETARIO
Archivado de registros de auditoría de Azure AD en el sistema SIEM	Equipo de operaciones de InfoSec
Detección de aplicaciones que se administran fuera del cumplimiento	Equipo de operaciones IAM
Revisión periódica del acceso a las aplicaciones	Equipo de arquitectura de InfoSec
Revisión periódica del acceso a identidades externas	Equipo de arquitectura de InfoSec
Revisión periódica de quién tiene roles con privilegios	Equipo de arquitectura de InfoSec
Definición de puertas de seguridad para activar los roles con privilegios	Equipo de arquitectura de InfoSec
Revisión periódica de las concesiones de consentimiento	Equipo de arquitectura de InfoSec
Diseño de catálogos y paquetes de acceso para aplicaciones y recursos basados en empleados de la organización	Propietarios de la aplicación
Definición de directivas de seguridad para asignar usuarios a paquetes de acceso	Equipo de InfoSec + propietarios de aplicaciones
Si las directivas incluyen flujos de trabajo de aprobación, revisión periódica de las aprobaciones de flujo de trabajo	Propietarios de la aplicación

TAREA	PROPIETARIO
Revisión de excepciones en las directivas de seguridad, como las directivas de acceso condicional, mediante las revisiones de acceso	Equipo de operaciones de InfoSec

A medida que revise la lista, es posible que tenga que asignar un propietario a las tareas que no tienen uno o ajustar la propiedad de aquellas tareas con propietarios que no coincidan con las recomendaciones anteriores.

Lecturas recomendadas para propietarios

- [Asignación de roles de administrador en Azure Active Directory](#)
- [Gobernanza en Azure](#)

Pruebas de los cambios de configuración

Hay cambios que requieren consideraciones especiales a la hora de realizar pruebas, desde técnicas sencillas como la implementación de un subconjunto de usuarios de destino para implementar un cambio en un inquilino de prueba paralelo. Si no ha implementado una estrategia de pruebas, debe definir un enfoque de pruebas basado en las directrices de la tabla siguiente:

ESCENARIO	RECOMENDACIÓN
Cambio del tipo de autenticación de federado a PHS/PTA o viceversa	Use la implementación por fases para probar la repercusión del cambio del tipo de autenticación.
Implementación de una nueva directiva de acceso condicional o una directiva de protección de identidad	Cree una nueva directiva de acceso condicional y asígnela a usuarios de prueba.
Incorporación de un entorno de prueba de una aplicación	Agregue la aplicación a un entorno de producción, ocúltela en el panel Mis aplicaciones y asígnela a usuarios de prueba durante la fase de control de calidad.
Cambio de las reglas de sincronización	Realice los cambios en una instancia de Azure AD Connect de prueba con la misma configuración que está actualmente en producción, también conocido como modo de ensayo, y analice los resultados de CSExport. Si está satisfecho, pase a producción cuando esté listo.
Cambio de marca	Pruebe en un inquilino de prueba independiente.
Implementación de una nueva característica	Si la característica admite la implementación en un conjunto de usuarios de destino, asigne unos usuarios piloto y prosiga con la implementación. Por ejemplo, el autoservicio de restablecimiento de contraseña y la autenticación multifactor pueden dirigirse a usuarios o grupos específicos.
Traslado de una aplicación de un proveedor de identidades local (IdP), como Active Directory, a Azure AD	Si la aplicación admite varias configuraciones de IdP, por ejemplo, Salesforce, configure y pruebe Azure AD durante una ventana de cambio (en caso de que la aplicación introduzca la página de HRD). Si la aplicación no admite varios IdP, programe las pruebas durante una ventana de control de cambios y el tiempo de inactividad del programa.
Actualización de reglas de grupo dinámico	Cree un grupo dinámico paralelo con la nueva regla. Compare con el resultado calculado, por ejemplo, ejecute PowerShell con la misma condición. Si la prueba es satisfactoria, intercambie los lugares donde se usó el grupo anterior (si es factible).

ESCENARIO	RECOMENDACIÓN
Migración de licencias de productos	Consulte Cambio de la licencia de un solo usuario de un grupo con licencia en Azure Active Directory .
Cambio de reglas de AD FS como autorización, emisión, MFA	Use las notificaciones de grupo para dirigirse a un subconjunto de usuarios.
Cambio de la experiencia de autenticación de AD FS o cambios similares en toda la granja de servidores	Cree una granja de servidores paralela con el mismo nombre de host, implemente cambios de configuración y realice pruebas en clientes mediante el archivo HOSTS, las reglas de enrutamiento de NLB o un enrutamiento similar. Si la plataforma de destino no admite archivos HOSTS (por ejemplo, dispositivos móviles), controle el cambio.

Revisiones de acceso

Revisiones de acceso a las aplicaciones

Con el tiempo, los usuarios pueden acumular acceso a recursos a medida que van rotando entre distintos equipos y puestos. Es importante que los propietarios de los recursos revisen el acceso a las aplicaciones de forma regular y quiten los privilegios que ya no se necesiten durante todo el ciclo de vida de los usuarios. Las [revisiones de acceso](#) de Azure AD permiten a las organizaciones administrar de forma eficiente las pertenencias a grupos, el acceso a las aplicaciones empresariales y las asignaciones de roles. Los propietarios de los recursos deben revisar el acceso de los usuarios de forma periódica para asegurarse de que solo las personas adecuadas tengan acceso continuado. Idealmente, debería considerar el uso de revisiones de acceso de Azure AD para esta tarea.

Manage user's access with Azure AD Access Reviews

Recertify group memberships, access to enterprise applications, and privileged role assignments with Azure Active Directory (Azure AD) Access Reviews.

Getting started is fast and easy. You can start your access review within minutes.

1. Onboard with one-click
2. Create your first access review

Use Azure AD Access Reviews to:

- ✓ Recertify employee and guest's group memberships, access to applications, and role assignments on a recurring basis
- ✓ Automate access removal with custom settings
- ✓ Make informed decisions with the help of smart recommendations
- ✓ Organize and track reviews for compliance and risk management initiatives

[Onboard now](#)

NOTE

Cada usuario que interactúa con las revisiones de acceso debe tener una licencia de pago de Azure AD Premium P2.

Revisiones de acceso a identidades externas

Es fundamental mantener el acceso a las identidades externas restringido solo a los recursos necesarios, durante el tiempo necesario. Establezca un proceso de revisión de acceso automatizado periódico para todas las identidades externas y el acceso a las aplicaciones mediante [revisiones de acceso](#) de Azure AD. Si ya existe un

proceso local, considere la posibilidad de usar revisiones de acceso de Azure AD. Una vez que una aplicación se retire o se deje de usar, quite todas las identidades externas que tuvieran acceso a la aplicación.

NOTE

Cada usuario que interactúa con las revisiones de acceso debe tener una licencia de pago de Azure AD Premium P2.

Administración de cuentas con privilegios

Uso de cuenta con privilegios

Los hackers a menudo tienen como objetivo las cuentas de administrador y otros elementos con acceso privilegiado para obtener acceso rápido a datos confidenciales y a sistemas. Dado que con el tiempo tienden a acumularse los usuarios con roles con privilegios, es importante revisar y administrar el acceso de administrador de forma periódica y proporcionar acceso con privilegios cuando sea necesario a Azure AD y los recursos de Azure.

Si no hay ningún proceso en su organización para administrar cuentas con privilegios o si actualmente tiene administradores que usan sus cuentas de usuario habituales para administrar servicios y recursos, debe empezar a usar cuentas independientes, por ejemplo, una para las actividades habituales del día a día y otra para el acceso privilegiado configurada con MFA. Mejor aún, si su organización tiene una suscripción Azure AD Premium P2, debe implementar inmediatamente [Azure AD Privileged Identity Management \(PIM\)](#). En el mismo token, también debe revisar esas cuentas con privilegios y [asignar roles con menos privilegios](#), si procede.

Otro aspecto de la administración de cuentas con privilegios que se debe implementar es la definición de [revisiones de acceso](#) para esas cuentas, ya sea de forma manual o [automatizada a través de PIM](#).

Lectura recomendada para la administración de cuentas con privilegios

- [Roles en Privileged Identity Management de Azure AD](#)

Cuentas de acceso de emergencia

Las organizaciones deben crear [cuentas de emergencia](#) a fin de prepararse para administrar Azure AD en casos de interrupciones de autenticación como los siguientes:

- Interrupción de los componentes de las infraestructuras de autenticación (AD FS, AD local, servicio MFA)
- Rotación del personal administrativo

Para evitar el bloqueo accidental del inquilino por no poder iniciar sesión o activar una cuenta de usuario individual existente como administrador, debe crear dos o más cuentas de emergencia y asegurarse de que estén implementadas y alineadas con los [procedimientos recomendados de Microsoft](#) y los [procedimientos de emergencia](#).

Acceso con privilegios al portal del Contrato Enterprise de Azure

El [portal de Contrato Enterprise de Azure \(Azure EA\)](#) le permite crear suscripciones de Azure en el marco de un Contrato Enterprise, que es un rol importante dentro de la empresa. Es habitual comenzar la creación de este portal antes incluso de que Azure AD esté vigente, por lo que es necesario usar identidades de Azure AD para bloquearlo, quitar cuentas personales del portal, asegurarse de que está implantada la delegación habitual y mitigar el riesgo de bloqueo.

En aras de la claridad, si el nivel de autorización del portal de EA está configurado actualmente en "modo mixto", debe eliminar cualquier [cuenta Microsoft](#) de todos los accesos con privilegios del portal de EA y configurar el portal de EA para usar solo cuentas de Azure AD. Si los roles delegados del portal de EA no están configurados, también debe buscar e implementar roles delegados para departamentos y cuentas.

Lectura recomendada para el acceso con privilegios

- [Permisos de roles de administrador en Azure Active Directory](#)

Administración de derechos

La [administración de derechos \(EM\)](#) permite a los propietarios de aplicaciones agrupar recursos y asignarlos a roles específicos de la organización (tanto internos como externos). Además, posibilita la delegación y el registro de autoservicio a los propietarios empresariales, a la vez que mantiene las directivas de gobernanza para conceder acceso, establecer duraciones de acceso y permitir flujos de trabajo de aprobación.

NOTE

La administración de derechos de Azure AD requiere licencias de Azure AD Premium P2.

Resumen

Una gobernanza de identidad segura está conformada por ocho aspectos. Esta lista le ayudará a identificar las acciones que debe realizar para evaluar y confirmar el acceso concedido a las identidades sin privilegios y con privilegios, así como auditar y controlar los cambios en el entorno.

- Asignar propietarios a las tareas principales.
- Implementar una estrategia de pruebas.
- Usar las revisiones de acceso de Azure AD para administrar de forma eficiente las pertenencias a grupos, el acceso a las aplicaciones empresariales y las asignaciones de roles.
- Establecer un proceso de revisión de acceso automatizado periódico para todos los tipos de identidades externas y acceso a las aplicaciones.
- Establecer un proceso de revisión de acceso para revisar y administrar el acceso de administrador de forma periódica y proporcionar acceso con privilegios cuando es necesario a Azure AD y los recursos de Azure.
- Aprovisionar cuentas de emergencia para que estén preparadas para administrar Azure AD ante interrupciones inesperadas.
- Bloquear el acceso al portal de Azure EA.
- Implementar la administración de derechos para proporcionar acceso controlado a una colección de recursos.

Pasos siguientes

Comience a trabajar con las [comprobaciones y las acciones operativas de Azure AD](#).

Referencia de la guía de operaciones generales de Azure Active Directory

22/07/2020 • 19 minutes to read • [Edit Online](#)

En esta sección de la [guía de referencia de operaciones de Azure AD](#) se describen las comprobaciones y las acciones que debe realizar para optimizar las operaciones generales de Azure Active Directory (Azure AD).

NOTE

Estas recomendaciones están actualizadas hasta la fecha de publicación, pero pueden cambiar con el tiempo. Las organizaciones deben evaluar continuamente sus prácticas de operaciones a medida que los productos y servicios de Microsoft evolucionen con el tiempo.

Procesos operativos clave

Asignación de propietarios a las tareas clave

La administración de Azure Active Directory requiere la ejecución continua de tareas y procesos operativos clave que pueden no formar parte de un proyecto de lanzamiento. Aun así, es importante que configure estas tareas con miras a optimizar su entorno. Entre las tareas clave y sus propietarios recomendados se incluyen:

TAREA	PROPIETARIO
Mejoras en la puntuación de seguridad de la identidad	Equipo de operaciones de InfoSec
Mantenimiento de servidores Azure AD Connect	Equipo de operaciones IAM
Ejecutar y evaluar periódicamente los informes de IdFix	Equipo de operaciones IAM
Evaluación de prioridades de las alertas de Azure AD Connect Health para la sincronización y AD FS	Equipo de operaciones IAM
Si no usa Azure AD Connect Health, el cliente tiene procesos y herramientas equivalentes para supervisar la infraestructura personalizada	Equipo de operaciones IAM
Si no usa AD FS, el cliente tiene procesos y herramientas equivalentes para supervisar la infraestructura personalizada	Equipo de operaciones IAM
Supervisar registros híbridos: Conectores de Azure AD Application Proxy	Equipo de operaciones IAM
Supervisar registros híbridos: Agentes para la autenticación de paso a través	Equipo de operaciones IAM
Supervisar registros híbridos: Servicio de escritura diferida de contraseñas	Equipo de operaciones IAM
Supervisar registros híbridos: Puerta de enlace de protección con contraseña local	Equipo de operaciones IAM

TAREA	PROPIETARIO
Supervisar registros híbridos: Extensión NPS para Azure MFA (si es aplicable)	Equipo de operaciones IAM

A medida que revise la lista, es posible que tenga que asignar un propietario a las tareas que no tienen uno o ajustar la propiedad de aquellas tareas con propietarios que no coincidan con las recomendaciones anteriores.

Lectura recomendada para propietarios

- [Asignación de roles de administrador en Azure Active Directory](#)
- [Gobernanza en Azure](#)

Administración híbrida

Versiones recientes de componentes locales

Tener las versiones más actualizadas de los componentes locales proporciona al cliente todas las actualizaciones de seguridad más recientes, mejoras de rendimiento, así como funcionalidades que podrían ayudarle a simplificar aún más el entorno. La mayoría de los componentes tienen una configuración de actualización automática, que automatiza el proceso de actualización.

Estos componentes incluyen:

- Azure AD Connect
- Conectores de Azure AD Application Proxy
- Agentes de autenticación de paso a través de Azure AD
- Agentes de Azure AD Connect Health

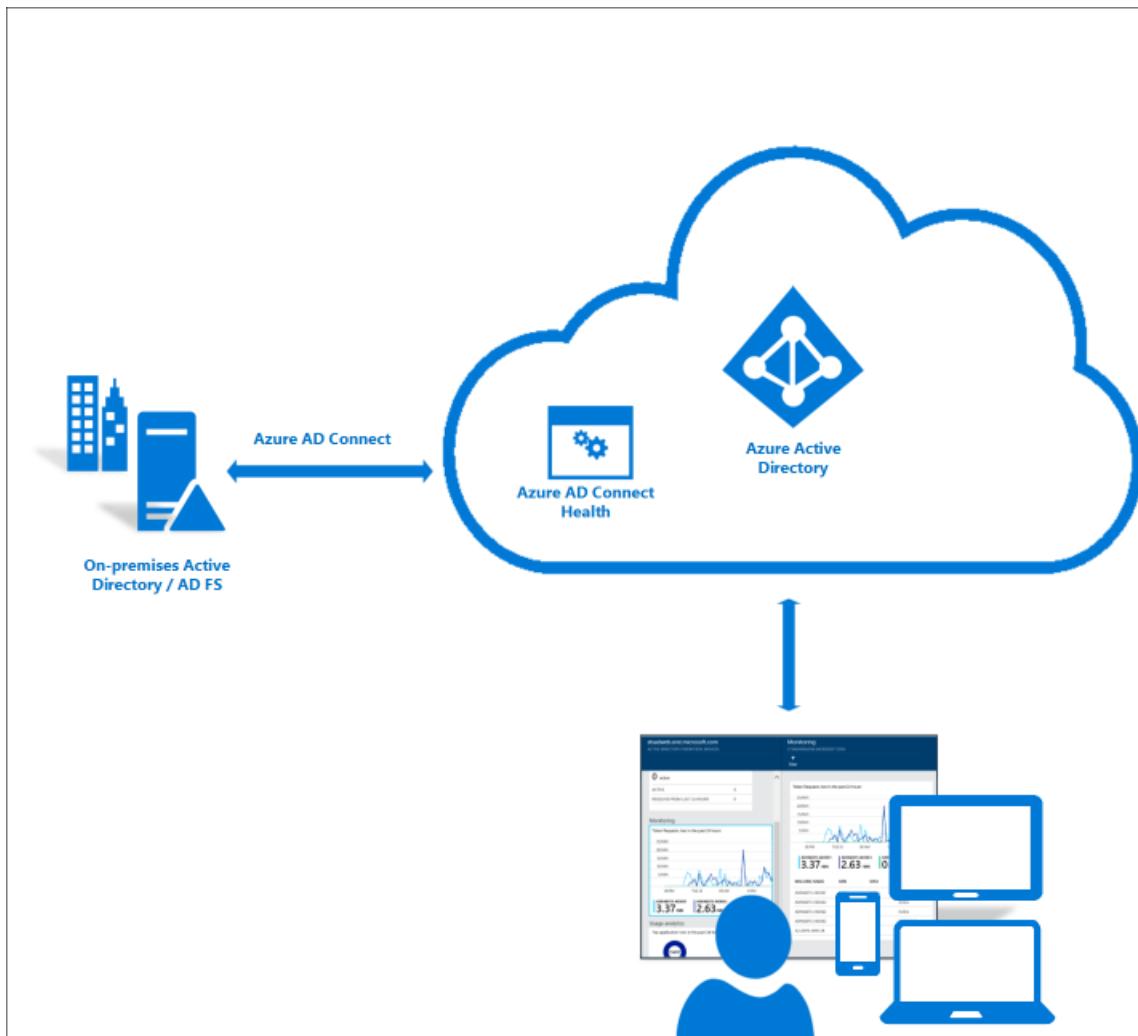
A menos que se haya establecido uno, debe definir un proceso para actualizar estos componentes y así poder basarse en la característica de actualización automática siempre que sea posible. Si encuentra componentes que tienen seis o más meses de retraso, debe realizar la actualización lo antes posible.

Lectura recomendada de administración híbrida

- [Azure AD Connect: actualización automática](#)
- [Descripción de los conectores de Azure AD Application Proxy | Actualizaciones automáticas](#)

Línea de base de las alertas de Azure AD Connect Health

Las organizaciones deben implementar [Azure AD Connect Health](#) para la supervisión y la generación de informes de Azure AD Connect y AD FS. Azure AD Connect y AD FS son componentes esenciales que pueden afectar a la administración y la autenticación del ciclo de vida y, por ello, provocar interrupciones. Azure AD Connect Health ayuda a supervisar y a conocer mejor su infraestructura de identidad local, lo que garantiza la confiabilidad de este entorno.



A medida que supervisa el estado de su entorno, debe hacerse cargo inmediatamente cualquier alerta de gravedad alta, además de las alertas de gravedad inferior.

Lectura recomendada de Azure AD Connect Health

- [Instalación del agente de Azure AD Connect Health](#)

Registros de los agentes locales

Algunos servicios de administración de identidades y acceso requieren agentes locales para habilitar escenarios híbridos. Algunos ejemplos son el restablecimiento de contraseña, la autenticación de paso a través (PTA), Azure AD Application Proxy y la extensión NPS de Azure MFA. Es fundamental que el equipo de operaciones establezca la línea de base y supervise el estado de estos componentes archivando y analizando los registros del agente de componentes, gracias a soluciones como System Center Operations Manager o SIEM. Es igualmente importante que el equipo de operaciones de INFOSEC o el Departamento de soporte técnico sepan cómo solucionar problemas de patrones de errores.

Lectura recomendada de registros de agentes locales

- [Solucionar problemas de Proxy de aplicación](#)
- [Solución de problemas del autoservicio de restablecimiento de contraseña: Azure Active Directory](#)
- [Descripción de los conectores del Proxy de aplicación de Azure AD](#)
- [Azure AD Connect: Solución de problemas de autenticación de paso a través](#)
- [Solución de problemas de códigos de error para la extensión de NPS de Azure MFA](#)

Administración de los agentes locales

La adopción de procedimientos recomendados puede ayudarle a optimizar el funcionamiento de los agentes locales. Puede usar los siguientes procedimientos recomendados:

- Se recomiendan varios conectores de Azure AD Application Proxy por grupo de conectores, para proporcionar

un equilibrio de carga continuo y una alta disponibilidad evitando puntos únicos de error al obtener acceso a las aplicaciones proxy. Si actualmente solo tiene un conector en un grupo de conectores que controla las aplicaciones en producción, debe implementar al menos dos conectores para la redundancia.

- Crear y usar un grupo de conectores del proxy de aplicación para la depuración puede serle de utilidad en escenarios de solución de problemas y para incorporar nuevas aplicaciones locales. También es recomendable instalar herramientas de red como el Analizador de mensajes y Fiddler en los equipos de conector.
- Asimismo, se recomiendan varios agentes de autenticación de paso a través para proporcionar un equilibrio de carga sin problemas y una alta disponibilidad, ya que así podrá evitar un único punto de error durante el flujo de autenticación. Asegúrese de implementar al menos dos agentes de autenticación de paso a través en la redundancia.

Lectura recomendada para la administración de agentes locales

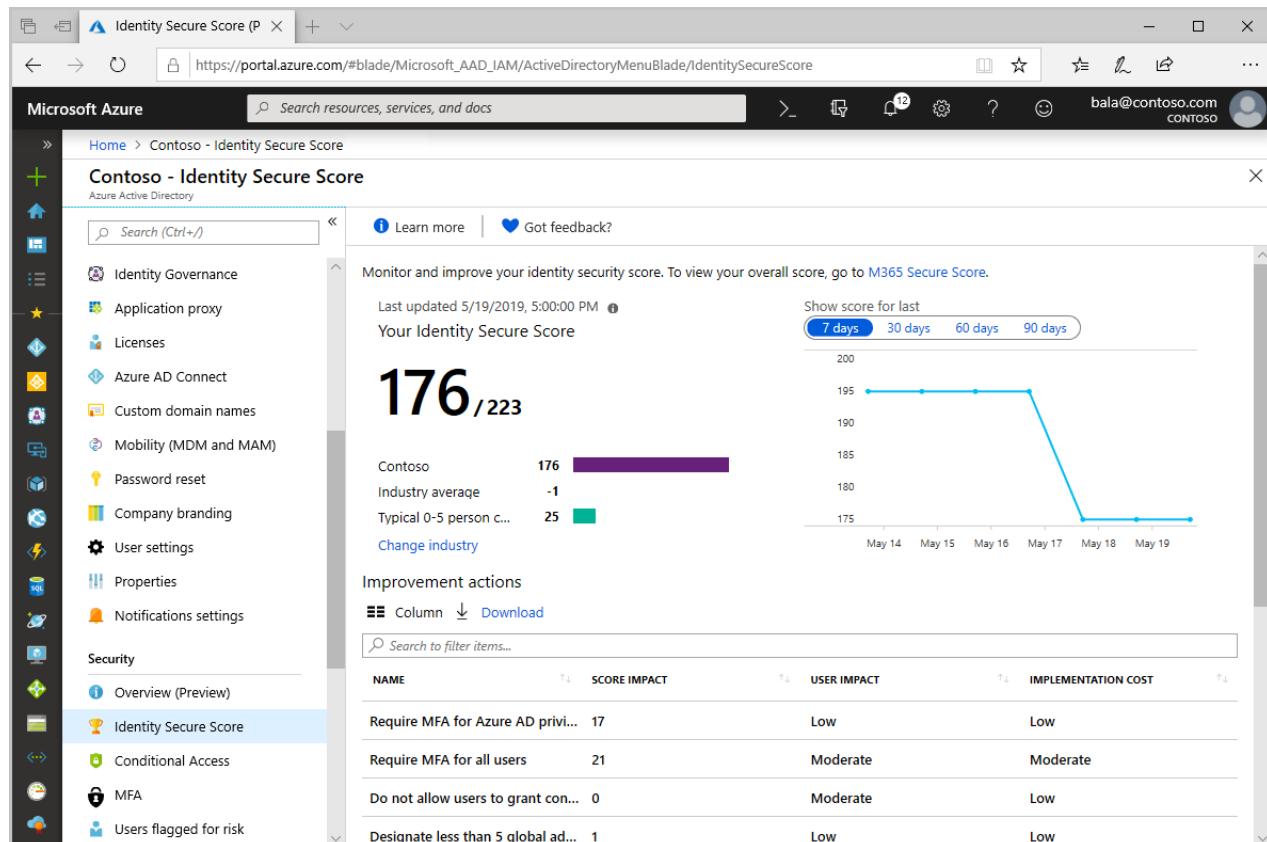
- [Descripción de los conectores del Proxy de aplicación de Azure AD](#)
- [Autenticación de paso a través de Azure AD: inicio rápido](#)

Administración a escala

Puntuación segura de identidad

La [puntuación de seguridad de la identidad](#) proporciona una medida cuantificable de la posición de seguridad de su organización. Es fundamental revisar y abordar constantemente los hallazgos de los que tenga información, y procurar tener la máxima puntuación posible. La puntuación le ayuda a:

- Medir de forma objetiva su nivel de seguridad de la identidad
- Planear la realización de mejoras en la seguridad de la identidad
- Ver si las mejoras han logrado sus objetivos



Si su organización no tiene ningún programa para supervisar los cambios en la puntuación de seguridad de la identidad, le recomendamos que implemente un plan y asigne propietarios para supervisar y controlar las acciones de mejora. Recuerde que las organizaciones deben corregir las acciones de mejora con un impacto de puntuación superior a 30 lo antes posible.

Notificaciones

Microsoft envía estas notificaciones por correo electrónico a los administradores, para informarles de los distintos cambios en el servicio, las actualizaciones de configuración necesarias y los errores que requieren la intervención del administrador. Es importante que los clientes escriban sus direcciones de correo electrónico de notificación, para que los mensajes se envíen a los miembros del equipo adecuados y que así puedan confirmar todas las notificaciones y actuar en consecuencia. Le recomendamos agregar varios destinatarios al [Centro de mensajes de Office 365](#) y solicitar que las notificaciones (incluidas las notificaciones de Azure AD Connect Health) se envíen a una lista de distribución o a un buzón compartido. Si solo tiene una cuenta de administrador global con una dirección de correo electrónico, asegúrese de configurar al menos dos cuentas compatibles con ese correo electrónico.

Existen dos direcciones de "remitente" que usa Azure AD: o365mc@email2.microsoft.com, que envía notificaciones del Centro de mensajes de Office 365 y azure-noreply@microsoft.com, que envía notificaciones relacionadas con lo siguiente:

- [Revisiones de acceso de Azure AD](#)
- [Azure AD Connect Health](#)
- [Azure AD Identity Protection](#)
- [Azure AD Privileged Identity Management](#)
- [Notificaciones de certificado que expirarán con una aplicación empresarial](#)
- Aplicación empresarial: aprovisionamiento de las notificaciones de servicio

Consulte la tabla siguiente para obtener información sobre el tipo de notificaciones que se envían y dónde buscarlas:

ORIGEN DE LA NOTIFICACIÓN	QUÉ SE ENVÍA	DÓNDE BUSCAR
Contacto técnico	Errores de sincronización	Azure Portal: hoja de propiedades
Centro de mensajes de Office 365	Avisos de incidentes y degradación de servicios de identidad y servicios backend de O365	Portal de Office
Resumen semanal de Identity Protection	Resumen de Identity Protection	Hoja de Azure AD Identity Protection
Azure AD Connect Health	Notificaciones de alerta	Azure Portal: hoja de Azure AD Connect Health
Notificaciones de aplicaciones empresariales	Notificaciones acerca de cuándo expirarán los certificados y aprovisionamiento de errores	Azure Portal: hoja de aplicaciones empresariales (cada aplicación tiene su propia configuración de dirección de correo electrónico)

Lectura recomendada de notificaciones

- [Cambio la dirección de la organización, el contacto técnico y más - Office 365](#)

Área expuesta operativa

Bloqueo de AD FS

Las organizaciones que configuran aplicaciones para que se autentiquen directamente en Azure AD se benefician del [bloqueo inteligente de Azure AD](#). Si usa AD FS en Windows Server 2012 R2, implemente la [protección de bloqueo de extranet](#) de AD FS. Si usa AD FS en Windows Server 2016 o posterior, implemente el [bloqueo inteligente de extranet](#). Como mínimo, se recomienda que habilite el bloqueo de la extranet para poder contener el

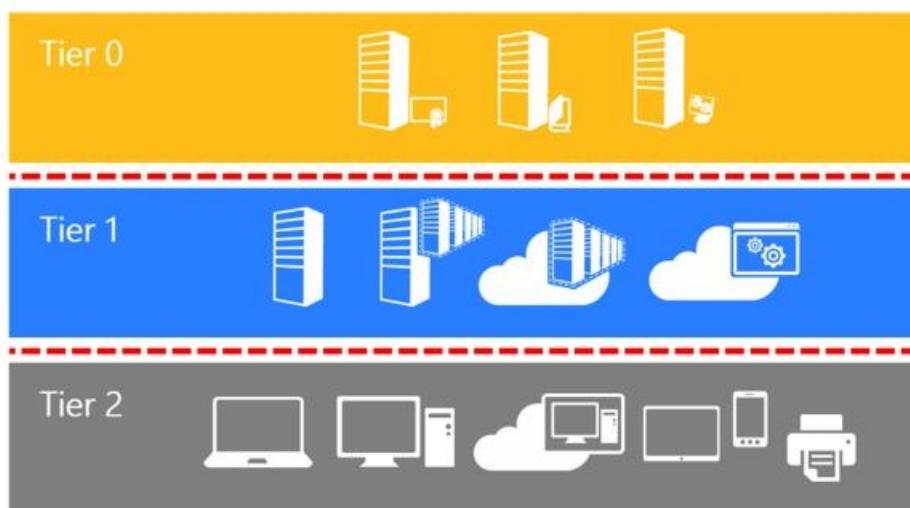
riesgo de ataques por fuerza bruta contra la instancia local de Active Directory. Sin embargo, si tiene AD FS en Windows 2016 o superior, también debe habilitar el bloqueo inteligente de la extranet que le ayudará a mitigar los ataques de [difusión de contraseñas](#).

Si AD FS solo se usa para la federación de Azure AD, hay algunos puntos de conexión que se pueden desactivar para minimizar el área expuesta a ataques. Por ejemplo, si AD FS solo se usa para Azure AD, debe deshabilitar los distintos puntos de conexión de WS-Trust de aquellos puntos de conexión habilitados para los elementos `usernamemixed` y `windowstransport`.

Acceso a equipos con componentes de identidad locales

Las organizaciones deben bloquear el acceso a las máquinas con componentes híbridos locales de la misma manera que el dominio local. Por ejemplo, un operador de copia de seguridad o un administrador de Hyper-V no debe poder iniciar sesión en el servidor de Azure AD Connect para cambiar las reglas.

Este modelo de niveles administrativo de Active Directory se diseñó para proteger los sistemas de identidad mediante un conjunto de zonas de búfer que se encuentran entre el control total del entorno (nivel 0) y los recursos de la estación de trabajo de alto riesgo que los atacantes suelen poner en peligro.



El [modelo de niveles](#) se compone de tres niveles y solo incluye las cuentas administrativas, no las cuentas de usuario estándar.

- **Nivel 0** : control directo de las identidades de empresa en el entorno. El nivel 0 incluye cuentas, grupos y otros recursos que tienen control administrativo directo o indirecto de los bosques, dominios o controladores de dominio de Active Directory y todos los recursos que haya en él. La sensibilidad de la seguridad de todos los recursos de nivel 0 es equivalente, ya que todos se controlan de forma efectiva entre sí.
- **Nivel 1** : control de aplicaciones y servidores empresariales. Los recursos de nivel 1 incluyen sistemas operativos de servidor, servicios en la nube y aplicaciones empresariales. Las cuentas de administrador de nivel 1 tienen el control administrativo de una cantidad considerable de valor empresarial que se hospeda en estos recursos. Una función común de ejemplo son los administradores de servidores que mantienen estos sistemas operativos con la capacidad de afectar a todos los servicios de empresa.
- **Nivel 2** : control de los dispositivos y estaciones de trabajo de usuarios. Las cuentas de administrador de nivel 2 tienen el control administrativo de una cantidad considerable de valor empresarial que se hospeda en dispositivos y estaciones de trabajo de usuarios. Algunos ejemplos son el departamento de soporte técnico y los administradores de soporte técnico del equipo, porque pueden afectar a la integridad de casi cualquier dato de usuario.

Bloquee el acceso a componentes de identidad locales tales como Azure AD Connect, AD FS y servicios de SQL, de la misma manera que lo hace en los controladores de dominio.

Resumen

Una infraestructura de identidad segura está conformada por siete aspectos. Esta lista le ayudará a encontrar las acciones que debe realizar para optimizar las operaciones de Azure Active Directory (Azure AD).

- Asignar propietarios a las tareas principales.
- Automatice el proceso de actualización de los componentes híbridos locales.
- Implemente Azure AD Connect Health para supervisar y generar informes de Azure AD Connect y AD FS.
- Supervise el estado de los componentes híbridos locales archivando y analizando los registros del agente de componentes mediante System Center Operations Manager o una solución SIEM.
- Implemente mejoras de seguridad midiendo su posición de seguridad mediante la puntuación segura de identidad.
- Bloquee AD FS.
- Bloquee el acceso a equipos con componentes de identidad locales

Pasos siguientes

Consulte los [planes de implementación de Azure AD](#) para obtener detalles de la implementación de cualquier funcionalidad que no haya implementado.

Suscripción de la organización para usar Azure Active Directory

22/07/2020 • 2 minutes to read • [Edit Online](#)

Suscriba para Azure Active Directory (Azure AD) o una suscripción nueva de Microsoft Azure mediante una de las siguientes opciones:

- **Cuenta Microsoft.** Use su cuenta Microsoft personal para obtener acceso a todos los productos y servicios en la nube de Microsoft orientados al cliente, como Outlook (Hotmail), Messenger, OneDrive, MSN, Xbox LIVE u Office 365. El registro en un buzón de Outlook.com crea automáticamente una cuenta Microsoft con una dirección @Outlook.com. Para más información, consulte [Introducción a las cuentas Microsoft](#).
- **Cuenta profesional o educativa.** Use su cuenta profesional o educativa para obtener acceso a todos los servicios en la nube pequeños, medios y de empresa de Microsoft, como Azure, Microsoft Intune u Office 365. Tras registrarse en uno de estos servicios como organización, Azure AD aprovisionará automáticamente un directorio basado en la nube para representar a su organización. Para más información, consulte [Administración del directorio de Azure AD](#).

NOTE

Se recomienda usar la cuenta profesional o educativa si ya tiene acceso a Azure AD. Sin embargo, debe utilizar el tipo de cuenta que esté asociada a su suscripción de Azure.

Pasos siguientes

- [Instrucciones para comprar Azure](#)
- [Suscripción a las ediciones de Azure Active Directory Premium](#)
- [Más información acerca de Azure AD](#)
- [Uso de la infraestructura de identidad local en la nube](#)
- [Visitar el blog de Microsoft Azure](#)

Suscripción a las ediciones Azure Active Directory Premium

22/07/2020 • 7 minutes to read • [Edit Online](#)

Puede adquirir ediciones Azure Active Directory (Azure AD) Premium y asociarlas a su suscripción de Azure. Si necesita crear una suscripción de Azure, debe activar también el plan de licencias y el acceso al servicio de Azure AD.

NOTE

Las ediciones Azure AD Premium y Basic están disponibles para los clientes de China que utilizan la instancia de Azure Active Directory en todo el mundo. Las ediciones Azure AD Premium y Basic no se admiten actualmente en el servicio de Azure administrado por 21Vianet en China. Para más información, póngase en contacto con nosotros en el [foro de Azure Active Directory](#).

Antes de suscribirse a Active Directory Premium 1 o Premium 2, primero debe determinar qué suscripción o plan existente se va a usar:

- Mediante su suscripción de Azure u Office 365 existente
- Mediante su plan de licencias de Enterprise Mobility + Security
- Mediante un plan de licencias por volumen de Microsoft

El registro con su suscripción de Azure con licencias de Azure AD activadas y adquiridas previamente activa automáticamente las licencias en el mismo directorio. Si no es así, aún debe activar el plan de licencias y el acceso a Azure AD. Para más información sobre la activación del plan de licencias, vea [Activación del plan de licencias](#).

Para más información sobre la activación del acceso de Azure AD, vea [Activación de acceso de Azure Active Directory](#).

Registro mediante la suscripción existente de Azure u Office 365

Si ya cuenta con una suscripción a Azure u Office 365, puede comprar las ediciones en línea de Azure Active Directory Premium. Para obtener pasos detallados, consulte [Cómo comprar Azure Active Directory Premium: nuevos clientes](#).

Registro mediante su plan de licencias de Enterprise Mobility + Security

Enterprise Mobility + Security es un conjunto compuesto por Azure AD Premium, Azure Information Protection y Microsoft Intune. Si ya tiene una licencia de EMS, puede empezar a trabajar con Azure AD mediante una de estas opciones de licencias:

Para más información sobre EMS, vea el [sitio web de Enterprise Mobility + Security](#).

- Pruebe EMS con una [suscripción de prueba de Enterprise Mobility + Security E5](#)
- Adquiera [licencias E5 de Enterprise Mobility + Security](#)
- Adquiera [licencias E3 de Enterprise Mobility + Security](#)

Registro mediante su plan de licencias por volumen de Microsoft

Con su plan de licencias por volumen de Microsoft, puede suscribirse a Azure AD Premium con uno de estos dos programas, en función del número de licencias que desea obtener:

- Para 250 o más licencias. [Contrato Enterprise \(EA\) de Microsoft](#)
- Para 5 a 250 licencias. [Licencia por volumen Open](#)

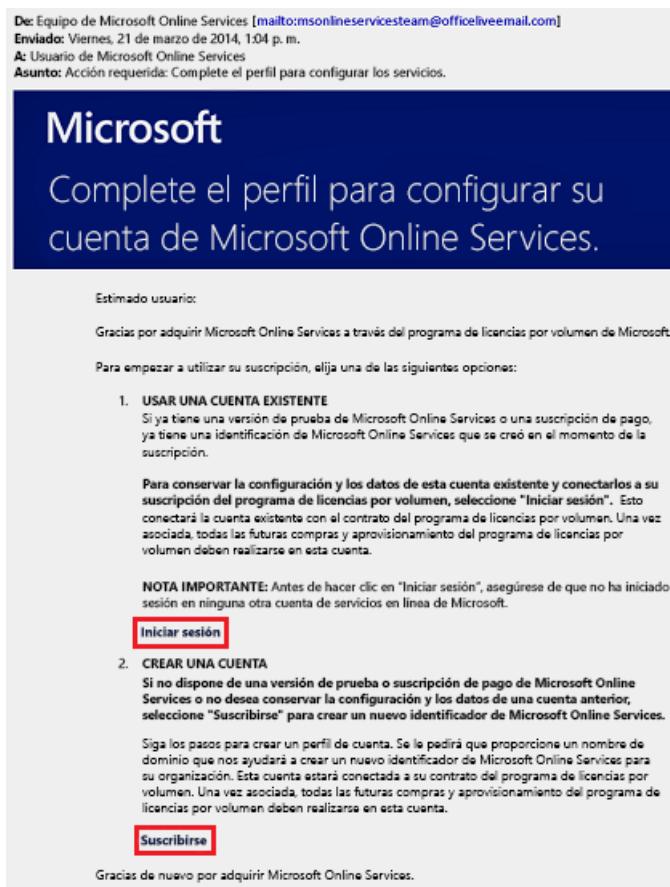
Para más información sobre las opciones de compra de licencias por volumen, vea [Cómo comprar mediante el programa de licencias por volumen](#).

Activación del nuevo plan de licencias

Si ha iniciado sesión con el nuevo plan de licencias de Azure AD, debe activarlo para su organización, con el uso del correo electrónico de confirmación enviado después de la compra.

Para activar el plan de licencias

- Abra el correo electrónico de confirmación recibido de Microsoft después de suscribirse y luego haga clic en **Iniciar sesión** o **Registrarse**.



- **Iniciar sesión.** Seleccione este vínculo si tiene un inquilino existente y luego inicia sesión con la cuenta de administrador existente. Debe ser administrador global en el inquilino en el que se activan las licencias.
- **Registrarse.** Seleccione este vínculo si desea abrir la página **Crear perfil de cuenta** y cree un inquilino de Azure AD para el plan de licencias.

Crear perfil de cuenta

Si su empresa ya está utilizando Microsoft Online Services para servicios como Microsoft Office 365, le recomendamos que utilice el mismo id. de usuario para suscribirse en Windows Intune. [Más información](#) sobre por qué es importante suscribirse con el mismo identificador de usuario. [Iniciar sesión](#)

* Obligatorio

* País o región: Estados Unidos
No se puede cambiar después de la suscripción. ¿Por qué?

* Idioma de la organización: Inglés

* Nombre: myfirstname

* Apellidos: myfirstname

* Nombre de la organización: domoorg4

* Dirección 1: one microsoft way

Dirección 2:

* Ciudad: redmond

* Estado: Washington

* Código postal: 98052

* Número de teléfono: 4252222222

* Dirección de correo electrónico: amyrotest@live.com

Comience a usar su solución de servicio en línea

Empiece ahora mismo siguiendo estos sencillos pasos:

- Complete su perfil de cliente
- Seleccione un nombre de dominio único
- Cree su nuevo id. de usuario, lo utilizará para iniciar sesión en el servicio
- Cree una nueva contraseña
- Como opción, puede seleccionar entre las opciones de contacto donde Microsoft puede proporcionarle información y ofertas
- Tras enviar el formulario, se enviará un correo electrónico de confirmación a la dirección de correo electrónico que nos ha proporcionado

Cuando haya terminado, verá un cuadro de confirmación de agradecimiento por activar el plan de licencias del inquilino.



Activación del acceso a Azure AD

Si va a agregar nuevas licencias de Azure AD Premium a una suscripción existente, ya se debe haber activado el acceso a Azure AD. En caso contrario, debe activar el acceso a Azure AD después de recibir el **mensaje de correo electrónico de bienvenida**.

Una vez aprovisionadas las licencias adquiridas en el directorio, recibirá un **correo electrónico de bienvenida**. El correo electrónico confirma que puede empezar a administrar las licencias y características de Azure AD Premium o Enterprise Mobility + Security.

TIP

No podrá acceder a Azure AD en el nuevo inquilino hasta que active el acceso al directorio de Azure AD desde el correo electrónico de bienvenida.

Para activar el acceso a Azure AD

1. Abra el **correo electrónico de bienvenida** y luego haga clic en **Iniciar sesión**.

De: Equipo de Microsoft Online Services [mailto:msonlineservicesteam@officeliveemail.com]
Enviado: Martes, 25 de marzo, 2014 10:07 a. m.
Para: Usuario de Microsoft Azure Active Directory
Subject: Get started with your Windows Azure Active Directory Premium!



COMIENCE HOY MISMO.

Organización: AAD.Premium

Inicie sesión para empezar.

Iniciar sesión
<http://go.microsoft.com/fwlink/?LinkId=393623>

Id. de usuario ([¿Qué es esto?](#))

Nombre: AAD.Premium

Id. de usuario: lornagarner@aadpremium.csclp.net

Su organización ahora tiene acceso a Windows Azure Active Directory Premium, el servicio de administración de acceso e identidad en nube de Microsoft. Inicie sesión con su identificador de usuario y comience a crear un directorio y una administración de acceso en la nube, configure un inicio de sesión perfecto para los recursos de la nube y mejore la seguridad de acceso a las aplicaciones.

Gracias por elegir Windows Azure Active Directory Premium a través del programa de licencias por volumen de Microsoft. Esperamos poder ayudar a su organización a obtener el máximo valor de su suscripción.

Atentamente,

- Después de iniciar sesión correctamente, se le remitirá a una verificación en dos pasos mediante un dispositivo móvil.

A screenshot of the Microsoft Azure subscription sign-up process. It shows two steps: Step 1, "Acera de usted" (About you), where personal information like name and email is entered. Step 2, "Confirmación por móvil" (Mobile verification), where a phone number and verification code are provided. The user's email address "lornagarner@aadpremium.csclp.net" is visible at the top right.

El proceso de activación normalmente tarda solo unos minutos y después puede usar el inquilino de Azure AD.

Pasos siguientes

Ahora que tiene Azure AD Premium, puede [personalizar su dominio](#), agregar su [personalización de marca corporativa](#), [crear un inquilino](#) y [agregar grupos y usuarios](#).

Incorporación del nombre de dominio personalizado mediante el portal de Azure Active Directory

22/07/2020 • 9 minutes to read • [Edit Online](#)

Cada inquilino de Azure AD nuevo incluye un nombre de dominio inicial, <domainname>.onmicrosoft.com. No se puede cambiar o eliminar el nombre de dominio inicial, pero puede agregar nombres de la organización. La incorporación de nombres de dominio personalizados le ayuda a crear nombres de usuario que resultan familiares a los usuarios, como *alain@contoso.com*.

Antes de empezar

Para poder agregar un nombre de dominio personalizado, cree el nombre de dominio con un registrador de dominios. Para un registrador de dominios acreditado, consulte [ICANN: Registradores acreditados](#).

Creación del directorio en Azure AD

Después de obtener el nombre de dominio, puede crear su primer directorio de Azure AD. Inicie sesión en Azure Portal para su directorio con una cuenta que tenga el rol **Propietario** de la suscripción.

Cree el nuevo directorio siguiendo los pasos descritos en [Creación de un nuevo inquilino para la organización](#).

IMPORTANT

La persona que crea el inquilino es automáticamente el administrador global de ese inquilino. El administrador global puede agregar administradores adicionales al inquilino.

Para más información sobre los roles de suscripción, consulte [Roles de Azure](#).

TIP

Si tiene previsto federar la instancia local de Windows Server AD en Azure AD, tiene que seleccionar la opción **Voy a configurar este dominio para el inicio de sesión único con mi Active Directory local** cuando ejecute la herramienta Azure AD Connect para sincronizar los directorios.

También tiene que registrar el mismo nombre de dominio que seleccione para la federación con su directorio local en el paso **Dominio de Azure AD** del asistente. Para ver el aspecto de la configuración, consulte [Comprobación del dominio de Azure AD seleccionado para la federación](#). Si no tiene la herramienta Azure AD Connect, puede [descargarla aquí](#).

Adición del nombre de dominio personalizado en Azure AD

Después de crear el directorio, puede agregar el nombre de dominio personalizado.

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Busque y seleccione *Azure Active Directory* en cualquier página. Luego, seleccione **Nombres de dominio personalizado** > **Agregar dominio personalizado**.

fourcoffee - Nombres de dominio personalizados

Azure Active Directory

Información general Agregar un dominio personalizado Actualizar Solución de problemas

ADMINISTRAR

- Usuarios y grupos
- Aplicaciones empresariales
- Dispositivos
- Registros de aplicaciones
- Proxy de la aplicación
- Licencias
- Azure AD Connect
- Nombres de dominio perso...
- Movilidad (MDM v MAM)

NOMBRE	ESTADO
fourcoffee.com	⚠ Sin comprobar
fourcoffee.onmicrosoft.com	✅ Disponible

3. En **Nombre de dominio personalizado**, escriba el nombre nuevo de la organización, en este ejemplo, *contoso.com*. Seleccione **Add domain** (Agregar dominio).

Home > Fabrikam - Custom domain names > Custom domain name

Custom domain name □ X

Fabrikam

* Custom domain name ⓘ

contoso.com ✓

Add Domain

IMPORTANT

Debe incluir *.com*, *.net* o cualquier otra extensión de nivel superior para un correcto funcionamiento.

Se agrega el dominio sin comprobar. Aparece la página **contoso.com**, donde se muestra la información de DNS. Guarde esta información. La necesitará más adelante para crear un registro TXT y configurar DNS.

Home > Fabrikam - Custom domain names > contoso.com

contoso.com
Custom domain name

Delete

To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE **TXT** **MX**

ALIAS OR HOST NAME

DESTINATION OR POINTS TO ADDRESS

TTL

[Share these settings via email](#)

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

Adición de la información de DNS en el registrador de dominios

Después de agregar el nombre de dominio personalizado a Azure AD, debe volver al registrador de dominios y agregar la información de DNS de Azure AD desde el archivo TXT copiado. La creación de este registro TXT en el dominio comprueba la propiedad del nombre de dominio.

Vuelva al registrador de dominios y cree un nuevo registro TXT para el dominio, según la información de DNS copiada. Establezca el período de vida (TTL) en 3600 segundos (60 minutos) y, luego, guarde el registro.

IMPORTANT

Puede registrar tantos nombres de dominio como desee. Sin embargo, cada dominio obtiene su propio registro TXT de Azure AD. Tenga cuidado al escribir la información del archivo TXT en el registrador de dominios. Si escribe por error información incorrecta o duplicada, deberá esperar hasta que expire el TTL (60 minutos) antes de volver a intentarlo.

Comprobación del nombre de dominio personalizado

Después de registrar el nombre de dominio personalizado, asegúrese de que es válido en Azure AD. La propagación desde el registrador de dominios a Azure AD puede ser instantánea o puede tardar unos días, dependiendo del registrador de dominios.

Siga estos pasos para comprobar el nombre de dominio personalizado:

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Busque y seleccione *Azure Active Directory* en cualquier página y, luego, seleccione **Nombres de dominio personalizado**.
3. En **Nombres de dominio personalizado**, seleccione el nombre de dominio personalizado. En este ejemplo, seleccione **contoso.com**.

NAME	STATUS	FEDERATED	PRIMARY
contoso.com	⚠️ Unverified		
fabrikam.onmicrosoft.com	🟢 Available	✓	

4. En la página **contoso.com**, seleccione **Comprobar** para asegurarse de que el dominio personalizado se ha registrado correctamente y es válido para Azure AD.

To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE	TXT	MX
ALIAS OR HOST NAME	@	
DESTINATION OR POINTS TO ADDRESS	MS=ms64983159	
TTL	3600	

Share these settings via email

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.
Verify

Después de comprobar su nombre de dominio personalizado, puede eliminar el archivo TXT o MX de comprobación.

Problemas comunes de comprobación

Si Azure AD no puede comprobar un nombre de dominio personalizado, pruebe las sugerencias siguientes:

- **Espere al menos una hora y vuelva a intentarlo.** Los registros de DNS deben propagarse antes de que Azure AD compruebe el dominio. Este proceso puede tardar una hora o más.
- **Asegúrese de que el registro de DNS es correcto.** Vuelva al sitio del registrador de nombres de dominio. Asegúrese de que exista la entrada y que coincida con la información de la entrada DNS proporcionada por Azure AD.

Si no puede actualizar el registro en el sitio del registrador, comparta la entrada con alguien que tenga los

permisos para agregar la entrada y comprobar que es correcta.

- **Asegúrese de que el nombre de dominio no está en uso en otro directorio.** Un nombre de dominio solo se puede comprobar en un directorio. Si el nombre de dominio se comprueba actualmente en otro directorio, no se puede comprobar también en el directorio nuevo. Para corregir este problema de duplicación, debe eliminar el nombre de dominio en el directorio antiguo. Para más información sobre la eliminación de nombres de dominio, consulte [Administración de nombres de dominio personalizados](#).
- **Asegúrese de que no tiene ningún inquilino de Power BI no administrado.** Si los usuarios han activado Power BI a través del registro de autoservicio y han creado a un inquilino no administrado para la organización, debe asumir la administración como administrador interno o externo, mediante PowerShell. Para más información, vea [Adquisición de un directorio no administrado como administrador en Azure Active Directory](#).

Pasos siguientes

- Agregar otro administrador global al directorio. Para más información, consulte [Asignación de roles y administradores](#).
- Agregue usuarios a su dominio. Para más información, consulte [Incorporación o eliminación de usuarios](#).
- Administrar la información del nombre de dominio en Azure AD. Para más información, consulte [Administración de nombres de dominio personalizados](#).
- Si tiene versiones locales de Windows Server que desea usar junto con Azure Active Directory, consulte [Integración de los directorios locales con Azure Active Directory](#).

Incorporación de la personalización de marca en la página de inicio de sesión de Azure Active Directory de la organización

22/07/2020 • 15 minutes to read • [Edit Online](#)

Use el logotipo de la organización y combinaciones de colores personalizadas para proporcionar un aspecto coherente en las páginas de inicio de sesión de Azure Active Directory (Azure AD). Las páginas de inicio de sesión aparecen cuando los usuarios inician sesión en las aplicaciones web de su organización, como Office 365, que usan Azure AD como proveedor de identidades.

NOTE

Para agregar personalización de marca, es necesario usar las ediciones de Azure Active Directory Premium 1, Premium 2 o Basic, o bien tener una licencia de Office 365. Para obtener más información acerca de las ediciones y licencias, consulte [Suscripción a Azure AD Premium](#).

Las ediciones Azure AD Premium y Basic están disponibles para los clientes de China que utilizan la instancia de Azure Active Directory en todo el mundo. Las ediciones Azure AD Premium y Basic no se admiten actualmente en el servicio de Azure administrado por 21Vianet en China. Para más información, póngase en contacto con nosotros en el [foro de Azure Active Directory](#).

Personalización de la página de inicio de sesión de Azure AD

Puede personalizar las páginas de inicio de sesión de Azure AD. Estas páginas aparecen cuando los usuarios inician sesión en aplicaciones específicas del inquilino de la organización, como <https://outlook.com/contoso.com>, o al pasar una variable de dominio, como <https://passwordreset.microsoftonline.com/?whr=contoso.com>.

La personalización de marca no aparecerá inmediatamente cuando los usuarios tengan acceso a sitios como www.office.com. En su lugar, el usuario tiene que iniciar sesión para que aparezca la personalización de marca. Una vez que el usuario ha iniciado sesión, la personalización de marca puede tardar 15 minutos o más en aparecer.

NOTE

Todos los elementos de personalización de marca son opcionales. Por ejemplo, si especifica un logotipo del banner sin ninguna imagen de fondo, se mostrará en la página de inicio de sesión su logotipo con una imagen de fondo predeterminada del sitio de destino (por ejemplo, Office 365).

Además, la personalización de marca de la página de inicio de sesión no se incluye en las cuentas Microsoft personales. Si los usuarios o los invitados de la empresa inician sesión con una cuenta Microsoft personal, la página de inicio de sesión no reflejará la personalización de marca de la organización.

Para personalizar su marca

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, después, seleccione **Personalización de marca de empresa** y, a continuación, seleccione **Configurar**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a dark sidebar with various service icons and links like 'Create a resource', 'All services', 'Dashboard', etc. The main area has a breadcrumb navigation path: Home > Contoso - Company branding > Configure company branding. The title bar says 'Contoso - Company branding' and 'Azure Active Directory'. A search bar at the top says 'Search resources, services, and docs'. On the right, there's a 'Configure' button with a blue icon, which is highlighted with a red box. Below it, a status message says 'STATUS: Not configured' with an info icon. A descriptive text box says 'Configure the text and graphics your users see when they sign in to Azure Active Directory.' A sidebar on the left lists several management options under 'Manage': Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, and Company branding. The 'Company branding' option is highlighted with a light blue box.

3. En la página **Configurar personalización de marca de empresa**, proporcione parte o la totalidad de la siguiente información.

IMPORTANT

Todas las imágenes personalizadas que agregue en esta página tienen restricciones de tamaño de imagen (píxeles) y del posible tamaño de archivo (KB). Debido a estas restricciones, lo más probable es que necesite usar un editor de fotografía para crear imágenes con el tamaño adecuado.

- **Configuración general**

Configure company branding

Contoso

Language i

Default



Sign-in page background image

Image size: 1920x1080px

File size: <300KB

File type: PNG or JPG i[Remove](#)[Select a file](#)**Microsoft**[Remove](#)[Select a file](#)

Banner logo

Image size: 280x60px

File size: 10KB

File type: Transparent PNG or JPG iUsername hint i[Forgot your username?](#)Sign-in page text iIf you need help, contact the Help Desk online ✓
at www.contoso.com/helpdesk.

- **Idioma.** El idioma se establece automáticamente como valor predeterminado y no se puede cambiar.
- **Imagen de fondo de la página de inicio de sesión.** Seleccione un archivo de imagen .png o .jpg para que aparezca como fondo de las páginas de inicio de sesión. La imagen se anclará al centro del explorador y se escalará según el tamaño del espacio visible. No se puede seleccionar una imagen de más de 1920 x 1080 píxeles de tamaño o con un tamaño de archivo superior a los 300 KB.

Se recomienda usar imágenes sin enfoque en un sujeto definido; por ejemplo, aparece un cuadro blanco opaco en el centro de la pantalla y puede cubrir cualquier parte de la imagen según las dimensiones del espacio visible.

- **Logotipo del banner.** Seleccione una versión .png o .jpg del logotipo para que aparezca en la página de inicio de sesión después de que el usuario escriba un nombre de usuario y en la página del portal **Mis aplicaciones**.

La imagen no puede tener más de 60 píxeles de alto ni más de 280 píxeles de ancho. Se recomienda usar una imagen transparente, ya que el fondo podría no coincidir con el fondo del logotipo. También se recomienda no agregar relleno alrededor de la imagen, ya que podría reducir la apariencia del logotipo.

- **Sugerencia de nombre de usuario.** Escriba el texto de sugerencia que se muestra a los usuarios en caso de que olviden su nombre de usuario. Este texto debe ser Unicode, sin código ni vínculos y no puede superar los 64 caracteres. Si un invitado inicia sesión en la aplicación, se recomienda no agregar esta sugerencia.

- **Texto y formato de la página de inicio de sesión.** Escriba el texto que aparece en la parte inferior de la página de inicio de sesión. Puede usar este texto para comunicar información adicional, como el número de teléfono de su departamento de soporte técnico o una declaración legal. Este texto debe ser Unicode y no superar los 1024 caracteres.

Puede personalizar el texto de la página de inicio de sesión que ingresó. Para comenzar un párrafo nuevo, use la tecla Intro dos veces. También puede cambiar el formato del texto para incluir negrita, cursiva, un subrayado o un enlace en el que se pueda hacer clic. Use la siguiente sintaxis para agregar formato al texto:

Hipervínculo: [text](link)

Negrita: **text** o __text__

Cursiva: *text* o _text_

Subrayado: ++text++

• Configuración avanzada

Advanced settings

Sign-in page background color ⓘ #FFFFFF ✓

Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG ⓘ




Remove Select a file

Square logo image, dark theme
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG ⓘ




Remove Select a file

Show option to remain signed in ⓘ Yes No

- **Color de fondo de la página de inicio de sesión.** Especifique el color hexadecimal (por ejemplo, el blanco es #FFFFFF) que aparecerá en lugar de la imagen de fondo en situaciones de conexión de ancho de banda bajo. Se recomienda usar el color principal del logotipo del banner o el color de la organización.
- **Imagen de logotipo cuadrado.** Seleccione una imagen .png (formato preferido) o .jpg del logotipo de la organización para mostrársela a los usuarios durante el proceso de configuración de los nuevos dispositivos Windows 10 Enterprise. Esta imagen se utiliza únicamente para la autenticación de Windows y aparece solo en inquilinos que usan [Windows Autopilot](#) para la implementación o para páginas de entrada de contraseñas en otras experiencias de Windows 10. En algunos casos también pueden aparecer en el cuadro de diálogo de consentimiento.

La imagen no puede tener más de 240 x 240 píxeles de tamaño y el tamaño de archivo debe ser inferior a 10 KB. Se recomienda usar una imagen transparente, ya que el fondo podría no coincidir con el fondo del logotipo. También se recomienda no agregar relleno alrededor de la

imagen, ya que podría reducir la apariencia del logotipo.

- **Logotipo cuadrado, tema oscuro.** Igual que la imagen de logotipo cuadrado anterior. Esta imagen de logotipo ocupa el lugar de la imagen de logotipo cuadrado cuando se usa con un fondo oscuro, como con las pantallas unidas a Azure AD de Windows 10 en la configuración rápida (OOBE). Si el logotipo se ve bien en un fondo blanco, azul oscuro o negro, no es necesario agregar esta imagen.
- **Visualización de la opción para seguir conectado.** Puede optar por permitir que los usuarios permanezcan con la sesión iniciada en Azure AD hasta que cierren sesión explícitamente. Si elige **No**, esta opción se oculta y los usuarios deberán iniciar sesión cada vez que el explorador se cierre y se vuelva a abrir.

Para más información sobre la configuración y la solución de problemas de la opción para mantener la sesión iniciada, consulte [Configurar el símbolo del sistema "¿Mantener la sesión iniciada?" para cuentas de Azure AD](#)

NOTE

Algunas características de SharePoint Online y Office 2010 dependen de que los usuarios puedan elegir seguir conectados. Si establece esta opción en **No**, puede que los usuarios reciban solicitudes adicionales e inesperadas de inicio de sesión.

4. Una vez haya terminado de agregar la personalización de marca, seleccione **Guardar**.

Si este proceso supone la creación de la primera configuración de personalización de marca personalizada, se convertirá en el valor predeterminado del inquilino. Si tiene configuraciones adicionales, podrá elegir la configuración predeterminada.

IMPORTANT

Para agregar más configuraciones de personalización de marca corporativa al inquilino, debe elegir **Nuevo idioma** en la página **Contoso: personalización de marca de empresa**. Se abrirá la página **Configurar personalización de marca de empresa**, donde puede seguir los pasos anteriores.

Actualización de la personalización de marca personalizada

Después de crear la personalización de marca personalizada, puede volver atrás y cambiar todo lo que quiera.

Para editar la personalización de marca personalizada

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, después, seleccione **Personalización de marca de empresa** y, a continuación, seleccione **Configurar**.

The screenshot shows the Azure portal interface with the 'Company branding' section selected. A red box highlights the 'New language' row in a table, which contains columns for LOCALE, BACKGROUND IMAGE, BANNER LOGO, USERNAME HINT, and SIGN-IN PAGE TEXT. The 'Default' row is also visible.

3. En la página **Configurar personalización de marca de empresa**, agregue, quite o cambie información basándose en las descripciones de la sección **Personalización de la página de inicio de sesión de Azure AD** de este artículo.
4. Seleccione **Guardar**.

Puede transcurrir hasta una hora para que los cambios efectuados se muestren en la personalización de marca de la página de inicio de sesión.

Incorporación de personalización de marca de empresa específica de un idioma a su directorio

No se puede cambiar el idioma de la configuración original del idioma predeterminado. Sin embargo, si necesita una configuración en otro idioma, puede crear una configuración nueva.

Para agregar una configuración de personalización de marca específica del idioma

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, después, seleccione **Personalización de marca de empresa** y, a continuación, seleccione **Nuevo idioma**.

The screenshot shows the 'Configure company branding' page with the '+ New language' button highlighted by a red box. The rest of the interface is similar to the previous screenshot, showing the table with the 'Default' row.

3. En la página **Configurar personalización de marca de empresa**, seleccione el idioma (por ejemplo, francés) y, a continuación, agregue la información traducida en función de las descripciones que aparecen en la sección **Personalización de la página de inicio de sesión de Azure AD** de este artículo.
4. Seleccione **Guardar**.

La página Contoso: personalización de marca de empresa se actualiza para mostrar la nueva configuración en francés.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, All services, Favorites, Dashboard, Resource groups, App Services, Function Apps, SQL databases, Virtual machines, Azure Active Directory, Security Center, Cost Management + Billing, and Help + support. The main area is titled 'Contoso - Company branding' under 'Azure Active Directory'. It has a search bar at the top. Below it, there's a table with columns: LOCALE, BACKGROUND IMAGE, BANNER LOGO, USERNAME HINT, and SIGN-IN PAGE TEXT. There are two rows: 'Default' and 'français (France)'. The 'français (France)' row is highlighted with a red box. The 'USERNAME HINT' column for this row contains the text 'Vous avez oublié votre nom ...'. The 'SIGN-IN PAGE TEXT' column also contains some French text: 'If you need help, contact the Help Desk online at www.contoso.com/helpdesk.' and 'Si vous avez besoin d'aide, contactez le service d'assistance en ligne à l'adr...'. At the bottom right of the main area, there's a note: 'Forgot your username? If you need help, contact the Help Desk online at www.contoso.com/helpdesk.' and 'Si vous avez besoin d'aide, contactez le service d'assistance en ligne à l'adr...'.

Incorporación de la personalización de marca personalizada a páginas

Agregue la personalización de marca personalizada a páginas mediante la modificación de la parte final de la dirección URL con el texto `?whr=yourdomainname`. Esta modificación funciona en varias páginas, incluidas la página de configuración de Multi-Factor Authentication (MFA), la página de configuración de autoservicio de restablecimiento de contraseña (SSPR) y la página de inicio de sesión.

Ejemplos:

Dirección URL original: <https://aka.ms/MFASetup>

Dirección URL personalizada: <https://account.activedirectory.windowsazure.com/proofup.aspx?whr=contoso.com>

Dirección URL original: <https://aka.ms/SSPR>

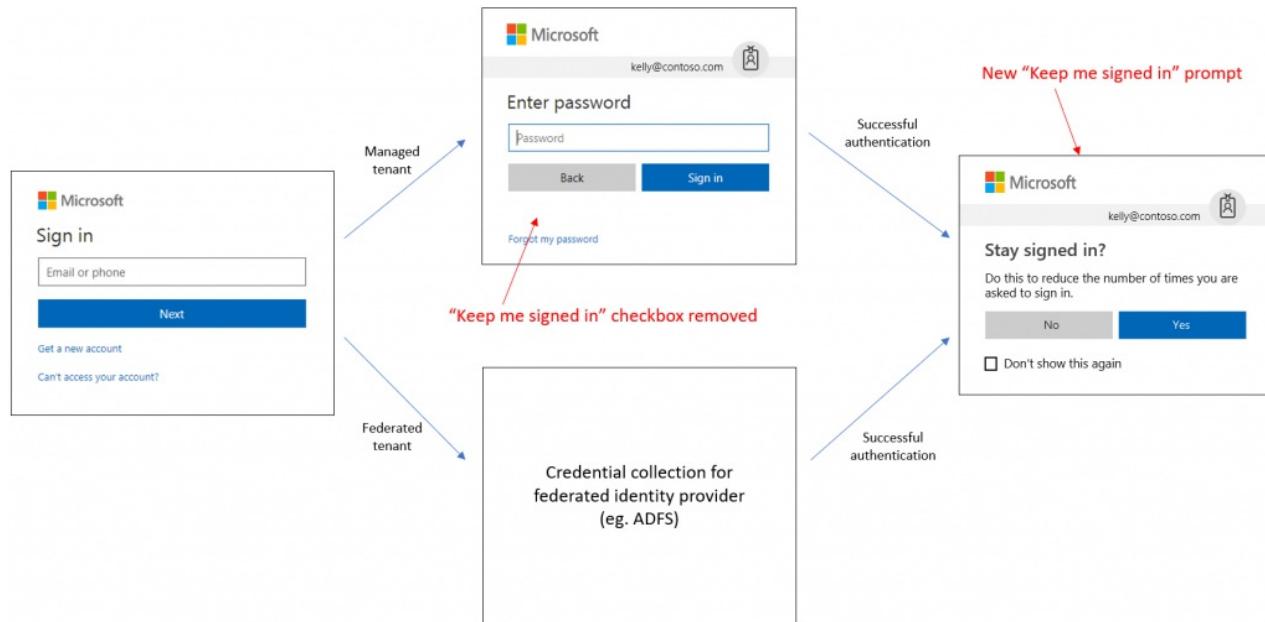
Dirección URL personalizada: <https://passwordreset.microsoftonline.com/?whr=contoso.com>

Configuración del mensaje "¿Quiere mantener la sesión iniciada?" para las cuentas de Azure AD

22/07/2020 • 6 minutes to read • [Edit Online](#)

Mantener la sesión iniciada (KMSI) muestra un mensaje **¿Quiere mantener la sesión iniciada?** después de que un usuario inicie sesión correctamente. Si un usuario responde **Sí** a este mensaje, el servicio para mantener la sesión iniciada le proporciona un [token de actualización](#) persistente. Para los inquilinos federados, el mensaje se muestra cuando el usuario se autentica correctamente en el servicio de identidad federada.

En el siguiente diagrama se muestra el flujo de inicio de sesión del usuario para un inquilino administrado y un inquilino federado, así como el nuevo mensaje para mantener la sesión iniciada. Este flujo contiene lógica inteligente para que la opción **¿Quiere mantener la sesión iniciada?** no se muestre si el sistema de aprendizaje automático detecta un inicio de sesión de alto riesgo o un inicio de sesión desde un dispositivo compartido.



NOTE

La configuración de la opción para mantener la sesión iniciada requiere el uso de las ediciones Azure Active Directory (Azure AD) Premium 1, Premium 2 o Basic, o bien una licencia de Microsoft 365. Para obtener más información acerca de las ediciones y licencias, consulte [Suscripción a Azure AD Premium](#).

Las ediciones Azure AD Premium y Basic están disponibles para los clientes de China que utilizan la instancia mundial de Azure AD. Las ediciones Azure AD Premium y Basic no se admiten actualmente en el servicio de Azure administrado por 21Vianet en China. Para más información, póngase en contacto con nosotros en el [foro de Azure AD](#).

Configuración de KMSI

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, elija **Personalización de marca de empresa** y, a continuación, **Configurar**.
3. En la sección **Configuración avanzada**, busque el ajuste **Mostrar la opción para mantener la sesión iniciada**.

Esta opción de configuración permite elegir si los usuarios deben mantener la sesión iniciada en Azure AD hasta que cierren sesión explícitamente.

- Si elige **No**, la opción **¿Quiere mantener la sesión iniciada?** estará oculta cuando el usuario inicie sesión correctamente. El usuario deberá iniciar sesión cada vez que se cierre y vuelva a abrir el explorador.
- Si elige **Sí**, la opción **¿Quiere mantener la sesión iniciada?** se muestra al usuario.

Advanced settings

Sign-in page background color

Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

Square logo image, dark theme
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

Show option to remain signed in Yes No

Solución de problemas con el inicio de sesión

Si un usuario no actúa con el mensaje **¿Quiere mantener la sesión iniciada?**, tal como se muestra en el diagrama siguiente, pero abandona el intento de inicio de sesión, verá una entrada de registro de inicio de sesión que indica la interrupción.

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

Don't show this again

Los detalles sobre el error de inicio de sesión son los siguientes y se resaltan en el ejemplo.

- **Código de error de inicio de sesión:** 50140
- **Motivo del error:** Este error se produjo debido a una interrupción en "Mantener la sesión iniciada" cuando el usuario estaba iniciando sesión.

The screenshot shows the Azure Active Directory Sign-ins page. The left sidebar includes options like Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Configuration assessment, Security, Monitoring, Sign-ins (selected), Audit logs, Provisioning logs (Preview), Logs, Diagnostic settings, Workbooks, Usage & insights, and Troubleshooting + Support. The main area displays sign-in activity. A table lists two entries: one from 6/4/2020 at 11:20:55 AM for Timothy Perkins to the Azure Portal, which was interrupted, and another from 6/4/2020 at 11:09:04 AM for Timothy Perkins to the Azure Portal, which was successful. Below the table, a 'Details' section provides more information about the interrupted sign-in, including the status 'Interrupted', sign-in error code '50140', and failure reason 'This error occurred due to 'Keep me signed in' interrupt when the user was signing-in.' A red box highlights this failure reason.

Para evitar que los usuarios vean la interrupción, establezca **Mostrar la opción para mantener la sesión iniciada** en **No** en la configuración de personalización de marca avanzada. Esta acción deshabilita el mensaje de KMSI para todos los usuarios del directorio de Azure AD.

También puede usar los controles de sesión del explorador persistentes en el acceso condicional para impedir que los usuarios vean el mensaje de KMSI. Esta opción le permite deshabilitar el mensaje de KMSI para un grupo de usuarios seleccionado (por ejemplo, los administradores globales) sin que ello afecte al comportamiento de inicio de sesión del resto de usuarios del directorio. Para más información, consulte [Frecuencia de inicio de sesión de usuario](#).

Para asegurar que el aviso de KMSI se muestre sólo cuando pueda beneficiar al usuario, el aviso de KMSI no se muestra intencionadamente en los siguientes escenarios:

- El usuario ha iniciado sesión mediante SSO de conexión directa y la autenticación integrada de Windows (IWA)
- El usuario inició sesión mediante los Servicios de federación de Active Directory (AD FS) y Autenticación integrada de Windows
- El usuario es un invitado en el inquilino
- La puntuación de riesgo del usuario es alta
- El inicio de sesión se produce durante el flujo de consentimiento del usuario o administrador
- El control de sesión del explorador persistente se configura en una directiva de acceso condicional

Pasos siguientes

Obtenga información sobre otras opciones que afectan al tiempo de expiración de la sesión de inicio de sesión:

- Microsoft 365: [tiempo de expiración de sesión inactiva](#)
- Acceso condicional de Azure AD: [frecuencia de inicio de sesión de usuario](#)
- Azure Portal: [tiempo de expiración de inactividad de nivel de directorio](#)

Asociación o incorporación de una suscripción de Azure al inquilino de Azure Active Directory

22/07/2020 • 8 minutes to read • [Edit Online](#)

Una suscripción de Azure tiene una relación de confianza con Azure Active Directory (Azure AD). Una suscripción confía en Azure AD para autenticar usuarios, servicios y dispositivos.

Varias suscripciones pueden confiar en el mismo directorio de Azure AD. Cada suscripción solo puede confiar en un único directorio.

Si su suscripción expira, se pierde el acceso a los otros recursos asociados a la suscripción. Sin embargo, el directorio de Azure AD permanece en Azure. Puede asociar y administrar el directorio con una suscripción de Azure diferente.

Todos los usuarios tienen un único directorio *particular* para la autenticación. Los usuarios también pueden ser invitados en otros directorios. Puede ver los directorios principales e invitados para cada usuario en Azure AD.

IMPORTANT

Al asociar una suscripción a un directorio diferente, los usuarios que tengan roles asignados mediante el [control de acceso basado en rol \(RBAC\)](#) pierden el acceso. Los administradores de suscripciones clásicas, incluidos el administrador y los coadministradores del servicio, también pierden el acceso.

También se quitan las asignaciones de directivas de una suscripción cuando dicha suscripción está asociada a un directorio diferente.

El traslado del clúster de Azure Kubernetes Service (AKS) a otra suscripción o el traslado de la suscripción propietaria del clúster a un nuevo inquilino, provoca que el clúster pierda funcionalidad debido a la pérdida de asignaciones de roles y derechos de las entidades de servicio. Para obtener más información sobre AKS, consulte [Azure Kubernetes Service \(AKS\)](#).

Antes de empezar

Antes de poder asociar o agregar la suscripción, realice las siguientes tareas:

- Revise la siguiente lista de cambios que se producirán después de asociar o agregar su suscripción e infórmese sobre cómo podría verse afectado:
 - Los usuarios que tienen roles asignados mediante RBAC perderán el acceso.
 - El administrador y los coadministradores del servicio perderán el acceso.
 - Si tiene almacenes de claves, no se podrá acceder a ellos y tendrá que corregirlos después de la asociación.
 - Si tiene identidades administradas para recursos, como Virtual Machines o Logic Apps, debe volver a habilitarlas o crearlas después de la asociación.
 - Si tiene una instancia de Azure Stack registrada, tendrá que volver a registrarla después de la asociación.
- Iniciar sesión con una cuenta que:
 - Tiene una asignación de rol [Propietario](#) para la suscripción. Para obtener más información sobre cómo asignar el rol Propietario, consulte [Administración del acceso a los recursos de Azure mediante RBAC y Azure Portal](#).
 - Existe en el directorio actual y en el nuevo directorio. El directorio actual está asociado a la suscripción.

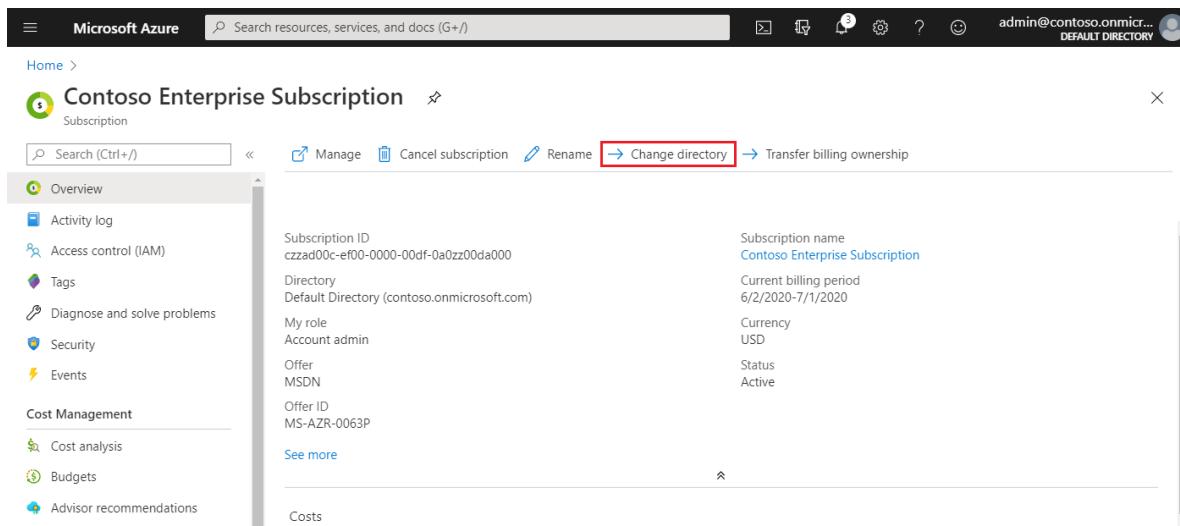
Va a asociar el nuevo directorio a la suscripción. Para más información sobre cómo obtener acceso a otro directorio, consulte [Adición de usuarios de colaboración B2B de Azure Active Directory en Azure Portal](#).

- Asegúrese de que no usa una suscripción de proveedores de servicios en la nube de Azure (CSP) (MS-AZR-0145P, MS-AZR-0146P, MS-AZR-159P), una suscripción interna de Microsoft (MS-AZR-0015P) o una suscripción a Microsoft Imagine (MS-AZR-0144P).

Asociación de una suscripción a un directorio

Para asociar una suscripción existente al directorio de Azure AD, siga estos pasos:

1. Inicie sesión y seleccione la suscripción que quiere usar en la [Página de suscripciones de Azure Portal](#).
2. Seleccione **Cambiar directorio**.



The screenshot shows the Azure portal interface for managing a subscription. The top navigation bar includes 'Microsoft Azure', a search bar, and user information ('admin@contoso.onmicrosoft.com'). Below the bar, the title 'Contoso Enterprise Subscription' is displayed. On the left, a sidebar lists various management options like 'Overview', 'Activity log', and 'Cost Management'. The main content area shows subscription details: 'Subscription ID: czzad00c-ef00-0000-00df-0a0zz00da000', 'Directory: Default Directory (contoso.onmicrosoft.com)', 'My role: Account admin', 'Offer: MSDN', and 'Offer ID: MS-AZR-0063P'. To the right of these details is a section for 'Subscription name' (set to 'Contoso Enterprise Subscription'), 'Current billing period' (set to '6/2/2020-7/1/2020'), 'Currency' (set to 'USD'), and 'Status' (set to 'Active'). At the top of the main content area, there are several buttons: 'Manage', 'Cancel subscription', 'Rename', 'Change directory' (which is highlighted with a red box), and 'Transfer billing ownership'. A 'See more' link is also present.

3. Revise las advertencias que aparecen y, a continuación, seleccione **Cambiar**.

Change the directory

X



Changing the directory removes access for all Role-Based Access Control users and other admins (including co-administrators). [See affected users](#)



Changing the directory doesn't change billing ownership for the subscription. You won't be able to delete the original directory until billing ownership is transferred to someone else. [Learn more](#)

From

Default Directory (contoso.onmicrosoft.com)

To

Contoso East Coast (000fb00a-0000-00fe-a00f-0d0ae0bcd0... ▾)

Change

Cancel

Una vez que se cambie el directorio para la suscripción, se mostrará un mensaje de confirmación.

4. Seleccione Cambiar directorios en la página suscripción para ir al nuevo directorio.

The screenshot shows two side-by-side views of the Azure portal. On the left, the 'Subscriptions' page lists 8 selected subscriptions. A red box highlights the 'Switch directories' link under the 'Showing subscriptions in Default Directory directory. Don't see a subscription?' section. On the right, the 'Directory + subscription' page shows the current directory as 'ajaneaburnley@gmail.onmicrosoft.com'. It includes a 'Switch directory' section with a dropdown set to 'Sign in to your last visited directory', and a list of available directories including 'Contoso East Coast' and 'Default Directory'.

Puede tardar varias horas hasta que todo se muestre correctamente. Si parece que tarda demasiado tiempo, compruebe el **filtro de suscripción global**. Asegúrese de que la suscripción que se ha trasladado no esté oculta. Es posible que tenga que cerrar la sesión de Azure Portal y volver a iniciarla para ver el directorio nuevo.

Cambiar el directorio de suscripción es una operación de nivel de servicio, por lo que no afecta a la propiedad de facturación de suscripción. El administrador de cuenta todavía puede cambiar al administrador de servicio desde el [centro de cuentas](#). Para eliminar el directorio original, debe transferir la propiedad de facturación de suscripción a un nuevo administrador de cuenta. Para más información acerca de cómo transferir la propiedad de facturación, vea [Transferencia de la propiedad de una suscripción de Azure a otra cuenta](#).

Pasos posteriores a la asociación

Después de asociar una suscripción a un directorio diferente, puede que tenga que realizar las siguientes tareas para reanudar las operaciones:

- Si tiene almacenes de claves, debe cambiar el Id. de inquilino del almacén de claves. Para más información, consulte [Cambio del identificador de inquilino de Key Vault después de mover una suscripción](#).
- Si usaba identidades administradas asignadas por el sistema para los recursos, debe volver a habilitar estas identidades. Si usaba identidades administradas asignadas por el usuario, debe volver a crear estas identidades. Después de volver a habilitar o crear las identidades administradas, debe volver a restablecer los permisos asignados a esas identidades. Para más información, consulte [¿Qué es Managed Identities for Azure Resources?](#)
- Si ha registrado una instancia de Azure Stack que usa esta suscripción, debe volver a registrarla. Para obtener más información, consulte [Registro de Azure Stack con Azure](#).

Pasos siguientes

- Para crear un nuevo inquilino de Azure AD, consulte [Inicio rápido: Creación de un inquilino en Azure Active Directory](#).
- Para más información sobre cómo controla Microsoft Azure el acceso a los recursos, consulte [Roles de administrador de suscripciones clásicas, roles de RBAC de Azure y roles de administrador de Azure AD](#).
- Para más información sobre cómo asignar roles en Azure AD, consulte [Asignación de roles de administrador y no administrador a los usuarios con Azure Active Directory](#).

Incorporación de información de privacidad de su organización con Azure Active Directory

22/07/2020 • 3 minutes to read • [Edit Online](#)

En este artículo se explica cómo un administrador de inquilinos puede agregar información relacionada con la privacidad al inquilino de Azure Active Directory (Azure AD) de una organización, a través de Azure Portal.

Se recomienda agregar su contacto de privacidad global y la declaración de privacidad de su organización, de modo que los empleados internos e invitados externos puedan revisar las directivas. Dado que las declaraciones de privacidad se crean de forma única y específica para cada negocio, es recomendable ponerse en contacto con un abogado para obtener ayuda.

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](#).

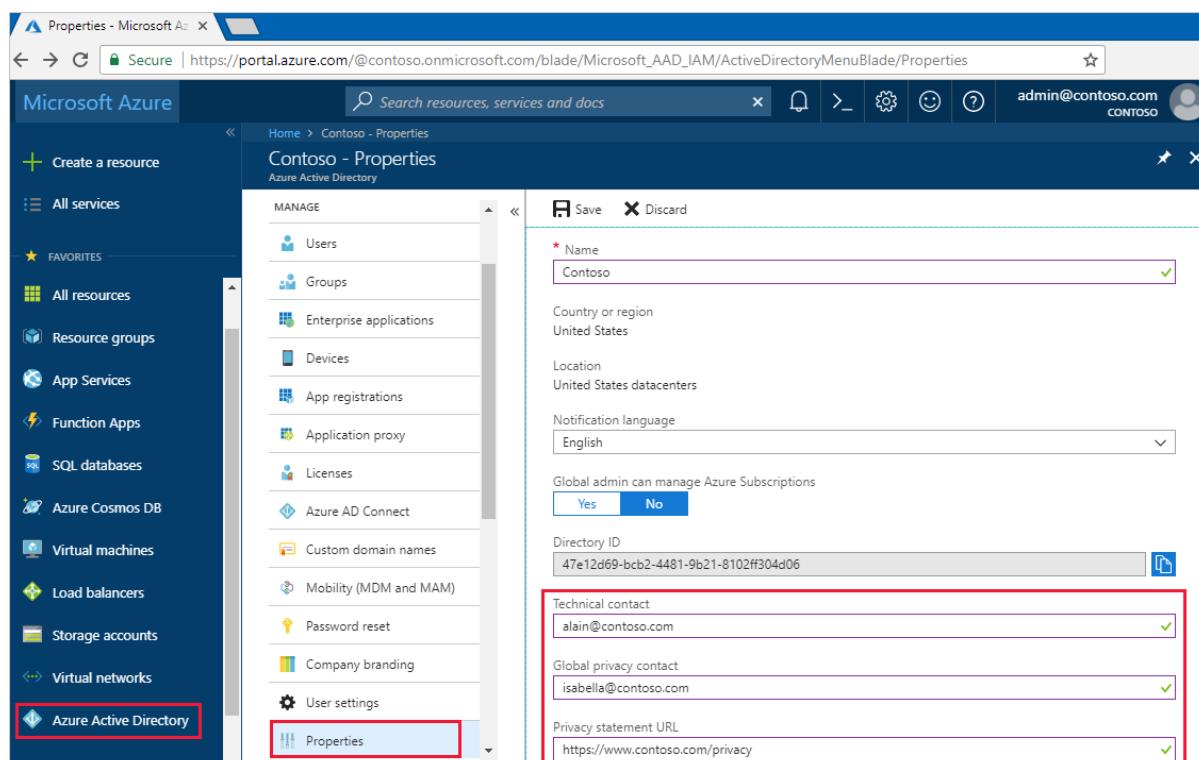
Incorporación de la información de privacidad en Azure AD

Puede agregar información de privacidad de su organización en el área de **Propiedades** de Azure AD.

Para acceder al área de propiedades y agregar la información de privacidad

1. Inicie sesión en Azure Portal como administrador de inquilinos.
2. En la barra de navegación izquierda, seleccione **Azure Active Directory** y, luego, seleccione **Propiedades**.

Se muestra el área de **Propiedades**.



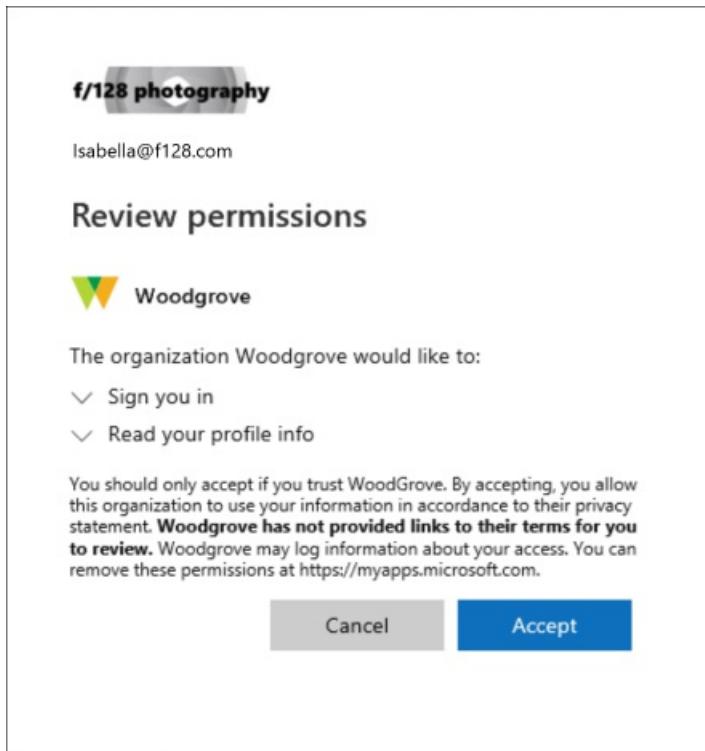
The screenshot shows the Azure portal interface with the URL https://portal.azure.com/@contoso.onmicrosoft.com/blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties. The left sidebar has 'Azure Active Directory' selected. The main area shows the 'Contoso - Properties' blade for 'Azure Active Directory'. The 'MANAGE' section on the left includes options like Users, Groups, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, and User settings. The 'Properties' option is highlighted with a red box. The right side shows fields for 'Name' (Contoso), 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), 'Global admin can manage Azure Subscriptions' (Yes), 'Directory ID' (47e12d69-bcb2-4481-9b21-8102ff304d06), 'Technical contact' (alain@contoso.com), 'Global privacy contact' (isabella@contoso.com), and 'Privacy statement URL' (<https://www.contoso.com/privacy>). The 'Technical contact' field is also highlighted with a red border.

3. Agregar la información de privacidad de sus empleados:

- **Contacto técnico.** Escriba la dirección de correo electrónico de la persona de contacto para el soporte técnico de su organización.
- **Contacto de privacidad global.** Escriba la dirección de correo electrónico de la persona de contacto para consultas sobre privacidad de los datos personales. Esta persona también es quien se pone en contacto con Microsoft si se produce una vulneración de datos. Si no aparece ninguna persona aquí, Microsoft se pone en contacto con los administradores globales.
- **URL de la declaración de privacidad.** Escriba el vínculo del documento de su organización que describe la forma en que su organización controla la privacidad de datos interna y externa del invitado.

IMPORTANT

Si no incluye su propia declaración de privacidad o su contacto de privacidad, los invitados externos verán el texto en el cuadro de diálogo **Permisos de revisión** que dice: <*nombre de su organización*> no ha proporcionado vínculos de sus términos que pueda revisar. Por ejemplo, un usuario invitado verá este mensaje cuando reciba una invitación para acceder a una organización a través de la colaboración B2B.



4. Seleccione Guardar.

Pasos siguientes

- [Canje de invitación de colaboración B2B de Azure Active Directory](#)
- [Adición o modificación de la información de perfil de un usuario en Azure Active Directory](#)

Creación de un grupo básico e incorporación de miembros con Azure Active Directory

22/07/2020 • 8 minutes to read • [Edit Online](#)

Puede crear un grupo básico con el portal de Azure Active Directory (Azure AD). Para los fines de este artículo, el propietario del recurso (administrador) agrega un grupo básico a un único recurso e incluye miembros específicos (empleados) que necesitan acceder a dicho recurso. Para escenarios más complejos, incluida la creación de reglas y las pertenencias dinámicas, vea la [documentación de administración de usuarios de Azure Active Directory](#).

Tipos de grupo y pertenencia

Hay varios tipos de grupo y de pertenencia. La siguiente información explica cada tipo de grupo y pertenencia, así como el motivo por el que se usan, para ayudarle a decidir las opciones que usará al crear un grupo.

Tipos de grupo:

- **Seguridad.** Se usa 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 para 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 agregar permisos a cada miembro individualmente. Un grupo de seguridad puede tener usuarios, dispositivos, grupos y entidades de servicio como miembros y usuarios y entidades de servicio como propietarios. Para más información sobre la administración de acceso a los recursos, vea [Administración de acceso a los recursos con grupos de Azure Active Directory](#).
- **Office 365.** Ofrece oportunidades de colaboración al conceder acceso a los miembros a un correo compartido, calendarios, archivos, el sitio de SharePoint y mucho más. Esta opción también permite ofrecer a personas de fuera de su organización acceso al grupo. Un grupo de Office 365 solo puede tener usuarios como miembros. Tanto los usuarios como las entidades de servicio pueden ser propietarios de registros de Office 365. Para más información sobre los Grupos de Office 365, vea [Obtenga más información sobre los grupos de Office 365](#).

Tipos de pertenencia:

- **Asignado.** Le permite agregar usuarios específicos para que sean miembros de este grupo y para que tengan permisos exclusivos. Para los fines de este artículo, vamos a usar esta opción.
- **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 ver si el miembro cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).
- **Dispositivo dinámico.** Le 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 ver si el dispositivo cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).

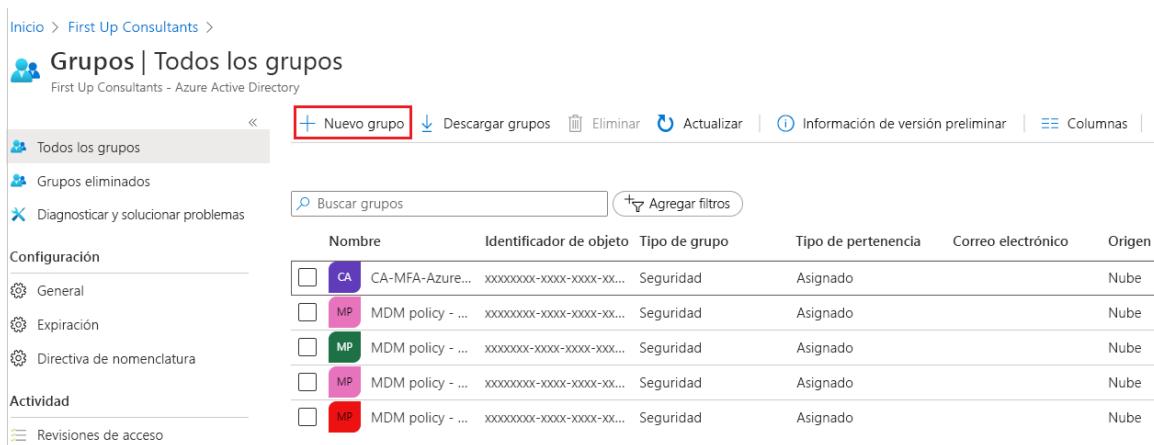
IMPORTANT

Puede crear un grupo dinámico para dispositivos o usuarios, pero no para ambos. Tampoco 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. Para más información sobre cómo crear un grupo dinámico para usuarios y dispositivos, consulte [Creación de un grupo dinámico y comprobación de su estado](#).

Creación de un grupo básico y adición de miembros

Puede crear un grupo básico y agregar los miembros al mismo tiempo. Para crear un grupo básico y agregar miembros, use el procedimiento siguiente:

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Busque y seleccione **Azure Active Directory**.
3. En la página **Active Directory**, seleccione **Grupos** y, a continuación, seleccione **Nuevo grupo**.



The screenshot shows the 'Grupos | Todos los grupos' page in the Azure Active Directory portal. The top navigation bar includes 'Inicio > First Up Consultants >' followed by the title 'Grupos | Todos los grupos'. Below the title, there's a breadcrumb trail 'First Up Consultants - Azure Active Directory'. The main area has a header with 'Nuevo grupo' (highlighted with a red box), 'Descargar grupos', 'Eliminar', 'Actualizar', 'Información de versión preliminar', and 'Columnas'. On the left, a sidebar lists 'Todos los grupos', 'Grupos eliminados', and 'Diagnosticar y solucionar problemas'. Under 'Configuración', there are sections for 'General', 'Expiración', and 'Directiva de nomenclatura'. Under 'Actividad', there's a link to 'Revisiones de acceso'. The main content area displays a table of groups with columns: 'Nombre', 'Identificador de objeto', 'Tipo de grupo', 'Tipo de pertenencia', 'Correo electrónico', and 'Origen'. The table contains six entries, each with a checkbox and a small icon (purple CA, pink MP, green MP, pink MP, red MP). The first entry is CA-MFA-Azure... and the last is MDM policy -

4. Aparecerá el panel **Nuevo grupo** y deberá llenar la información necesaria.

Nuevo grupo

Tipo de grupo *

Office 365

Nombre del grupo * ⓘ

Directiva MDM: Este



Dirección de correo electrónico de grupo * ⓘ

MDMPolicy-East



@firstupconsultants92157408.onmicrosoft.com

Descripción del grupo ⓘ

Usuarios de MDM en la costa este



Tipo de pertenencia ⓘ

Asignado



Propietarios

No se ha seleccionado ningún propietario.

Miembros

No hay miembros seleccionados.

Crear

5. Seleccione un valor de **Tipo de grupo** predefinido. Para obtener más información sobre los tipos de grupo, consulte [Tipos de grupo y pertenencia](#).
6. Cree y agregue un **nombre de grupo**. Agregue un nombre que sea fácil de recordar y que tenga sentido para el grupo. Se realizará una comprobación para determinar si el nombre ya se utiliza para otro grupo. Si el nombre ya está en uso, para evitar duplicarlo, se le pedirá que modifique el nombre del grupo.
7. Agregue una **Dirección de correo electrónico de grupo** o deje la dirección de correo electrónico que se rellena automáticamente.
8. **Descripción del grupo**. Agregue una descripción opcional al grupo.
9. Seleccione un **Tipo de pertenencia** (obligatorio) predefinido. Para obtener más información sobre los tipos de pertenencia, consulte [Tipos de grupo y pertenencia](#).
10. Seleccione **Crear**. El grupo se crea y está listo para que agregue miembros.
11. Seleccione el área **Miembros** de la página **Grupo** y después empiece a buscar los miembros para agregarlos al grupo en la página **Seleccionar miembros**.

12. Cuando haya terminado de agregar miembros, elija **Seleccionar**.

La página **Información general del grupo** se actualiza para mostrar el número de miembros que ahora se agregan al grupo.

Activación o desactivación del correo electrónico de bienvenida al grupo

Siempre que se crea un grupo de Office 365, independientemente de que la pertenencia sea estática o dinámica, se envía una notificación de bienvenida a todos los usuarios que se agregan al grupo. Cuando cambian los atributos de un usuario o dispositivo, se procesan todas las reglas de grupo dinámico de la organización para comprobar si hay posibles cambios de pertenencia. Los usuarios que se agregan también reciben la notificación de bienvenida. Este comportamiento se puede desactivar en [Exchange PowerShell](#).

Pasos siguientes

- Administrar el acceso a las aplicaciones SaaS mediante grupos
- Administrar grupos mediante los comandos de PowerShell

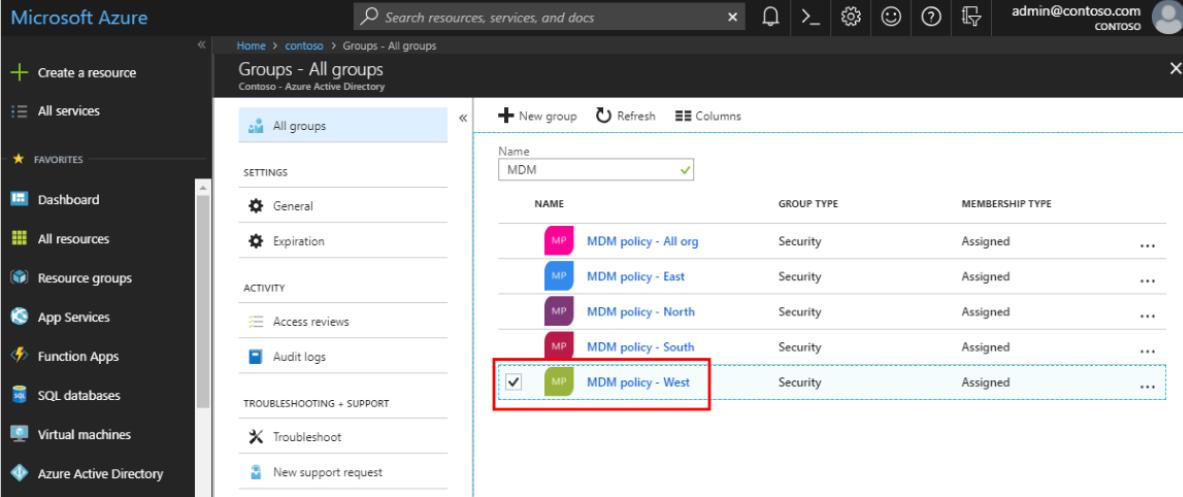
Incorporación o eliminación de los miembros de un grupo mediante Azure Active Directory

22/07/2020 • 2 minutes to read • [Edit Online](#)

Con Azure Active Directory, puede seguir agregando y quitando miembros del grupo.

Para agregar miembros al grupo

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory** y después seleccione **Grupos**.
3. En la página **Grupos - Todos los grupos**, busque y seleccione el grupo al que quiere agregar el miembro.
En este caso, use nuestro grupo creado anteriormente, **MDM policy - West**.



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, All services, Favorites, Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Virtual machines, and Azure Active Directory. The Azure Active Directory icon is selected. The main area is titled 'Groups - All groups' under 'Contoso - Azure Active Directory'. It shows a list of groups with columns for Name, Group Type, and Membership Type. One group, 'MDM policy - West', is highlighted with a red box around its row. The 'Name' column shows 'MDM' and the 'Membership Type' column shows 'Assigned'. The 'Group Type' column shows 'Security'.

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM	Security	Assigned
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

4. En la página **Información general de MDM policy - West**, seleccione **Miembros** en el área **Administrar**.

MDM policy - West

Group

The screenshot shows the 'MDM policy - West' group page. On the left, a navigation pane lists 'Overview', 'Properties', 'Members' (which is highlighted with a red box), 'Owners', 'Group memberships', 'Applications', 'Licenses', and 'Azure resources'. Below this is an 'ACTIVITY' section with 'Access reviews' and 'Audit logs'. The main content area has a large green 'MP' logo. It displays membership details: 'Assigned' (Type: Security, Source: Cloud), 'Members' (50 User(s), 0 Group(s), 50 Device(s), 0 Other(s)), 'Group memberships' (0), and 'Owners' (2). A 'Delete' button is at the top right.

5. Seleccione Agregar miembros y, a continuación, busque y seleccione a cada uno de los miembros que desea agregar al grupo y elija Seleccionar.

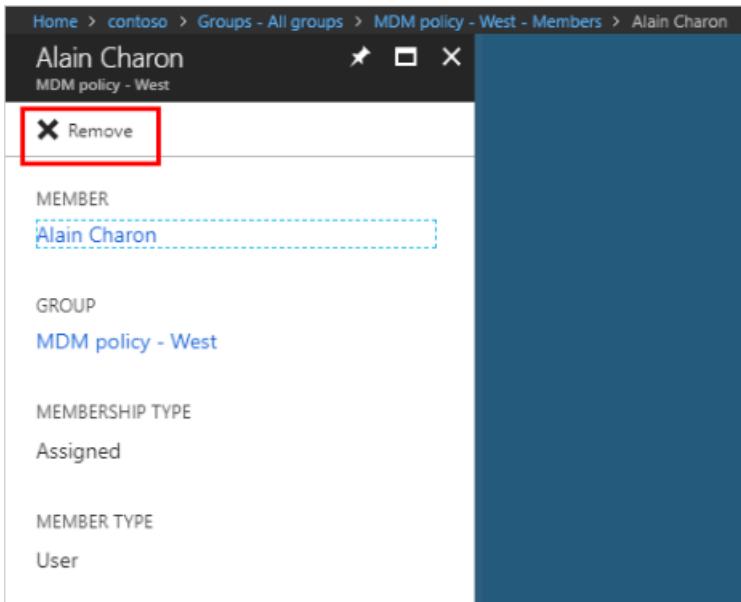
Obtendrá un mensaje que indica que los miembros se han agregado correctamente.

The screenshot shows the 'MDM policy - West - Members' page with the 'Add members' dialog open. The 'Add members' button is highlighted with a red box. In the search bar, 'Alain' is typed, and a result for 'Alain Charon' (alain@contoso.com) is shown. Below the search bar, the 'Selected members:' list contains Danielle McKay (danielle@contoso.com) and Eggert Schafer (eggert@contoso.com), each with a 'Remove' link. At the bottom of the dialog, a 'Select' button is highlighted with a red box.

6. Actualice la pantalla para ver el nombre de todos los miembros agregados al grupo.

Para eliminar miembros del grupo

1. En la página Grupos - Todos los grupos, busque y seleccione el grupo al que quiere quitar un miembro. De nuevo, usaremos como ejemplo a MDM policy - West.
2. Seleccione Miembros desde el área Administrar, busque y seleccione el nombre del miembro que desea quitar y, a continuación, seleccione Quitar.



Pasos siguientes

- [Visualización de grupos y miembros](#)
- [Edición de la configuración de un grupo](#)
- [Administrar el acceso a los recursos mediante grupos](#)
- [Administrar reglas dinámicas de los usuarios de un grupo](#)
- [Asociar o agregar una suscripción de Azure a Azure Active Directory](#)

Eliminación de un grupo con Azure Active Directory

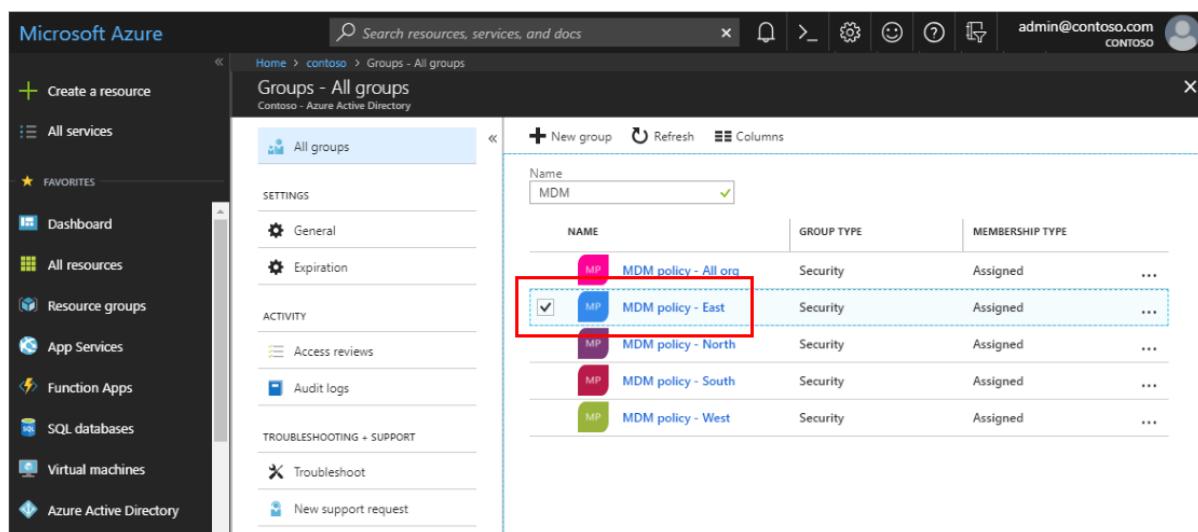
22/07/2020 • 2 minutes to read • [Edit Online](#)

Puede eliminar un grupo de Azure Active Directory (Azure AD) por infinidad de motivos, pero normalmente será porque:

- Ha establecido incorrectamente el **Tipo de grupo** en la opción incorrecta.
- Ha creado un grupo incorrecto o duplicado por error.
- Ya no necesita el grupo.

Para eliminar un grupo

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory** y después seleccione **Grupos**.
3. En la página **Grupos - Todos los grupos**, busque y seleccione el grupo que quiere eliminar. Para estos pasos, vamos a usar **MDM policy - East**.



The screenshot shows the Azure portal interface. On the left, the navigation menu includes 'Create a resource', 'All services', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'. The main content area is titled 'Groups - All groups' under 'Contoso - Azure Active Directory'. It shows a list of groups with columns for 'NAME', 'GROUP TYPE', and 'MEMBERSHIP TYPE'. One group, 'MDM policy - East', is highlighted with a red box and has a checkmark in its selection column. Other groups listed are 'MDM policy - All org', 'MDM policy - North', 'MDM policy - South', and 'MDM policy - West'. Each group has a 'More options' button ('...') at the end of its row.

4. En la página **Información general de MDM policy - East**, seleccione **Eliminar**.

Se elimina el grupo del inquilino de Azure Active Directory.

MDM policy - East

Group

Overview

Delete

MDM policy - East

Membership type: Assigned

Type: Security

Source: Cloud

Members: 0 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

Group memberships: 0

Owners: 0

Pasos siguientes

- Si elimina por error un grupo, puede crearlo de nuevo. Para más información, consulte [Cómo crear un grupo básico y agregar miembros](#).
- Si elimina un grupo de Office 365 por error, puede restaurarlo. Para más información, consulte [Restauración de un grupo eliminado de Office 365](#).

Incorporación o eliminación de un grupo de otro grupo con Azure Active Directory

22/07/2020 • 5 minutes to read • [Edit Online](#)

En este artículo encontrará ayuda para agregar y quitar un grupo de otro grupo con Azure Active Directory.

NOTE

Si intenta eliminar el grupo primario, consulte el artículo sobre [la actualización y la eliminación de un grupo y sus miembros](#).

Incorporación de un grupo a otro grupo

Puede agregar un grupo de seguridad existente a otro grupo de seguridad existente (lo que también se conoce como grupos anidados), y crear un grupo de miembros (subgrupo) y un grupo principal. El grupo miembro hereda los atributos y las propiedades del grupo primario, lo que le ahorra tiempo de configuración.

IMPORTANT

En este momento, no se admite:

- Agregar grupos a un grupo sincronizado con Active Directory local.
- Agregar grupos de seguridad a grupos de Office 365.
- Agregar grupos de Office 365 a grupos de seguridad u otros grupos de Office 365.
- Asignar aplicaciones a grupos anidados.
- Aplicar licencias a grupos anidados.
- Agregar grupos de distribución en escenarios de anidamiento.

Para agregar un grupo como miembro de otro grupo, siga estos pasos:

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory** y después seleccione **Grupos**.
3. En la página **Grupos - Todos los grupos**, busque y seleccione el grupo que va a convertirse en miembro de otro grupo. Para este ejercicio, usaremos el grupo **MDM policy - West**.

NOTE

Puede agregar el grupo como miembro solo a un otro grupo a la vez. Además, el cuadro **Seleccionar grupo** filtra la visualización en función de si coincide lo que ha escrito con cualquier parte del nombre de un usuario o dispositivo. Sin embargo, no se admiten caracteres comodín.

4. En la página **MDM policy - West - Group memberships**, seleccione **Pertenencia a grupos**, seleccione **Agregar**, busque el grupo de que quiere que su grupo sea miembro y, luego, elija **Seleccionar**. Para este ejercicio, usaremos el grupo **MDM policy - All org**.

El grupo **MDM policy - West** ahora es miembro del grupo **MDM policy - All org**, y hereda todas las propiedades y la configuración del grupo **MDM policy - All org**.

5. Revise la página **MDM policy - West - Group memberships** para ver la relación entre el grupo y el miembro.
6. Para obtener una vista más detallada de la relación entre el grupo y el miembro, seleccione el nombre del grupo (**MDM policy - All org**) y eche un vistazo a los detalles de la página **MDM policy - West**.

Eliminación de un grupo de otro grupo

Puede quitar un grupo de seguridad existente de otro grupo de seguridad. Sin embargo, al quitar el grupo también se eliminan los atributos y propiedades heredados de sus miembros.

Para quitar un grupo miembro de otro grupo

1. En la página **Grupos - Todos los grupos**, busque y seleccione el grupo que va a quitarse como miembro de otro grupo. Para este ejercicio, volveremos a usar el grupo **MDM policy - West**.
2. En la página **Información general de MDM policy - West**, seleccione **Pertenencia a grupos**.

3. Seleccione el grupo MDM policy - All org de la página MDM policy - West - Group memberships y, luego, seleccione Quitar de los detalles de la página MDM policy - West.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a navigation bar with 'Home > Contoso > Groups - All groups > MDM policy - West - Group memberships'. Below this, the title 'MDM policy - West - Group memberships' is displayed next to a gear icon and the word 'Group'. On the left, a sidebar titled 'Manage' lists several options: 'Properties' (selected), 'Members', 'Owners', 'Group memberships' (highlighted with a red box), 'Applications', 'Licenses', and 'Azure resources'. The main content area has a header with buttons for 'Add memberships' (with a plus sign), 'Remove memberships' (with a trash bin icon), 'Refresh' (with a circular arrow), 'Columns' (with a grid icon), and 'Got feedback?' (with a heart icon). Below the header, a purple banner says 'Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview.' A table follows, showing one group entry: 'MDM policy - All o...' with 'Object Id' 'MP', 'Group Type' 'Security', and 'Membership Type' 'Assigned'. The 'Name' column has a blue checkbox icon.

Información adicional

Estos artículos proporcionan información adicional sobre Azure Active Directory.

- [Visualización de grupos y miembros](#)
- [Creación de un grupo básico e incorporación de miembros](#)
- [Incorporación o eliminación de miembros de un grupo](#)
- [Edición de la configuración de un grupo](#)
- [Uso de un grupo para administrar el acceso a las aplicaciones SaaS](#)
- [Escenarios, limitaciones y problemas conocidos del uso de grupos para administrar las licencias en Azure Active Directory](#)

Edición de la información de un grupo mediante Azure Active Directory

22/07/2020 • 3 minutes to read • [Edit Online](#)

Con Azure Active Directory (Azure AD), puede editar la configuración de un grupo, lo que incluye actualizar su nombre, descripción o tipo de pertenencia.

Para editar la configuración de un grupo

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.

2. Seleccione **Azure Active Directory** y después seleccione **Grupos**.

Aparecerá la página **Grupos - Todos los grupos** con todos los grupos activos.

3. Desde la página **Grupos - Todos los grupos**, escriba parte del nombre del grupo en el cuadro de **Búsqueda**. Para los fines de este artículo, buscaremos el grupo **MDM policy - West**.

Los resultados de búsqueda aparecen bajo el cuadro de **Búsqueda**, y se actualizan a medida que escribe más caracteres.

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

4. Seleccione el grupo **MDM policy - West** y, a continuación, seleccione **Propiedades** desde la sección **Administrar**.

MDM policy - West

Properties

Membership type: Assigned
Type: Security
Source: Cloud

Members: 50 User(s), 0 Group(s), 50 Device(s), 0 Other(s)

Group memberships: 0 Owners: 2

5. Actualice la información de **configuración general** según sea necesario, incluidos:

MDM policy - West - Properties

General settings

* Group name: MDM policy - West

Group description: MDM users on West coast

Group type: Security

* Membership type: Assigned

Object ID: 9f33d478-96e3-4577-894e-02f406e8c804

- Nombre del grupo.** Edite el nombre de grupo existente.
- Descripción del grupo.** Edite la descripción de grupo existente.
- Tipo de grupo.** No se puede cambiar el tipo de grupo después de que se ha creado. Para cambiar el **tipo de grupo**, debe eliminar el grupo y crear uno nuevo.
- Tipo de pertenencia.** Cambie el tipo de pertenencia de un grupo. Para más información sobre los distintos tipos de pertenencia disponibles, consulte [Creación de un grupo básico e incorporación de miembros mediante el portal de Azure Active Directory](#).
- Identificador de objeto.** No se puede cambiar el identificador de objeto, pero puede copiarlo para usarlo en los comandos de PowerShell para el grupo. Para más información acerca del uso de cmdlets de PowerShell, consulte [Cmdlets de Azure Active Directory para configurar las opciones de grupo](#).

Pasos siguientes

Estos artículos proporcionan información adicional sobre Azure Active Directory.

- [Visualización de grupos y miembros](#)
- [Creación de un grupo básico e incorporación de miembros](#)
- [Incorporación o eliminación de miembros de un grupo](#)
- [Administrar reglas dinámicas de los usuarios de un grupo](#)
- [Administrar la pertenencia a grupos](#)
- [Administrar el acceso a los recursos mediante grupos](#)
- [Asociar o agregar una suscripción de Azure a Azure Active Directory](#)

Adición o eliminación de propietarios del grupo en Azure Active Directory

22/07/2020 • 4 minutes to read • [Edit Online](#)

Los grupos de Azure Active Directory (Azure AD) pertenecen a propietarios del grupo, quienes también lo administran. Los propietarios del grupo pueden ser usuarios o entidades de servicio y disponen de la capacidad de administrar el grupo, incluida la pertenencia. Los propietarios de grupos existentes o los administradores de gestión de grupos son los únicos que pueden asignar propietarios de grupos. Los propietarios del grupo no deben ser miembros del grupo.

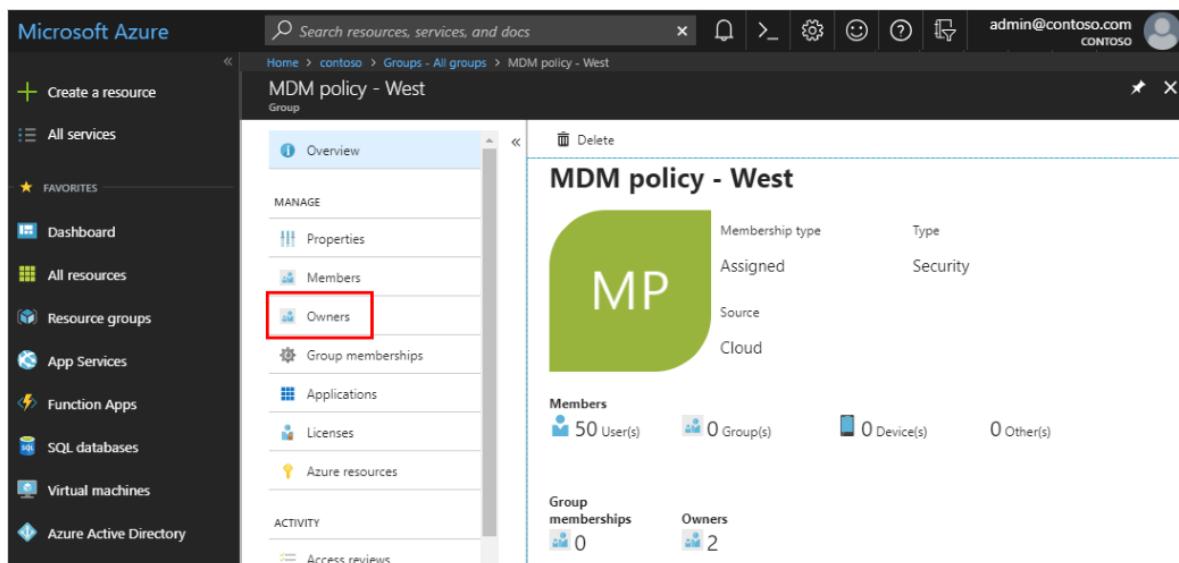
Cuando un grupo no tiene propietario, los administradores de gestión de grupos pueden administrar el grupo. Se recomienda que cada grupo tenga al menos un propietario. Una vez que se asignan los propietarios a un grupo, no se puede quitar el último propietario del grupo. Asegúrese de seleccionar otro propietario antes de quitar el último propietario del grupo.

Adición de un propietario a un grupo

A continuación encontrará las instrucciones para agregar un usuario como propietario a un grupo mediante el portal de Azure AD. Para agregar una entidad de servicio como propietario de un grupo, siga las instrucciones para hacerlo mediante [PowerShell](#).

Para agregar un propietario del grupo

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, **Grupos** y, a continuación, el grupo para el que quiera agregar un propietario (en este ejemplo, *MDM policy - West* (Directiva MDM - Oeste)).
3. En la página **MDM policy - West Overview** (Información general de la directiva de MDM - Oeste), seleccione **Propietarios**.



The screenshot shows the Azure portal interface. On the left, there's a navigation bar with 'Create a resource', 'All services', 'Favorites', and specific service links like 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'. The 'Azure Active Directory' link is underlined. The main content area shows the 'MDM policy - West' group overview. The left sidebar has sections for 'Overview', 'MANAGE' (Properties, Members, Owners, Group memberships, Applications, Licenses, Azure resources), 'ACTIVITY' (Access reviews), and 'DELETE'. The 'Owners' link is highlighted with a red box. The main panel displays the group details: 'MDM policy - West' (Membership type: Assigned, Type: Security, Source: Cloud), 'Members' (50 User(s), 0 Group(s), 0 Device(s), 0 Other(s)), 'Group memberships' (0), and 'Owners' (2). At the bottom, there are 'Edit' and 'Delete' buttons.

4. En la página **MDM policy - West - Owners** (Directiva MDM - Oeste - Propietarios), seleccione **Agregar propietarios**, busque y seleccione el usuario que será el nuevo propietario del grupo y, a continuación, elija **Seleccionar**.

The screenshot shows the 'MDM policy - West - Owners' page in the Azure portal. On the left, there's a navigation menu with options like Overview, Properties, Members, Owners (which is selected), Group memberships, Applications, Licenses, and Azure resources. Below that is an Activity section with Access reviews and Audit logs. In the center, there's a list of owners: Danielle McKay and Eggert Schafer. At the top right, there's a '+ Add owners' button. A modal window titled 'Add Owners' is open, showing a search bar with 'Alain' and a result for 'Alain Charon alain@contoso.com'. A red box highlights the 'Select' button at the bottom right of the modal.

Después de seleccionar el nuevo propietario, puede actualizar la página **Propietarios** y ver el nombre agregado a la lista de propietarios.

Eliminación de un propietario de un grupo

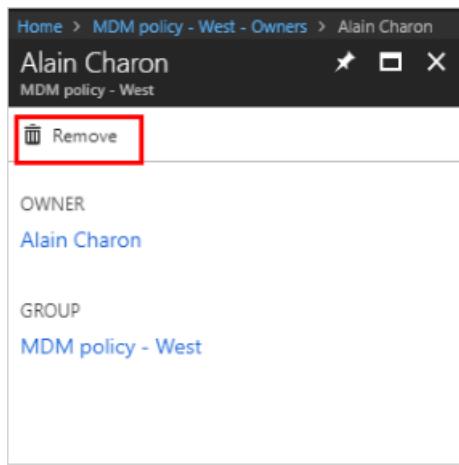
Elimine un propietario de un grupo mediante Azure AD.

Para quitar un propietario

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Seleccione **Azure Active Directory**, **Grupos** y a continuación el grupo en el que quiera eliminar un propietario (en este ejemplo, *MDM policy - West*).
3. En la página **MDM policy - West Overview** (Información general de la directiva de MDM - Oeste), seleccione **Propietarios**.

The screenshot shows the 'MDM policy - West' overview page in the Azure portal. On the left, there's a navigation menu with Create a resource, All services, and a Favorites section containing Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Virtual machines, and Azure Active Directory. Below that is an Activity section with Access reviews. In the center, there's a large green button with 'MP'. To its right, there are sections for Membership type (Assigned), Type (Security), Source (Cloud), and Members (50 User(s)). At the bottom, there are sections for Group memberships (0) and Owners (3). A red box highlights the 'Owners' link in the left sidebar.

4. En la página **MDM policy - West - Owners** (Directiva MDM - Oeste - Propietarios), seleccione el usuario que quiera quitar como propietario del grupo, elija **Quitar** en la página de información del usuario y seleccione Sí para confirmar su decisión.



Después de quitar el propietario, puede volver a la página **Propietarios** y ver que se ha quitado el nombre de la lista de propietarios.

Pasos siguientes

- [Administración del acceso a los recursos con grupos de Azure Active Directory](#)
- [Cmdlets de Azure Active Directory para configurar las opciones de grupo](#)
- [Uso de grupos para asignar acceso a una aplicación SaaS integrada](#)
- [Integración de las identidades locales con Azure Active Directory](#)
- [Cmdlets de Azure Active Directory para configurar las opciones de grupo](#)

Administración del acceso a recursos y aplicaciones con grupos en Azure Active Directory

22/07/2020 • 7 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) le permite usar grupos para administrar el acceso a las aplicaciones en la nube, las aplicaciones locales y los recursos. Sus recursos pueden formar parte de la organización de Azure AD, como los permisos para administrar objetos a través de los roles en Azure AD, o pueden estar fuera de la organización, como las aplicaciones SaaS (software como servicio), los servicios de Azure, los sitios de SharePoint y los recursos locales.

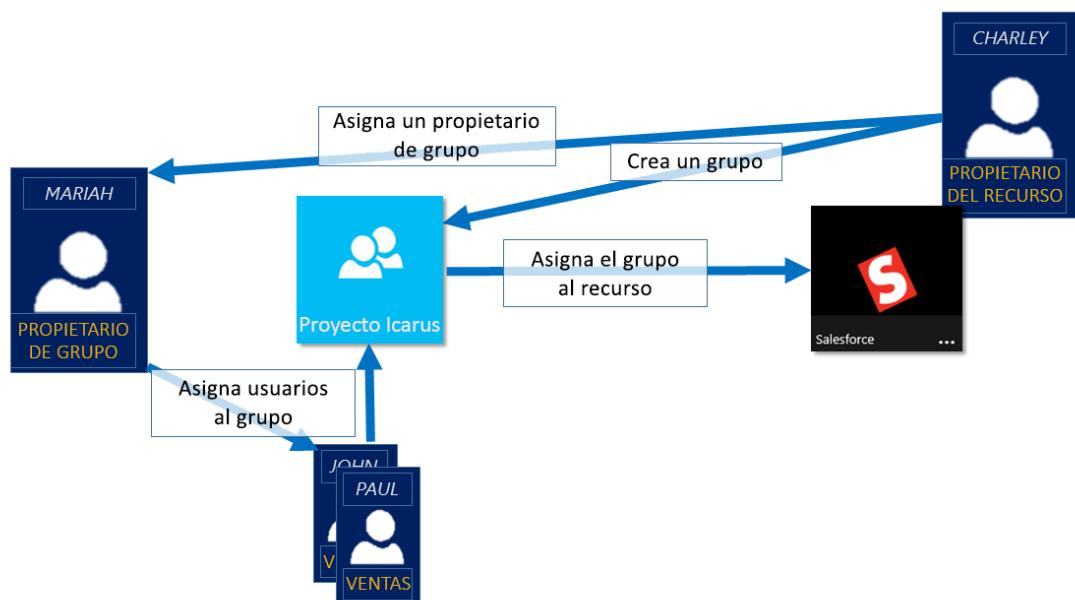
NOTE

En Azure Portal, puede ver algunos grupos cuyos miembros y detalles de grupo no se pueden administrar en el portal:

- Los grupos sincronizados desde Active Directory local solo se pueden administrar en Active Directory local.
- Otros tipos de grupos, como 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.

Funcionamiento de la administración de acceso en Azure AD

Azure AD le ayuda a proporcionar acceso a los recursos de su organización, ya que proporciona derechos de acceso a un usuario individual o a todo un grupo de Azure AD. El uso de grupos permite al propietario de los recursos (o al propietario del directorio de Azure AD) asignar un conjunto de permisos de acceso a todos los miembros del grupo, en lugar de tener que proporcionar los derechos uno por uno. El propietario del recurso o del directorio también puede conceder derechos de administrador para la lista de miembros a otra persona, como por ejemplo, a un director de departamento o a un administrador del departamento de soporte técnico, y dejar que dicha persona agregue y quite miembros, según sea necesario. Para más información acerca de cómo administrar propietarios de grupos, consulte [Administración de propietarios de grupos](#)



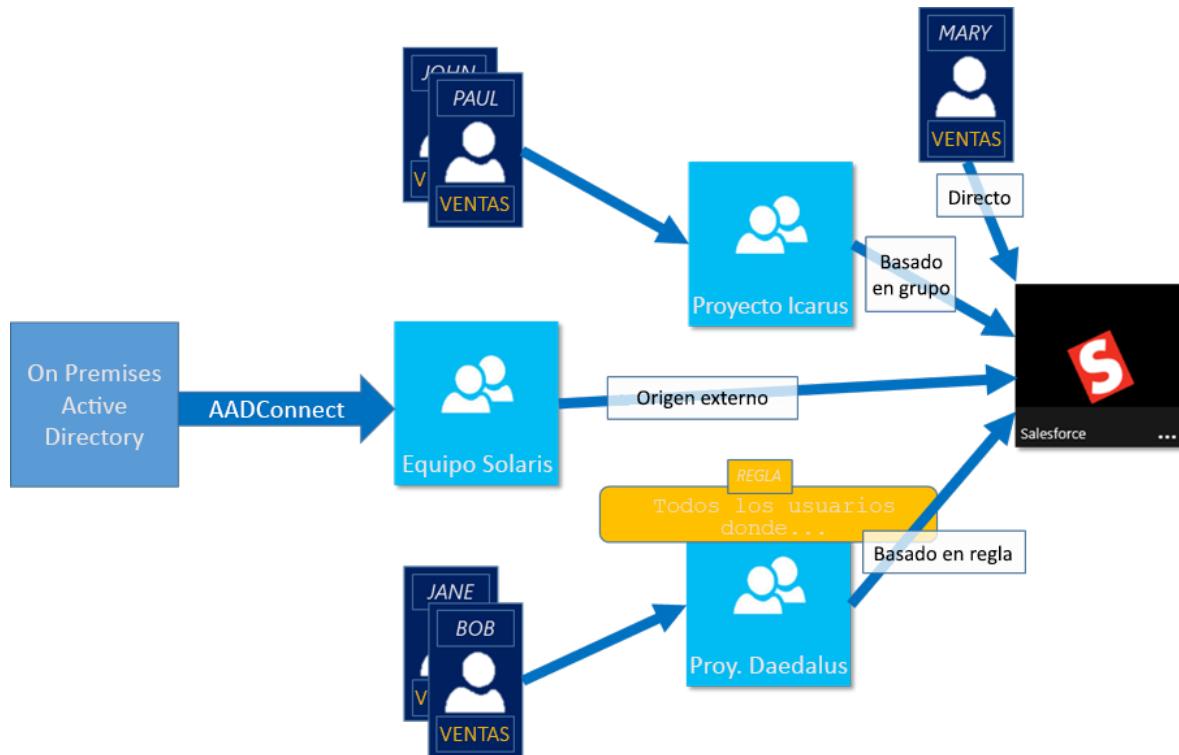
Formas de asignar derechos de acceso

Hay cuatro maneras de asignar derechos de acceso a los recursos a los usuarios:

- **Asignación directa.** El propietario del recurso asigna directamente el usuario al recurso.
- **Asignación de un grupo.** El propietario del recurso asigna un grupo de Azure AD al recurso, que automáticamente concede a todos sus miembros acceso al recurso. La pertenencia a un grupo la administran el propietario del grupo y el propietario del recurso, lo que permite a ambos propietarios agregar o quitar miembros del grupo. Para más información acerca de cómo agregar o eliminar miembros del grupo, consulte [Procedimiento para cómo agregar o quitar un grupo de otro grupo con Azure Active Directory](#).
- **Asignación basada en reglas.** El propietario del recurso crea un grupo y usa una regla para definir qué usuarios están asignados a un recurso concreto. La regla se basa en atributos que se asignan a usuarios individuales. El propietario del recurso administra la regla, lo que determina los atributos y valores que son necesarios para permitir el acceso al recurso. Para más información, consulte [Creación de un grupo dinámico y comprobación de su estado](#).

También puede ver este breve vídeo, donde encontrará para obtener una explicación rápida sobre cómo crear y usar grupos dinámicos:

- **Asignación de una autoridad externa.** El acceso procede de un origen externo, como un directorio local o una aplicación SaaS. En esta situación, el propietario del recurso asigna al grupo para proporcionar acceso al recurso y, después, el origen externo administra los miembros del grupo.



¿Pueden los usuarios unirse a grupos sin que se les asignen?

El propietario del grupo puede permitir a los usuarios buscar los grupos a los que se van a unir, en lugar de asignarlos. El propietario también puede configurar el grupo para que acepte todos los usuarios que se unan a o para que exija aprobación.

Cuando un usuario solicita unirse a un grupo, la solicitud se reenvía al propietario del mismo. Si es necesario, el

propietario puede aprobar la solicitud y se notifica al usuario de la pertenencia al grupo. Sin embargo, si tiene varios propietarios y uno de ellos la rechaza, el usuario recibe una notificación, pero no se agrega al grupo. Para más información e instrucciones acerca de cómo permitir a los usuarios solicitar su unión a grupos, consulte [Configuración de Azure AD para que los usuarios puedan solicitar unirse a grupos](#)

Pasos siguientes

Tras esta introducción a la administración de acceso mediante grupos, empiece a administrar los recursos y aplicaciones.

- [Creación de un grupo y adición de miembros en Azure Active Directory](#) o [Creación y administración de grupos mediante los cmdlets de PowerShell](#)
- [Uso de grupos para asignar acceso a una aplicación SaaS integrada](#)
- [Sincronización de un grupo local con Azure mediante Azure AD Connect](#)

Incorporación o eliminación de usuarios mediante Azure Active Directory

22/07/2020 • 7 minutes to read • [Edit Online](#)

Agregue usuarios nuevos o elimine usuarios existentes desde la organización de Azure Active Directory (Azure AD). Para agregar o eliminar usuarios debe ser administrador de usuarios o administrador de empresa.

Agregar un nuevo usuario

Puede crear un nuevo usuario con el portal de Azure Active Directory.

Para agregar un usuario, siga estos pasos:

1. Inicie sesión en [Azure Portal](#) como administrador de usuarios para la organización.
2. Busque y seleccione *Azure Active Directory* en cualquier página.
3. Seleccione **Usuarios** y, a continuación, seleccione **Nuevo usuario**.

4. En la página **Usuario**, escriba información para este usuario:

- **Nombre**. Necesario. Nombre y apellidos del nuevo usuario. Por ejemplo, *Mary Parker*.
- **Nombre de usuario**. Necesario. Nombre de usuario del nuevo usuario. Por ejemplo, .

La parte del dominio del nombre de usuario debe usar el nombre de dominio predeterminado inicial, *<yourdomainname>.onmicrosoft.com* o un nombre de dominio personalizado, como de *contoso.com*. Para más información sobre cómo crear un nombre de dominio personalizado, consulte [Incorporación del nombre de dominio personalizado mediante el portal de Azure Active Directory](#).

- **Grupos**. Si quiere, puede agregar el usuario a uno o varios de los grupos existentes. También puede agregar el usuario a grupos en un momento posterior. Para más información sobre cómo agregar usuarios a grupos, consulte [Creación de un grupo básico e incorporación de miembros con Azure Active Directory](#).
- **Rol del directorio**. Si necesita permisos administrativos de Azure AD para el usuario, puede agregarlos a un rol de Azure AD. Puede asignar el rol de administrador global al usuario, o uno o

varios de los otros roles de administrador limitados de Azure AD. Para obtener más información sobre la asignación de roles, consulte [Asignación de roles a usuarios](#).

- **Información del trabajo.** Puede agregar más información sobre el usuario aquí o hacerlo más adelante. Para obtener más información sobre cómo agregar información de usuario, vea [How to add or change user profile information](#) (Incorporación o modificación de la información del perfil de usuario).
5. Copie la contraseña generada automáticamente proporcionada en el cuadro de texto **Contraseña**. Deberá proporcionar esta contraseña al usuario para iniciar sesión por primera vez.
6. Seleccione **Crear**.

El usuario se crea y se agrega a la organización de Azure AD.

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 se configura de modo tal que se le permite invitar a otros usuarios, el usuario recibirá una invitación por correo electrónico que debe aceptar para empezar a colaborar. Para más información sobre cómo invitar a usuarios de colaboración B2B, consulte [Invitación a usuarios B2B a Azure Active Directory](#).

Incorporación de un usuario consumidor

Puede haber escenarios en los que desee crear manualmente cuentas de consumidor en el directorio de Azure Active Directory B2C (Azure AD B2C). Para más información sobre cómo crear cuentas de consumidor, consulte [Creación y eliminación de usuarios consumidores en Azure AD B2C](#).

Agregar un nuevo usuario en un entorno híbrido

Si tiene un entorno con Azure Active Directory (nube) y Windows Server Active Directory (local), puede agregar nuevos usuarios mediante la sincronización de los datos de la cuenta de usuario existentes. Para obtener más información sobre los entornos híbridos, consulte [Integración de los directorios locales con Azure Active Directory](#).

Eliminar un usuario

Puede eliminar un usuario existente mediante el portal de Azure Active Directory.

Siga estos pasos para eliminar un usuario:

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador de usuarios para la organización.
2. Busque y seleccione *Azure Active Directory* en cualquier página.
3. Busque y seleccione el usuario que quiere eliminar del inquilino de Azure AD. Por ejemplo, *Mary Parker*.
4. Seleccione **Eliminar usuario**.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. On the left, there's a sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', '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' (which is highlighted with a red box), 'Multi-Factor Authentication', and 'More'. Below these are filters for 'Name' (set to 'Mary') and 'Show' (set to 'All users'). A table lists users: Mary Parker (mary@contoso.com, Member, Azure Active Directory). The 'Delete user' button is located at the top right of the main content area.

El usuario se elimina y ya no aparece en la página **Users - All users** (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. Para más información sobre cómo restaurar un usuario, consulte [Restauración o eliminación de un usuario recientemente eliminado mediante Azure Active Directory](#).

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

NOTE

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

Pasos siguientes

Después de agregar a los usuarios, puede realizar los procesos básicos siguientes:

- [Add or change profile information](#) (Incorporación o modificación de la información del perfil)
- [Asignación de roles a usuarios](#)
- [Creación de un grupo básico e incorporación de miembros](#)
- [Trabajo con usuarios y grupos dinámicos](#)

O bien puede realizar otras tareas de administración de usuarios, como [agregar usuarios invitados de otro directorio](#) o [restaurar un usuario eliminado](#). Para obtener más información acerca de otras acciones disponibles, consulte la [documentación de administración de usuarios en Azure Active Directory](#).

Adición o actualización de la información de perfil de un usuario mediante Azure Active Directory

22/07/2020 • 5 minutes to read • [Edit Online](#)

Agregue información de perfil de usuario, como la imagen de perfil, información específica del trabajo y algunos valores de configuración mediante Azure Active Directory (Azure AD). Para obtener más información acerca de la adición de nuevos usuarios, consulte [cómo agregar o eliminar usuarios en Azure Active Directory](#).

Adiciones o cambios a la información del perfil

Como verá, hay más información disponible en un perfil de usuario que la que puede agregarse durante la creación del usuario. Toda esta información adicional es opcional y se puede agregar según sea necesario para su organización.

Para agregar o cambiar la información del perfil

1. Inicie sesión en [Azure Portal](#) como administrador de usuarios para la organización.
2. Seleccione **Azure Active Directory**, **Usuarios** y, a continuación, seleccione un usuario. Por ejemplo, *Alain Charon*.

Se muestra la página **Alain Charon - Perfil**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, All services, Favorites, and Azure Active Directory. Under Azure Active Directory, it lists Security Center, Cost Management + Billing, and Help + support. The main content area has a breadcrumb trail: Home > Contoso > Users - All users > Alain Charon - Profile. The title bar says "Alain Charon - Profile". Below the title, there are tabs for Manage (selected), Profile, and Activity. The Profile tab shows a circular profile picture with "AC" initials, the name "Alain Charon", and the email "alain@contoso.com". There are three buttons above the activity chart: Edit, Reset password, and Delete. The activity chart shows User Sign-ins (Aug 19, Aug 26, Sep 2, Sep 9) and Group memberships (2). The Activity section includes links for Sign-ins and Audit logs. At the bottom, there's an "Identity edit" section with fields for Name (Alain Charon), First name (Alain), Last name (Charon), User name (alain@contoso.com), and User type (Member).

3. Seleccione **Editar** para agregar o actualizar de forma opcional la información incluida en cada una de las secciones disponibles.

- **Imagen de perfil.** Seleccione una imagen en miniatura para la cuenta de usuario. Esta imagen aparece en Azure Active Directory y en las páginas personales del usuario, tales como la página myapps.microsoft.com.
- **Identidad.** Agregue o actualice un valor de identidad adicional para el usuario como, por ejemplo, el apellido de casada. Puede establecer este nombre de forma independiente de los valores de Nombre y Apellidos. Por ejemplo, podría utilizarlo para incluir iniciales, un nombre de empresa o para cambiar la secuencia de nombres mostrada. En otro ejemplo, para dos usuarios cuyos nombres son "Chris Green", podría utilizar la cadena de identidad para establecer sus nombres como "Chris B. Green" y "Chris R. Green (Contoso)".
- **Información del trabajo.** Agregue cualquier información relacionada con el trabajo, como el puesto, departamento o administrador del usuario.
- **Configuración.** Establezca si el usuario puede iniciar sesión en el inquilino de Azure Active Directory. También puede especificar la ubicación global del usuario.
- **Información de contacto.** Agregue cualquier información de contacto pertinente para el usuario excepto, en algunos usuarios, el teléfono o la información de contacto móvil (solo un administrador global puede actualizar los usuarios con roles de administrador).
- **Información de contacto para la autenticación.** Compruebe esta información para asegurarse de que hay una dirección de correo electrónico y un número de teléfono activos para el usuario. Azure Active Directory usa esta información para comprobar la identidad del usuario durante el inicio de sesión. Solo un administrador global puede actualizar la información de contacto para la autenticación.

4. Seleccione Guardar.

Todos los cambios se guardan para el usuario.

NOTE

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

Pasos siguientes

Después de actualizar los perfiles de los usuarios, puede realizar los siguientes procesos básicos:

- [Adición o eliminación de usuarios](#)
- [Asignación de roles a usuarios](#)
- [Creación de un grupo básico e incorporación de miembros](#)

O bien, puede realizar otras tareas de administración de usuarios, como asignar delegados, usar directivas y compartir cuentas de usuario. Para obtener más información acerca de otras acciones disponibles, consulte la [documentación de administración de usuarios en Azure Active Directory](#).

Restablecimiento de la contraseña de un usuario con Azure Active Directory

22/07/2020 • 3 minutes to read • [Edit Online](#)

Como administrador, puede restablecer la contraseña de un usuario si se olvida la contraseña, si el usuario bloquea su dispositivo o si nunca ha recibido una contraseña.

NOTE

Si el inquilino de Azure AD no es el directorio principal de un usuario, no podrá restablecer su contraseña. Esto significa que si el usuario inicia sesión en su organización mediante una cuenta de otra organización, una cuenta de Microsoft o una cuenta de Google, no podrá restablecer su contraseña.

Si el usuario tiene una fuente de autoridad como Windows Server Active Directory, solo podrá restablecer la contraseña si ha activado la escritura diferida de contraseñas.

Si el usuario tiene una fuente de autoridad como Azure AD externo, no podrá restablecer la contraseña. Solo el usuario, o un administrador en Azure AD externo, puede restablecer la contraseña.

NOTE

Si no es administrador y busca instrucciones acerca de cómo restablecer la contraseña profesional o educativa, consulte [Restablecimiento de la contraseña profesional o educativa](#).

Para restablecer una contraseña

1. Inicie sesión en [Azure Portal](#) como administrador de usuarios o administrador de contraseñas. Para más información acerca de los roles disponibles, consulte [Asignación de roles de administrador en Azure Active Directory](#)
2. Seleccione **Azure Active Directory**, seleccione **Usuarios** y, a continuación, busque y seleccione los usuarios que necesitan del restablecimiento y haga clic en **Restablecer contraseña**.

Se muestra la página **Alain Charon - Perfil** con la opción **Restablecer contraseña**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, All services, Favorites, Dashboard, etc. The main area shows the 'Alain Charon - Profile' page for a user named 'alain@contoso.com'. The 'Profile' tab is selected in the navigation bar. At the top right, there are three buttons: 'Edit', 'Reset password' (which is highlighted with a red box), and 'Delete'. Below these buttons, there's a circular profile picture with 'AC' initials. To the right of the picture, the user's name 'Alain Charon' and email 'alain@contoso.com' are displayed. A chart titled 'User Sign-ins' shows a single peak of 2 sign-ins in September. Below the chart, under the 'Identity' section, there are fields for Name (Alain Charon), First name (---), Last name (---), User name (alain@jflo.pro), User type (Member), Object ID (xxxxxx-xxxx-xxxx-xxxx-xxxxxx), and Source (Azure Active Directory). There are also sections for 'Job info' and 'Department'.

3. En la página Restablecer contraseña, seleccione Restablecer contraseña.

NOTE

Al usar Azure Active Directory, una contraseña temporal se genera automáticamente para el usuario. En cambio cuando se usa Active Directory local, se crea la contraseña del usuario.

4. Copie la contraseña y proporciónela al usuario. El usuario deberá cambiar la contraseña durante el siguiente proceso de inicio de sesión.

NOTE

La contraseña temporal nunca expira. La próxima vez que el usuario inicie sesión, la contraseña seguirá funcionando, sin importar cuánto tiempo haya transcurrido desde que se generó la contraseña temporal.

Pasos siguientes

Después de restablecer la contraseña del usuario, puede realizar los siguientes procesos básicos:

- [Adición o eliminación de usuarios](#)
- [Asignación de roles a usuarios](#)
- [Add or change profile information](#) (Incorporación o modificación de la información del perfil)
- [Creación de un grupo básico e incorporación de miembros](#)

O bien, puede realizar otros escenarios de usuario complejos, como asignar delegados, usar directivas y compartir cuentas de usuario. Para obtener más información acerca de otras acciones disponibles, consulte la [documentación de administración de usuarios en Azure Active Directory](#).

Asignación de roles de administrador y de no administrador a usuarios con Azure Active Directory

22/07/2020 • 3 minutes to read • [Edit Online](#)

Si un usuario de su organización necesita permiso para administrar recursos de Azure Active Directory (Azure AD), debe asignar al usuario un rol adecuado en Azure AD, en función de las acciones para las que el usuario necesita permisos.

Para más información acerca de los roles disponibles, consulte [Asignación de roles de administrador en Azure Active Directory](#). Para obtener información sobre cómo agregar usuarios, consulte [Incorporación de nuevos usuarios a Azure Active Directory](#).

Asignación de roles

Comúnmente, se asignan roles de Azure AD a los usuarios desde la página **Rol de directorio** de un usuario.

También puede asignar roles mediante Privileged Identity Management (PIM). Para obtener más información sobre cómo usar PIM, consulte [Privileged Identity Management](#).

Para asignar un rol a un usuario

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para el directorio.
2. Busque y seleccione **Azure Active Directory**.

Azure Active Directory

Services

All 41 results

- Azure Active Directory
- Activity log
- Azure Cosmos DB
- Azure Database for MySQL servers
- Azure Arc
- Azure Databricks
- Azure DevOps
- Azure Lighthouse
- Azure Migrate
- Azure Sentinel

Resources

No results were found.

Resource Groups

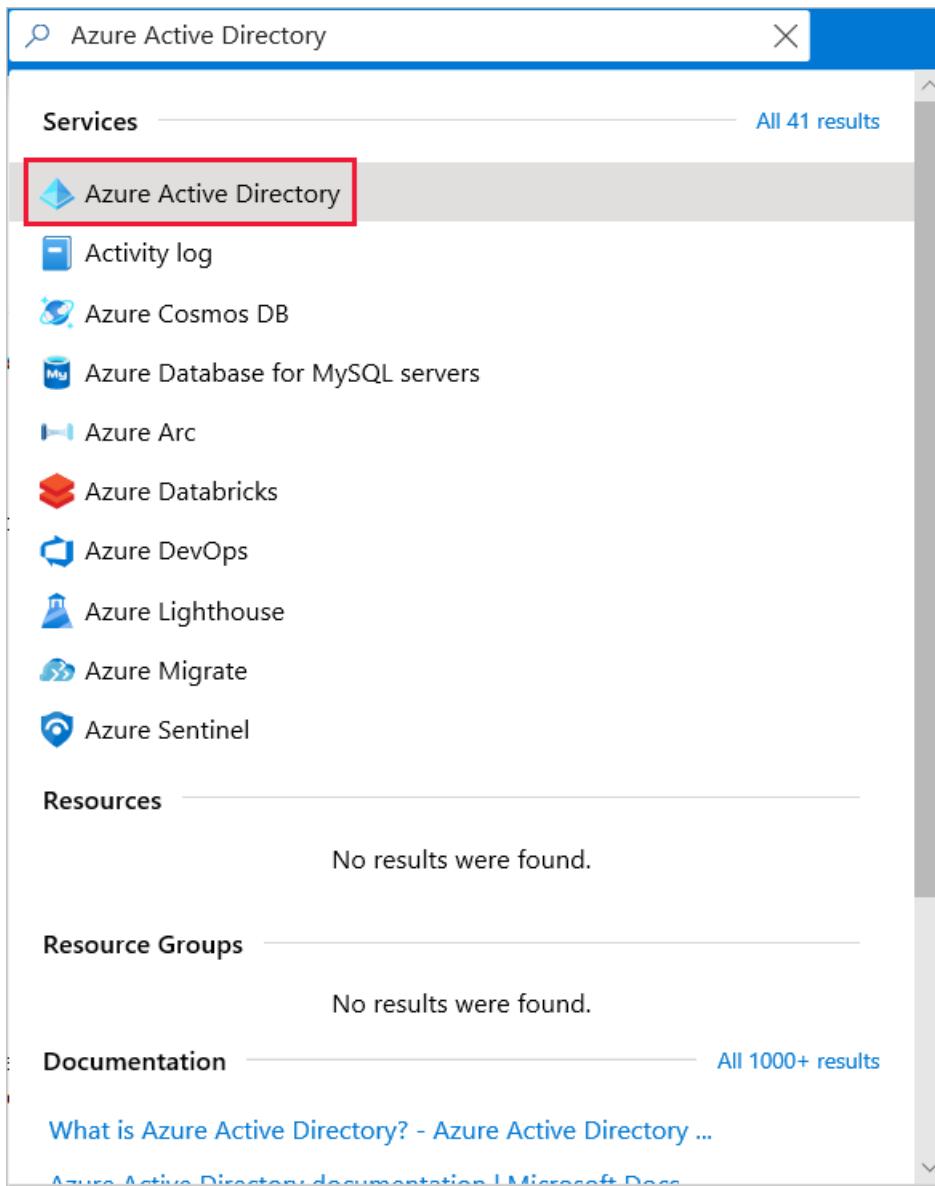
No results were found.

Documentation

All 1000+ results

[What is Azure Active Directory? - Azure Active Directory ...](#)

Azure Active Directory documentation | Microsoft Docs



3. Seleccione Usuarios.

4. Busque y seleccione el usuario que obtiene la asignación de roles. Por ejemplo, *Alain Charon*.

Users - All users

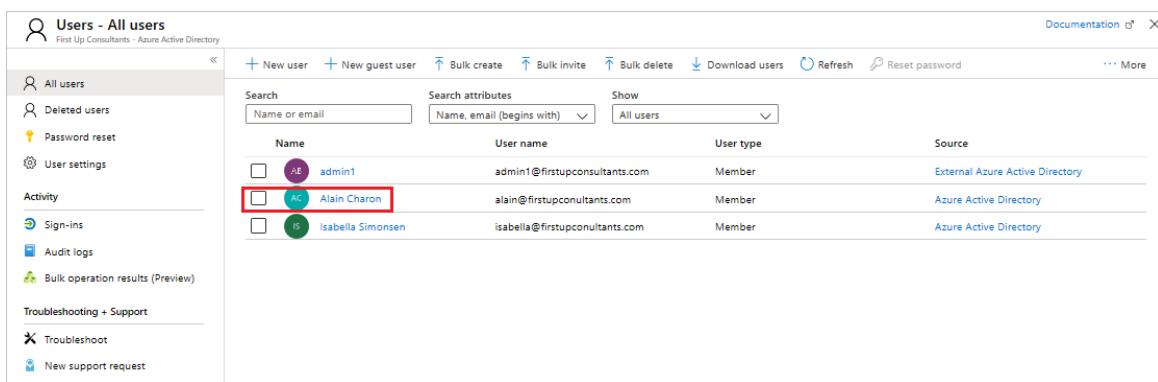
First Up Consultants - Azure Active Directory

Documentation

All users

New user New guest user Bulk create Bulk invite Bulk delete Download users Refresh Reset password More

Name	User name	User type	Source
admin1	admin1@firstupconsultants.com	Member	External Azure Active Directory
Alain Charon	alain@firstupconsultants.com	Member	Azure Active Directory
Isabella Simonsen	isabella@firstupconsultants.com	Member	Azure Active Directory



5. En la página **Alain Charon - Perfil**, seleccione Roles asignados.

Se muestra la página **Alain Charon - Rol de directorio**.

6. Seleccione **Agregar asignación**, seleccione el rol que asignará a Alain (por ejemplo, *Administrador de la aplicación*) y, a continuación, elija **Seleccionar**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like 'Diagnose and solve problems', 'Manage' (with 'Profile' and 'Assigned roles' selected), 'Activity', 'Troubleshooting + Support', etc. The main content area is titled 'Directory roles' and contains a message about needing Azure AD Premium P1 or P2 to assign custom roles. It has a search bar and a table of administrative roles. One row for 'Application administrator' is selected (indicated by a checked checkbox). At the bottom of the table is a blue 'Add' button.

El rol de administrador de la aplicación se asigna a Alain Charon y se muestra en la página **Alain Charon - Rol de directorio**.

Eliminación de una asignación de rol

Si necesita quitar la asignación de roles de un usuario, también puede hacerlo desde la página **Alain Charon - Rol de directorio**.

Para quitar una asignación de rol a un usuario

1. Seleccione Azure Active Directory, seleccione **Usuarios** y, a continuación, busque y seleccione los usuarios a los que quitará una asignación de roles. Por ejemplo, *Alain Charon*.
2. Seleccione **Roles asignados**, seleccione **Administrador de aplicaciones** y, luego, **Quitar asignación**.

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but with a different focus. The 'Assigned roles' section is highlighted in the sidebar. In the main content area, the 'Remove assignments' button is highlighted with a red box. Below it, the 'Application administrator' role is listed in the table, with its checkbox being unchecked, indicating it's being removed.

El rol de administrador de la aplicación se quita de Alain Charon y ya no se muestra en la página **Alain Charon - Rol de directorio**.

Pasos siguientes

- [Adición o eliminación de usuarios](#)
- [Add or change profile information](#) (Incorporación o modificación de la información del perfil)
- [Adición de usuarios invitados de otro directorio](#)

O bien, puede realizar otras tareas de administración de usuarios, como asignar delegados, usar directivas y compartir cuentas de usuario. Para obtener más información acerca de otras acciones disponibles, consulte la [documentación de administración de usuarios en Azure Active Directory](#).

Asignación o eliminación de licencias en el portal de Azure Active Directory

22/07/2020 • 8 minutes to read • [Edit Online](#)

Muchos servicios de Azure Active Directory (Azure AD) exigen que asigne licencias a cada uno de los usuarios o grupos (y los miembros asociados) para ese servicio. Solo los usuarios con licencias activas podrán acceder y usar los servicios de Azure AD licenciados que presentan este requisito. Las licencias se aplican a cada inquilino y no se transfieren a otros inquilinos.

Planes de licencia disponibles

Hay varios planes de licencia disponibles para el servicio de Azure AD, entre los que se incluyen:

- Azure AD Free
- Azure AD Premium P1
- Azure AD Premium P2

Para obtener información específica acerca de cada plan de licencia y los detalles de licencias asociados, consulte [¿Qué licencia necesito?](#)

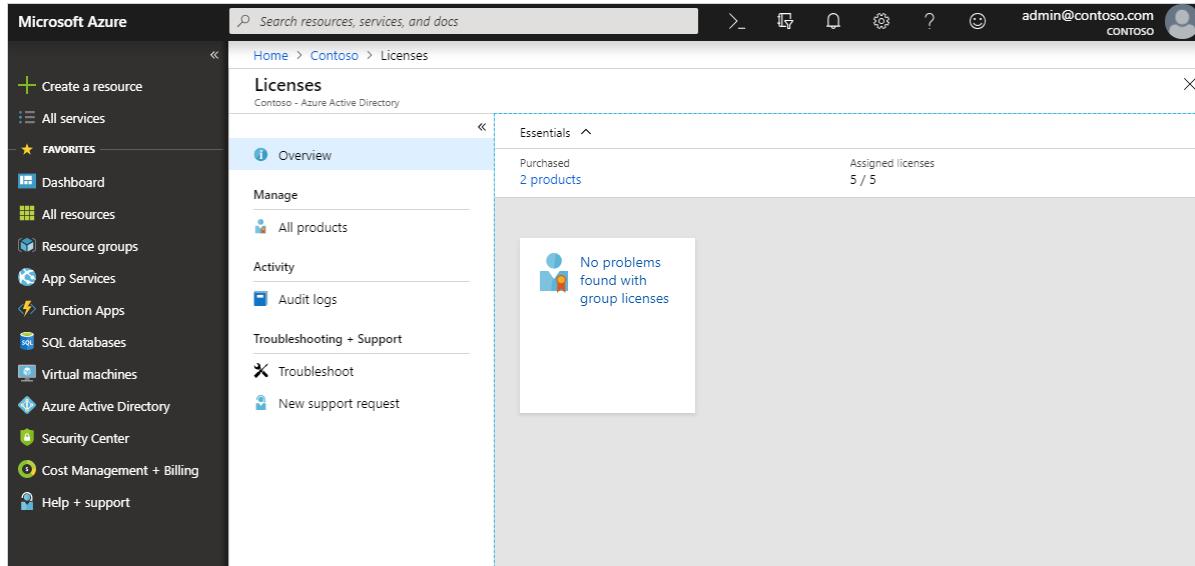
No todos los servicios de Microsoft están disponibles en todas las ubicaciones. Antes de poder asignar una licencia a un grupo, tiene que especificar la **Ubicación de uso** para todos los miembros. Puede establecer este valor en el área **Azure Active Directory > Usuarios > Perfil > Configuración** en Azure AD. Cualquier usuario cuya ubicación de uso no se especifique hereda la ubicación de la organización de Azure AD.

Consulta de los planes de licencia y sus detalles

Puede ver los planes de servicio disponibles —incluidas las licencias individuales—, comprobar las fechas de caducidad pendientes y ver el número de asignaciones disponibles.

Para buscar el plan de servicio y sus detalles

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador de licencias en la organización de Azure AD.
2. Seleccione **Azure Active Directory** y luego seleccione **Licencias**.



3. Seleccione el vínculo **Comprado** para acceder a la página **Productos** y ver los números en **Asignado**, **Disponible** y **Expira próximamente** para los planes de licencias.

NAME	ASSIGNED	AVAILABLE	EXPIRING SOON
Azure Active Directory Premium Plan 1	25	100	0
Azure Active Directory Premium Plan 2	300	0	250

4. Seleccione un nombre de plan para ver sus usuarios y grupos con licencias.

Asignación de licencias a usuarios o grupos

Asegúrese de que cualquier usuario que tenga que usar un servicio de Azure AD licenciado tenga la licencia apropiada. Puede agregar los derechos de licencia a usuarios o a un grupo completo.

Para asignar una licencia a un usuario

1. En la página **Productos**, seleccione el nombre del plan de licencia que quiere asignar al usuario.

NAME	ASSIGNED	AVAILABLE	EXPIRING SOON
Azure Active Directory Premium Plan 1	25	100	0
<input checked="" type="checkbox"/> Azure Active Directory Premium Plan 2	300	0	250

2. En la página de información general del plan de licencia, seleccione **Asignar**.

NAME	USER NAME	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
AC	Alain Charon alain@contoso.com	Active	9/9	Inherited (MDM policy - West)
DM	Danielle McKay danielle@contoso.com	Active	9/9	Inherited (MDM policy - West)
ES	Eggert Schafer eggert@contoso.com	Active	9/9	Inherited (MDM policy - West)

3. En la página **Asignar**, seleccione **Usuarios y grupos** y, luego, busque y seleccione el usuario al que va a asignar la licencia.

The screenshot shows two overlapping windows. On the left is the 'Assign license' window for 'Contoso'. It has a message bar stating 'This feature is currently in public preview'. Below it are sections for 'Users and groups' (set to 'None Selected') and 'Assignment options' (set to 'Assignment options'). At the bottom are 'Assign' and 'Select' buttons. The 'Select' button is highlighted with a red box. On the right is the 'Users and groups' window. It shows a search bar with 'mary' and a result for 'Mary Parker' (mary@contoso.com). Below this is a section titled 'Selected members' showing 'Mary Parker' with an email link and a 'Remove' button. The 'Select' button from the first window is also highlighted with a red box.

4. Seleccione **Opciones de asignación**, asegúrese de tener activadas las opciones de licencia apropiadas y, luego, seleccione **Aceptar**.

This screenshot shows the 'Assign license' window and the 'License options' configuration window side-by-side. The 'Assign license' window shows '2 products selected' and 'Configured' under 'Assignment options'. The 'License options' window lists several services with toggle switches: Enterprise Mobility + Security E3 (On), Azure Active Directory Premium P1 (On), Azure Information Protection Premium P1 (On), Azure Rights Management (On), Cloud App Security Discovery (On), Microsoft Azure Multi-Factor Authentication (On), Microsoft Intune (On), Azure Active Directory Premium P1 (On), and Azure Active Directory Premium P1 (On). The 'Assign' and 'Ok' buttons at the bottom are highlighted with red boxes.

La página **Asignar licencia** se actualiza para mostrar que hay un usuario seleccionado y que las asignaciones están configuradas.

NOTE

No todos los servicios de Microsoft están disponibles en todas las ubicaciones. Antes de poder asignar una licencia a un usuario, tiene que especificar la **Ubicación de uso**. Puede establecer este valor en el área **Azure Active Directory > Usuarios > Perfil > Configuración** en Azure AD. Cualquier usuario cuya ubicación de uso no se especifique hereda la ubicación de la organización de Azure AD.

5. Seleccione **Asignar**.

El usuario se agrega a la lista de usuarios con licencia y tiene acceso a los servicios de Azure AD incluidos.

NOTE

También se pueden asignar licencias directamente a un usuario desde la página **Licencias** del usuario. Si un usuario tiene una licencia asignada a través de una pertenencia a un grupo y quiere asignar la misma licencia directamente al usuario, solo se puede realizar esta acción desde la página **Productos** mencionada en el paso 1.

Para asignar una licencia a un grupo

1. En la página **Productos**, seleccione el nombre del plan de licencia que quiere asignar al usuario.

The screenshot shows the 'Products' section in the Azure portal. It lists two license plans: 'Azure Active Directory Premium Plan 1' and 'Azure Active Directory Premium Plan 2'. The second row, which contains a checked checkbox and the name 'Azure Active Directory Premium Plan 2', is highlighted with a dashed blue border. At the top of the list, there are buttons for 'Try / Buy', 'Assign', and 'Columns'.

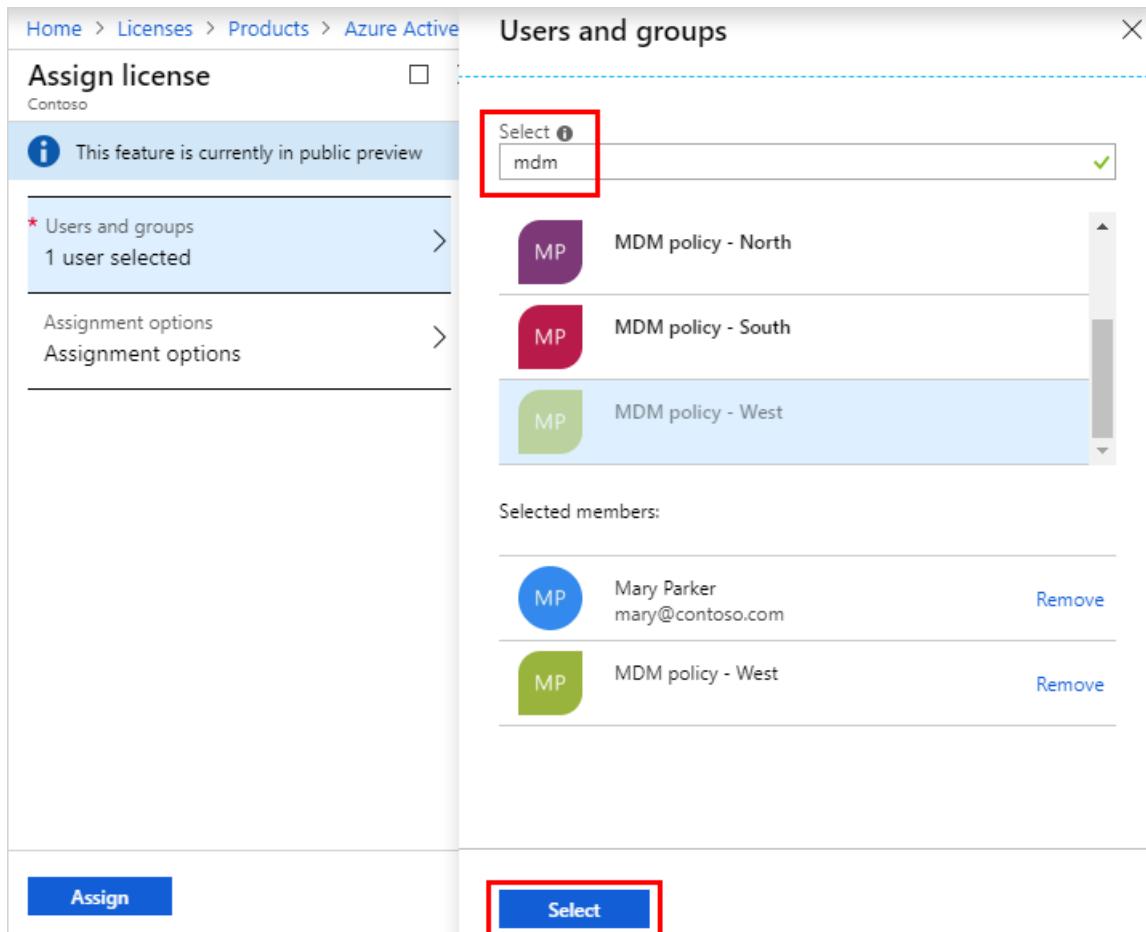
NAME	ASSIGNED	AVAILABLE	EXPIRING SOON
Azure Active Directory Premium Plan 1	25	100	0
Azure Active Directory Premium Plan 2	300	0	250

2. En la página **Azure Active Directory Premium Plan 2**, seleccione **Asignar**.

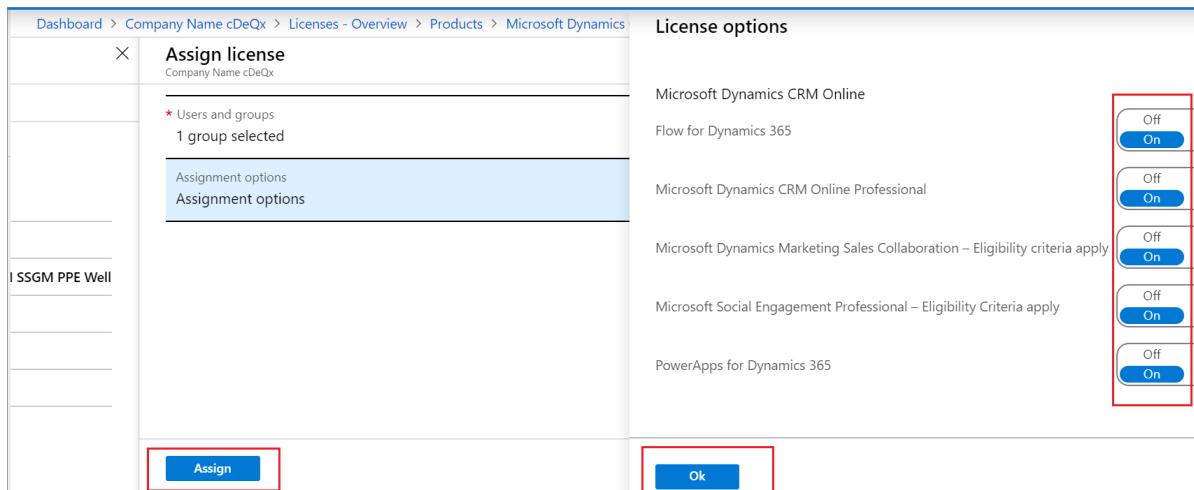
The screenshot shows the 'Azure Active Directory Premium Plan 2 - Licensed users' page. On the left, there's a navigation sidebar with 'General', 'Licensed users' (which is selected and highlighted in blue), and 'Licensed groups'. The main area has a search bar labeled 'Name' and a table of users assigned to the plan. The 'Assign' button at the top of the table is highlighted with a red box.

NAME	USER NAME	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
AC Alain Charon	alain@contoso.com	Active	9/9	Inherited (MDM policy - West)
DM Danielle McKay	danielle@contoso.com	Active	9/9	Inherited (MDM policy - West)
ES Eggert Schafer	eggert@contoso.com	Active	9/9	Inherited (MDM policy - West)

3. En la página **Asignar**, seleccione **Usuarios y grupos** y, luego, busque y seleccione el grupo al que va a asignar la licencia.



4. Seleccione **Opciones de asignación**, asegúrese de tener activadas las opciones de licencia apropiadas y, luego, seleccione **Aceptar**.



La página **Asignar licencia** se actualiza para mostrar que hay un usuario seleccionado y que las asignaciones están configuradas.

5. Seleccione **Asignar**.

El grupo se agrega a la lista de grupos con licencias, y todos los miembros tienen acceso a los servicios de Azure AD incluidos.

Eliminación de una licencia

Puede quitar una licencia desde la página de usuario de Azure AD de un usuario, desde la página general del grupo en una asignación de grupo o empezando desde la página **Licencias** de Azure AD para ver los usuarios y grupos de una licencia.

Para quitar una licencia de un usuario

1. En la página **Usuarios con licencias** para el plan de servicio, seleccione el usuario que ya no debe tener la licencia. Por ejemplo, *Alain Charon*.
2. Seleccione **Quitar licencia**.

NAME	EMAIL	STATE	6/6	Inherit
agilanico	agilar@aad27.ccsctp.net	Active	6/6	Inherit
allochroous	allochthon@aad27.ccsctp.net	Active	6/6	Direct,
almhult	almi@aad27.ccsctp.net	Active	6/6	Inherit
alteration	alteration's@aad27.ccsctp.net	Active	6/6	Inherit
amidases	amidate@aad27.ccsctp.net	Active	6/6	Inherit
anatahan	anatalia@aad27.ccsctp.net	Active	6/6	Inherit
ancientgreymon	ancientism@aad27.ccsctp.net	Active	6/6	Inherit
andrezinho	andrezj@aad27.ccsctp.net	Active	6/6	Inherit
aneurysmatic	aneurusmertomu@aad27.ccsctp.net	Active	6/6	Inherit

IMPORTANT

Las licencias que un usuario hereda de un grupo no se pueden quitar directamente. En su lugar, tiene que quitar el usuario del grupo desde el que haya heredado la licencia.

Para quitar una licencia de un grupo

1. En la página **Grupos con licencias** para el plan de licencia, seleccione el grupo que ya no debe tener la licencia.
2. Seleccione **Quitar licencia**.

NAME	STATE	ENABLED SERVICES
AniGroup	Active	16/17

NOTE

Cuando una cuenta de usuario local sincronizada con Azure AD no está en el ámbito de la sincronización, o si la sincronización se quita, el usuario se eliminará de forma temporal en Azure AD. Cuando esto ocurre, las licencias asignadas directamente a ese usuario o a través de licencias basadas en grupos se marcarán como **suspendidas** en lugar de como **eliminadas**.

Pasos siguientes

Después de haber asignado las licencias, puede seguir los procesos a continuación:

- [Identificación y resolución de problemas de asignación de licencias](#)

- Cómo agregar usuarios a un grupo para obtener licencias
- Escenarios, limitaciones y problemas conocidos del uso de grupos para administrar las licencias en Azure Active Directory
- Add or change profile information (Incorporación o modificación de la información del perfil)

Restauración o eliminación de un usuario recientemente eliminado mediante Azure Active Directory

22/07/2020 • 4 minutes to read • [Edit Online](#)

Después de eliminar a un usuario, la cuenta permanece en estado de suspensión durante 30 días. Durante ese período de 30 días, la cuenta de usuario se puede restaurar, junto con todas sus propiedades. Después de que pase esa ventana de 30 días, el usuario se elimina automáticamente y de forma permanente.

Puede ver a los usuarios que se pueden restaurar, restaurar un usuario eliminado o eliminar permanentemente a un usuario con Azure Active Directory (Azure AD) en Azure Portal.

IMPORTANT

Ni usted ni la asistencia técnica de Microsoft pueden restaurar a un usuario eliminado permanentemente.

Permisos necesarios

Debe tener uno de los roles siguientes para restaurar y eliminar permanentemente a los usuarios.

- Administrador global
- Soporte para asociados de nivel 1
- Soporte para asociados de nivel 2
- Administrador de usuarios

Visualización de los usuarios que se pueden restaurar

Puede ver a todos los usuarios que se eliminaron hace menos de 30 días. Estos usuarios se pueden restaurar.

Para ver a los usuarios que se pueden restaurar

1. Inicie sesión en [Azure Portal](#) con una cuenta de administrador global para la organización.
2. Seleccione **Azure Active Directory**, **Usuarios** y, a continuación, seleccione **Usuarios eliminados**.

Revise la lista de usuarios que están disponibles para restaurar.

NAME	USER NAME	USER TYPE	SOURCE	DELETION DATE	PERMANENT DELETION DATE
Mary Parker	marypa@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM
Rae Huff	rae@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM

Restauración de un usuario recién eliminado

Al eliminarse una cuenta de usuario de la organización, esta está en estado suspendido y se conserva toda la información de la organización relacionada. Cuando se restaura un usuario, también se restaura esta información de la organización.

NOTE

Una vez que se restaura un usuario, también se restauran las licencias que se asignaron al usuario en el momento de la eliminación aunque no haya puestos disponibles para esas licencias. Si a partir de ese momento consume más licencias de las que adquirió, su organización podría incumplir temporalmente todo lo relativo al uso de licencias.

Para restaurar a un usuario

1. En la página **Usuarios - usuarios eliminados**, busque y seleccione uno de los usuarios disponibles. Por ejemplo, *Mary Parker*.
2. Seleccione **Restaurar usuario**.

NAME	USER NAME	USER TYPE	SOURCE	DELETION DATE	PERMANENT DELETION DATE
Mary Parker	marypa@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM
Rae Huff	rae@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM

Eliminar un usuario permanentemente

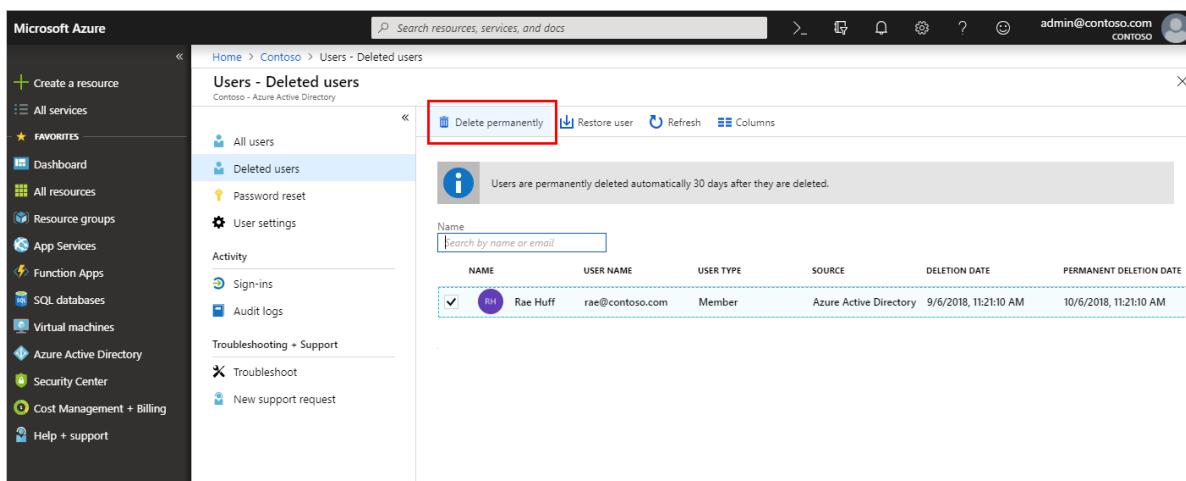
Puede eliminar permanentemente un usuario desde la organización sin esperar a que transcurran los 30 días de la eliminación automática. Ni usted, ni otro administrador, ni la asistencia técnica de Microsoft pueden restaurar a un usuario eliminado permanentemente.

NOTE

Si se elimina permanentemente a un usuario por error, tendrá que crear un nuevo usuario y escribir manualmente toda la información anterior. Para más información acerca de cómo crear un usuario, consulte [cómo agregar o eliminar usuarios](#).

Para eliminar un usuario permanentemente

1. En la página **Usuarios - usuarios eliminados**, busque y seleccione uno de los usuarios disponibles. Por ejemplo, *Rae Huff*.
2. Seleccione **Eliminar permanentemente**.



The screenshot shows the Microsoft Azure portal interface. On the left is the classic navigation menu. The main area shows the 'Deleted users' section under 'Users'. At the top, there are buttons for 'Delete permanently', 'Restore user', 'Refresh', and 'Columns'. A tooltip message states: 'Users are permanently deleted automatically 30 days after they are deleted.' Below this is a search bar and a table with columns: NAME, USER NAME, USER TYPE, SOURCE, DELETION DATE, and PERMANENT DELETION DATE. A single row is selected, showing 'Rae Huff' as the name, 'rae@contoso.com' as the user name, 'Member' as the user type, 'Azure Active Directory' as the source, and the deletion date as '9/6/2018, 11:21:10 AM'.

Pasos siguientes

Después de restaurar o eliminar a los usuarios, puede realizar los siguientes procesos básicos:

- [Adición o eliminación de usuarios](#)
- [Asignación de roles a usuarios](#)
- [Add or change profile information](#) (Incorporación o modificación de la información del perfil)
- [Adición de usuarios invitados de otra organización](#)

Para obtener más información acerca de otras tareas de administración de usuarios disponibles, consulte la [documentación de administración de usuarios en Azure AD](#).

Instrucciones para buscar ayuda y abrir una incidencia de soporte técnico para Azure Active Directory

22/07/2020 • 5 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](#).

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**.

All services > Microsoft | New support request

Microsoft | New support request

Azure Active Directory

Search (Ctrl+ /) Basics Solutions Details Review + create

Information provided on this tab will be used to further assess your issue and help the support engineer troubleshoot the problem. Verify the contact information before moving to the Review + Create.

PROBLEM DETAILS

When did the problem start? MM/DD/YYYY Enter in local time

* Description Provide additional information about your issue

File upload Select a file

Consent Share diagnostic information ⓘ

SUPPORT METHOD

Support plan Azure Support Plan - Internal

* Severity C - Minimal impact

* Preferred contact method

Contact me later Call me later

Email Phone

<< Previous: Solutions Next: Review + create >>

11. Proporcione la información de contacto y seleccione **Siguiente**.

12. Proporcione su información de contacto y seleccione **Crear**.

Home >

Microsoft | New support request

Azure Active Directory

Search (Ctrl+ /) Basics Solutions Details Review + create

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

Company branding

User settings

Properties

Security

Monitoring

Sign-ins

Audit logs

Provisioning logs (Preview)

Logs

Diagnostic settings

Workbooks

Usage & insights

Troubleshooting + Support

Virtual assistant (Preview)

New support request

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

By clicking "Create" you accept the [terms and conditions](#).

View our [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]

<< Previous: Details Create

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](#)

Preguntas más frecuentes sobre Azure Active Directory

22/07/2020 • 19 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) es una completa solución de identidad como servicio (IDaaS) que abarca todos los aspectos de la identidad, la administración de acceso y la seguridad.

Para más información, consulte [¿Qué es Azure Active Directory?](#)

Acceso a Azure y a Azure Active Directory

P: ¿Por qué veo "No se encontraron suscripciones" cuando intento acceder a Azure AD en Azure Portal?

R: Para acceder a Azure Portal, los usuarios necesitan permiso con una suscripción de Azure. Si no tiene una suscripción de Azure AD o de Office 365 de pago, deberá activar una [cuenta de Azure](#) gratuita o una suscripción de pago.

Para más información, consulte:

- [Asociación de las suscripciones de Azure con Azure Active Directory](#)

P: ¿Cuál es la relación entre Azure AD, Office 365 y Azure?

R: Azure AD ofrece funcionalidades de acceso e identidad comunes a todos los servicios web. Tanto si usa Office 365 como Microsoft Azure, Intune u otros servicios, ya está utilizando Azure AD para habilitar el inicio de sesión y la administración del acceso de todos estos servicios.

Todos los usuarios que están configurados para usar servicios web se definen como cuentas de usuario en una o varias instancias de Azure AD. Puede configurar gratis en estas cuentas las funcionalidades de Azure AD, como el acceso a aplicaciones en la nube.

Los servicios de pago de Azure AD, como Enterprise Mobility + Security, complementan otros servicios web como Office 365 y Microsoft Azure con completas soluciones de administración y seguridad para empresas.

P: ¿Cuáles son las diferencias entre el propietario y el administrador global?

R: De forma predeterminada, a la persona que se suscribe a una suscripción a Azure se le asigna el rol de propietario para los recursos de Azure. Un propietario puede usar una cuenta de Microsoft o una cuenta profesional o educativa del directorio al que está asociada la suscripción a Azure. Este rol tiene autorización para administrar servicios en Azure Portal.

Si otros usuarios necesitan iniciar sesión y acceder a los servicios con la misma suscripción, puede asignarles el [rol integrado](#) adecuado. Para obtener información adicional, consulte [Administración del acceso mediante RBAC y Azure Portal](#).

De forma predeterminada, a la persona que se suscribe a una suscripción a Azure se le asigna el rol de administrador global para el directorio. El administrador global tiene acceso a todas las características del directorio de Azure AD. Azure AD tiene un conjunto diferente de roles de administrador para gestionar las características relacionadas con la identidad y el directorio. Estos administradores tendrán acceso a varias características de Azure Portal. El rol de administrador determina qué puede hacer, como crear o editar usuarios, asignar roles administrativos a otros, restablecer contraseñas de usuario, administrar licencias de usuario o administrar

dominios. Para obtener más información sobre los administradores de directorios de Azure AD y sus roles, consulte [Asignación de un usuario a roles de administrador en Azure Active Directory](#) y [Asignación de roles de administrador en Azure Active Directory](#).

Además, los servicios de pago de Azure AD, como Enterprise Mobility + Security, complementan otros servicios web como Office 365 y Microsoft Azure con completas soluciones de administración y seguridad para empresas.

P: ¿Existe un informe que muestra cuándo expirarán mis licencias de usuario de Azure AD?

R: No. No está disponible actualmente.

Introducción a Azure AD híbrido

P: ¿Cómo dejo un inquilino cuando se me ha agregado como colaborador?

R: Cuando se agrega a otro inquilino de la organización como colaborador, puede usar el "cambio de inquilino" de la esquina superior derecha para cambiar entre los inquilinos. Actualmente, no hay forma de abandonar la organización que invita y Microsoft está trabajando para proporcionar esta funcionalidad. Hasta que esta característica esté disponible, puede pedir a la organización que invita que le quite de su inquilino.

P: ¿Cómo conecto mi directorio local a Azure AD?

R: Puede conectar su directorio local a Azure AD mediante Azure AD Connect.

Para más información, consulte [Integración de las identidades locales con Azure Active Directory](#).

P: ¿Cómo se configura el SSO entre mi directorio local y las aplicaciones de nube?

R: Solo es preciso configurar el inicio de sesión único (SSO) entre el directorio local y Azure AD. Mientras tenga acceso a las aplicaciones en la nube mediante Azure AD, el servicio lleva automáticamente a los usuarios a autenticarse correctamente con sus credenciales locales.

La implementación del SSO desde el entorno local se puede lograr fácilmente con soluciones de federación como Active Directory Federation Services (AD FS) o configurando la sincronización de la sincronización de hash de contraseña. Puede implementar fácilmente ambas opciones con el Asistente para configuración de Azure AD Connect.

Para más información, consulte [Integración de las identidades locales con Azure Active Directory](#).

P: ¿Proporciona Azure AD un portal de autoservicio para usuarios en mi organización?

R: Sí, Azure AD proporciona el [panel de acceso de Azure AD](#) para el autoservicio de los usuarios y el acceso a las aplicaciones. Si es cliente de Office 365, encontrará muchas de las mismas funcionalidades en el [portal de Office 365](#).

Para más información, consulte [Introducción al Panel de acceso](#).

P: ¿Me ayuda Azure AD a administrar la infraestructura local?

R: Sí. Azure AD Premium Edition incluye Azure AD Connect Health. Azure AD Connect Health le ayuda a supervisar y a comprender mejor su infraestructura de identidad local y los servicios de sincronización.

Para más información, consulte [Supervisión de la infraestructura de identidad local y los servicios de sincronización en la nube](#).

Administración de contraseñas

P: ¿Puedo usar la escritura diferida de contraseñas de Azure AD sin sincronización de contraseñas?
(En este escenario, ¿se puede usar el restablecimiento de contraseña de autoservicio de Azure AD (SSPR) con la escritura diferida de contraseñas y no almacenar las contraseñas en la nube?)

R: No es necesario sincronizar las contraseñas de Active Directory con Azure AD para habilitar la escritura diferida. En un entorno federado, el inicio de sesión único (SSO) de Azure AD se basa en el directorio local para autenticar al usuario. En este caso no se necesita la contraseña local para realizar el seguimiento en Azure AD.

P: ¿Cuánto se tarda en escribir una contraseña en diferido en Active Directory local?

R: La escritura diferida de contraseñas funciona en tiempo real.

Para más información, consulte [Introducción a la administración de contraseñas](#).

P: ¿Puedo usar la escritura diferida de contraseñas con las que administra un administrador?

R: Sí, si tiene la escritura diferida de contraseñas habilitada, las operaciones de contraseña realizadas por un administrador se escriben de manera diferida en el entorno local.

Para ver más respuestas a preguntas relativas a las contraseñas, consulte [Preguntas más frecuentes sobre la administración de contraseñas](#).

P: ¿Qué hago si no recuerdo mi contraseña de Office 365 o Azure AD cuando intento cambiarla?

R: En este tipo de situaciones, dispone de un par de opciones. Use el restablecimiento de la contraseña de autoservicio (SSPR), si está disponible. El funcionamiento de SSPR dependerá de cómo esté configurado. Para más información, consulte la sección [¿Cómo funciona el portal de restablecimiento de contraseñas?](#)

Para los usuarios de Office 365, el administrador puede restablecer la contraseña mediante los pasos que se describen en [Administradores: restablecer contraseñas de usuario](#).

Para las cuentas de Azure AD, los administradores pueden restablecer las contraseñas mediante uno de los siguientes procedimientos:

- [Restablecimiento de cuentas en Azure Portal](#)
- [Uso de PowerShell](#)

Seguridad

P: ¿Se bloquean las cuentas después de un número determinado de intentos erróneos o se usa una estrategia más sofisticada?

Usamos una estrategia más sofisticada para bloquear cuentas, que se basa en la dirección IP de la solicitud y las contraseñas escritas. El tiempo que dure el bloqueo también aumenta en función de la probabilidad de que sea un ataque.

P: Algunas contraseñas (comunes) se rechazan con mensajes del tipo "esta contraseña se ha usado demasiadas veces". ¿Se refiere esto a las contraseñas usadas en la instancia de Active Directory actual?

Se refiere a las contraseñas que son comunes a nivel global, como las variantes de "Contraseña" y "123456".

P: ¿Se bloqueará una solicitud de inicio de sesión de origen dudoso (botnets, punto de conexión Tor) en un inquilino B2C o se requerirá un inquilino de la edición Básica o Premium?

Tenemos una puerta de enlace que filtra las solicitudes y proporciona alguna protección contra los botnets, y se

aplica a todos los inquilinos B2C.

Acceso a las aplicaciones

P: ¿Dónde puedo encontrar una lista de las aplicaciones preintegradas en Azure AD y sus funcionalidades?

R: Azure AD cuenta con más de 2 600 aplicaciones preintegradas de Microsoft, proveedores de servicios de aplicaciones y asociados. Todas las aplicaciones preintegradas deben ser compatibles con el inicio de sesión único (SSO). El SSO permite utilizar las credenciales de su organización para acceder a las aplicaciones. Algunas de las aplicaciones también admiten el aprovisionamiento y el desaprovisionamiento automatizados.

Para ver una lista exhaustiva de las aplicaciones preintegradas, consulte [Active Directory Marketplace](#).

P: ¿Qué ocurre si no encuentro la aplicación que necesito en Marketplace de Azure AD?

R: Con Azure AD Premium puede agregar y configurar cualquier aplicación. Según las funcionalidades de la aplicación y sus preferencias, puede configurar el SSO y el aprovisionamiento automatizado.

Para más información, consulte:

- [Configuración del inicio de sesión único en aplicaciones que no están en la Galería de aplicaciones de Azure Active Directory](#)
- [Uso de SCIM para habilitar el aprovisionamiento automático de usuarios y grupos de Azure Active Directory a aplicaciones](#)

P: ¿Cómo inician los usuarios sesión en aplicaciones con Azure AD?

R: Azure AD proporciona varias formas de que los usuarios vean y accedan a sus aplicaciones, como:

- El Panel de acceso de Azure AD
- El iniciador de aplicaciones de Office 365
- Inicio de sesión directo en aplicaciones federadas
- Vínculos profundos a aplicaciones federadas, con contraseña o existentes

Para obtener más información, consulte [Experiencias de usuario final para aplicaciones](#).

P: ¿Cuáles son las distintas formas en que Azure AD permite la autenticación y el inicio de sesión único en aplicaciones?

R: Azure AD admite muchos protocolos estandarizados para la autenticación y la autorización, como SAML 2.0, OpenID Connect, OAuth 2.0 y WS-Federation. Además, Azure AD admite las funcionalidades de inicio de sesión automatizado y de almacenamiento de contraseñas para las aplicaciones que solo sean compatibles con la autenticación basada en formularios.

Para más información, consulte:

- [Escenarios de autenticación para Azure AD](#)
- [Protocolos de autenticación de Active Directory](#)
- [Inicio de sesión único para aplicaciones de Azure AD](#)

P: ¿Puedo agregar aplicaciones que ejecuto de manera local?

R: Azure Active Directory Application Proxy proporciona un acceso fácil y seguro a las aplicaciones web locales que elija. Puede acceder a estas aplicaciones como si se trataran de sus aplicaciones de software como servicio (SaaS) en Azure AD. No se necesita una VPN ni cambiar la infraestructura de red.

Para más información, consulte [Provisión de acceso remoto seguro a aplicaciones locales](#).

P: ¿Cómo requiero la autenticación multifactor para usuarios con acceso a una aplicación determinada?

R: Con el acceso condicional de Azure AD, puede asignar una directiva de acceso única a cada aplicación. En la directiva, puede solicitar la autenticación multifactor siempre o solo cuando los usuarios no estén conectados a la red local.

Para más información, consulte [Protección del acceso a Office 365 y otras aplicaciones conectadas a Azure Active Directory](#).

P: ¿Qué es el aprovisionamiento automático de usuarios para aplicaciones SaaS?

R: Use Azure AD para automatizar la creación, el mantenimiento y la eliminación de identidades de usuario en muchas aplicaciones SaaS en la nube conocidas.

Para más información, consulte [Automatización del aprovisionamiento y desaprovisionamiento de usuarios para aplicaciones SaaS con Azure Active Directory](#)

P: ¿Puedo configurar una conexión LDAP segura con Azure Active Directory?

R: No. Azure AD no admite el protocolo ligero de acceso a directorios (LDAP) o LDAP seguro directamente. Sin embargo, es posible habilitar la instancia de Azure AD Domain Services (Azure AD DS) en el inquilino de Azure AD con grupos de seguridad de red correctamente configurados mediante redes de Azure para lograr conectividad LDAP. Para más información, consulte [Configuración de LDAP seguro para un dominio administrado con Azure Active Directory Domain Services](#).