

Crear, configurar y administrar identidades

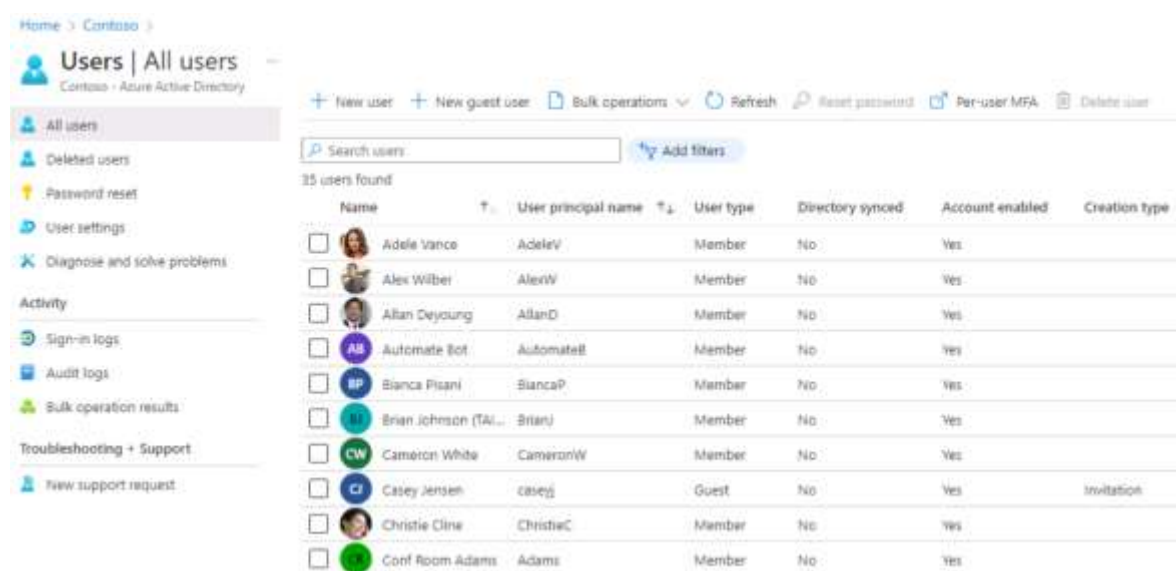
Crear, configurar y administrar usuarios.

Cada usuario que necesita acceso a los recursos de Azure precisa una cuenta de usuario de Azure. Una cuenta de usuario contiene toda la información necesaria para autenticar al usuario durante el proceso de inicio de sesión. Una vez autenticado, Azure AD crea un token de acceso para autorizar al usuario y determinar a qué recursos puede acceder y qué puede hacer con ellos.

Use el panel **Azure Active Directory** en Azure Portal para trabajar con objetos de usuario. Tenga en cuenta que solo se puede trabajar con un único directorio al mismo tiempo, pero puede usar el panel **Directorio + Suscripción** para cambiar de un directorio a otro. En la barra de herramientas del panel también hay un botón **Cambiar directorio** que facilita el cambio a otro directorio disponible.

Visualización de usuarios

Para ver usuarios de Azure AD, seleccione la entrada **Usuarios** en el grupo **Administrar**; se abrirá la vista **Todos los usuarios**. Dedique un minuto a acceder al portal y ver los usuarios. Observe la columna **Tipo de usuario** para ver los miembros y los invitados, como se muestra en la figura siguiente.



Name	User principal name	User type	Directory synced	Account enabled	Creation type
Adele Vance	AdeleV	Member	No	Yes	
Alex Wilber	AlexW	Member	No	Yes	
Allan Deyoung	AllanD	Member	No	Yes	
Automate Bot	AutomateB	Member	No	Yes	
Bianca Pisani	BiancaP	Member	No	Yes	
Brian Johnson (TAI...)	BrianJ	Member	No	Yes	
Cameron White	CameronW	Member	No	Yes	
Casey Jensen	caseyJ	Guest	No	Yes	Invitation
Christie Cline	ChristieC	Member	No	Yes	
Conf Room Adams	Adams	Member	No	Yes	

Normalmente, Azure AD define usuarios de tres maneras:

- **Identidades de nube:** estos usuarios solo existen en Azure AD. Algunos ejemplos son las cuentas de administrador y los usuarios que usted mismo administra. Su origen es **Azure Active Directory** o **Azure Active Directory externo** si el usuario está definido en otra instancia de Azure AD, pero necesita acceso a los recursos de la suscripción controlados por este directorio. Cuando estas cuentas se quitan del directorio principal, se eliminan.

- **Identidades sincronizadas con Directory:** estos usuarios existen en una instancia de Active Directory local. Una actividad de sincronización que se realiza a través de **Azure AD Connect** lleva a estos usuarios a Azure. Su origen es **Windows Server AD**.
- **Usuarios invitados:** estos usuarios se encuentran fuera de Azure. Algunos ejemplos son las cuentas de otros proveedores de nube y cuentas de Microsoft como una cuenta de Xbox LIVE. Su origen es **Usuario invitado**. Este tipo de cuenta es útil cuando los proveedores externos o los contratistas necesitan acceso a los recursos de Azure. Una vez que se puede prescindir de ellos, la cuenta correspondiente y todo el acceso del que disfrutaban se puede quitar.

Ejercicio: Asignar licencias a usuarios

Creación de un usuario en Azure Active Directory

Puede omitir la creación de este usuario si ya creó el mismo en el módulo anterior.

1. Visite [Azure Portal](#) y vaya a la página Azure Active Directory.
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Usuarios**.
3. En el menú de la página Usuarios, seleccione **Nuevo usuario**.
4. Cree un usuario con esta información:

Configuración	Valor
Nombre de usuario	ChrisG
Nombre	Chris Green
Nombre	Chris
Apellido	Verde
Contraseña	creación de una contraseña única

5. Cuando termine, compruebe que la cuenta de Chris Green aparece en la lista **Todos los usuarios**.

Creación de un grupo de seguridad en Azure Active Directory

1. Vaya a la hoja [Azure Active Directory](#).
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Grupos**.
3. En el menú de la hoja Grupos, seleccione **Nuevo grupo**.
4. Cree un grupo con esta información:

Configuración	Valor
Tipo de grupo	Seguridad

Configuración	Valor
Nombre del grupo	Marketing
Tipo de pertenencia	Asignada
Propietarios	Asigne su propia cuenta de administrador como propietario del grupo
Members	Chris Green

Inicio > Contoso > Grupos >

Nuevo grupo

Tipo de grupo * ⓘ
Seguridad

Nombre de grupo * ⓘ
Marketing

Descripción del grupo ⓘ
Se trata de un nuevo grupo de marketing como laboratorio para el curso SC-300

Los roles de Azure AD se pueden asignar al grupo ⓘ
☐ Sí ☒ No

Tipo de pertenencia * ⓘ
Asignado

Propietarios
No se ha seleccionado ningún propietario

Miembros
No hay miembros seleccionados

[Crear](#)

Agregar miembros

Búsqueda ⓘ
Chris

Chris Green
CG
ChrisG
Seleccionado

Christie Cline
ChristieC

Elementos seleccionados

CG Chris Green
ChrisG

[Eliminar](#)

[Select](#)

-
-
-
-
-
6. Cuando termine, compruebe que el grupo denominado **Marketing** aparece en la lista **Todos los grupos**.

Asignación de una licencia a un grupo

1. En la lista **Todos los grupos**, seleccione **Marketing**.
2. En la hoja Marketing, en **Administrar**, seleccione **Licencias**.
3. En el menú, seleccione **Asignaciones**.
4. En la hoja Actualizar asignaciones de licencia, en **Seleccionar licencias**, revise la lista de licencias disponibles y, a continuación, active la casilla de una de las licencias.

5. En las opciones de **Revisar licencia**, revise las opciones disponibles para la licencia que seleccionó; Cuando se seleccionan varias licencias, puede usar el menú de opciones de Revisar licencia para seleccionar una licencia específica y ver la opción de licencia para esta.

[Inicio](#) > [Contoso](#) > [Grupos](#) > [Marketing](#) >

Actualizar asignaciones de licencia

Seleccionar licencias

☐ Dynamics 365 Business Central for I/Es

☐ Dynamics 365 for Talent

☐ Enterprise Mobility + Security E5

☐ Microsoft 365 E5

☐ Microsoft 365 E5 Insider Risk Management

☐ Evaluación de usuario de Microsoft Dynamics AX7

☒ Office 365 E5

☒ Windows 10 Enterprise E3

Revisar opciones de licencia

Office 365 E5

Seleccionar

Office 365 E5

Windows 10 Enterprise E3

☒ Graph Connectors Search with Index

☒ Power Virtual Agents for Office 365

☒ Common Data Service for Teams

☒ Project for Office (Plan E5)

☒ Microsoft Excel Advanced Analytics

☒ Microsoft 365 Defender

☒ Common Data Service

☒ Microsoft Bookings

☒ Administración de registros de Microsoft

☒ Gobernanza de la Información de Microsoft

☒ Investigaciones de datos de Microsoft

☒ Clave de cliente de Microsoft

☒ Microsoft Communications DLP

☒ RETIRADO Microsoft Communications Compliance

☒ Microsoft 365 Advanced Auditing

☒ Information Barriers

☒ Microsoft Kaizala Pro

☒ Premium Encryption in Office 365

☒ Whiteboard (Plan 3)

☒ Information Protection para Office 365: Premium

☒ Information Protection for Office 365: Standard

Guardar

6. Seleccione **Guardar**.

Restauración o eliminación de un usuario recién eliminado con Azure Active Directory

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 proceso de eliminación se inicia de forma automática.

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.

Importante

Ni usted ni la asistencia técnica de Microsoft pueden restaurar a un usuario eliminado permanentemente.

Permisos necesarios

Si desea restaurar usuarios eliminados o quitarlos de manera permanente, debe tener uno de los roles siguientes:

- Administrador global
- Soporte para asociados de nivel 1
- Soporte para asociados de nivel 2
- Administrador de usuarios

Eliminación de un usuario de Azure Active Directory

1. En Azure Portal, vaya a [Azure Active Directory](#).
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Usuarios**.
3. En la lista **Usuarios**, active la casilla correspondiente al usuario que se va a eliminar. Por ejemplo, seleccione **Chris Green**.

Sugerencia

Seleccionar usuarios en la lista le permite administrar varios usuarios al mismo tiempo. Si selecciona un usuario y desea abrir la página de ese usuario, solo administrará a ese

usuario.

Home > Contoso >

Users | All users









Contoso - Azure Active Directory

«

+ New user + New guest

Search users

35 users found

	Name	↑↓
<input type="checkbox"/>	 Adele Vance	
<input checked="" type="checkbox"/>	 Alex Wilber	
<input type="checkbox"/>	 Allan Deyoung	
<input type="checkbox"/>	 AB Automate Bot	
<input type="checkbox"/>	 BP Bianca Pisani	
<input type="checkbox"/>	 BJ Brian Johnson (TAI...	
<input type="checkbox"/>	 CW Cameron White	
<input type="checkbox"/>	 CG Chris Green	

Activity

- Sign-in logs
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

4. Con la cuenta de usuario seleccionada, seleccione **Eliminar usuario** en el menú.
5. Revise el cuadro de diálogo y, luego, seleccione **Aceptar**.

Restaurar un usuario eliminado

Puede ver a todos los usuarios que se eliminaron hace menos de 30 días. Estos usuarios se pueden restaurar.

1. En la página Usuarios, en el panel de navegación izquierdo, seleccione **Usuarios eliminados**.
2. Revise la lista de usuarios eliminados y seleccione el que acaba de eliminar.

Importante

De manera predeterminada, las cuentas de usuario eliminadas se quitan permanentemente de Azure Active Directory de manera automática después de 30 días.

3. En el menú, seleccione **Restaurar usuario**.
4. Revise el cuadro de diálogo y, luego, seleccione **Aceptar**.
5. En el menú de navegación izquierdo, seleccione **Todos los usuarios**.
6. Compruebe que se restauró el usuario.

Crear, configurar y administrar grupos.

Un grupo de Azure Active Directory (Azure AD) ayuda a organizar a los usuarios, lo que facilita la administración de los permisos. 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 a uno. Los grupos permiten definir un límite de seguridad y, después, agregar y quitar usuarios concretos para concederles o denegarles el acceso con una cantidad mínima de esfuerzo. Es más, Azure AD permite definir la pertenencia basada en reglas, como el departamento en el que un usuario trabaja o el puesto que ostenta.

Azure AD permite definir dos tipos de grupos diferentes.

- **Grupos de seguridad:** es el tipo de grupos más común y 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 relativo a una directiva de seguridad específica. De esta forma, puede conceder una serie de permisos a todos los miembros a la vez, en lugar de tener que agregarlos a cada miembro individualmente. Esta opción requiere un administrador de Azure AD.
- **Grupos de Microsoft 365:** brindan oportunidades de colaboración al conceder acceso a los miembros a un buzón compartido, calendarios, archivos, un sitio de SharePoint y mucho más. Esta opción también permite ofrecer acceso al grupo a personas de fuera de la organización. Esta opción está disponible para los usuarios, así como para los administradores. Los grupos de Microsoft 365 a menudo se conocen como grupos de distribución.

Ver grupos disponibles

Todos los grupos se pueden ver a través del elemento **Grupos**, en el grupo **Administrar** del panel de Azure AD. Una instalación de Azure AD nueva no tendrá ningún grupo definido.

Usuarios y grupos -- Todos los grupos

Información general

ADMINISTRAR

Todos los usuarios

Todos los grupos

	NOMBRE	TIPO DE GRUPO	TIPO DE PERTENENCIA
GR	Grupo 1	Seguridad	Asignado
GR	Grupo 2	Seguridad	Asignado
GR	Grupo 23	Seguridad	Asignado

La segunda característica de un grupo que debe tener en cuenta es el **Tipo de pertenencia**. Esto especifica cómo se agregan miembros individuales al grupo. Los dos tipos que existen son los siguientes:

- Asignado: los miembros se agregan y mantienen manualmente.
- Dinámico: los miembros se agregan en función de las reglas y crean un grupo dinámico. Estos grupos siguen siendo un grupo de seguridad o de Microsoft 365, solo que a sus miembros los controla una regla.

Grupos dinámicos

El tipo de grupo final es un grupo dinámico, que el nombre implica, la pertenencia se genera mediante una fórmula cada vez que se usa el grupo. Un grupo de distribución dinámico incluye cualquier destinatario en Active Directory con valores de atributo que coincidan con su filtro. Si las propiedades de un destinatario se modifican para que coincidan con el filtro, el destinatario podría convertirse involuntariamente en miembro del grupo y empezar a recibir los mensajes que se envían al grupo. Los procesos de aprovisionamiento de cuentas coherentes y bien definidos reducirán las posibilidades de que se produzca este problema.

Reglas de pertenencia dinámica ✕

[m Guardar](#)
[✕ Descargar](#)
[🗨 Tiene algún comentario?](#)

Configurar reglas

Puede usar el generador de reglas o el cuadro de texto de sintaxis de regla para crear o editar una regla de pertenencia.

Y/O	Propiedad	Operador	Valor	
Y	<Elegir una propiedad>	< Elija un operad...	Agregar un valor	

+ Agregar expresión +[Obtener las propiedades de extensión personalizadas](#)

i Algunos elementos no se pudieron mostrar en el generador de reglas. Más información

Sintaxis de la regla Editar

user.objectid -ne null

Este grupo dinámico constaría de todos los miembros válidos de Azure AD.

Ejercicio: Agregar grupos en Azure Active Directory

Creación de un grupo de Microsoft 365 en Azure Active Directory

1. Visite [Azure Portal](#) y vaya a la página Azure Active Directory.
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Grupos**.
3. En el menú de la hoja Grupos, seleccione **Nuevo grupo**.
4. Cree un grupo con esta información:

Configuración	Valor
Tipo de grupo	Microsoft 365
Nombre del grupo	Northwest Sales
Tipo de pertenencia	Asignada
Propietarios	Asigne su propia cuenta de administrador como propietario del grupo
Members	Asigne a un miembro de este grupo

Nuevo grupo ...

Tipo de grupo * ⓘ
Microsoft 365

Nombre del grupo ⓘ
Northwest Sales

Dirección de correo electrónico ⓘ del grupo
NorthwestSales @<<domain/tenant>>.onmicrosoft.com

Descripción del grupo ⓘ
Escriba una descripción para el grupo

Tipo de pertenencia ⓘ
Asignado

Propietarios
1 propietario seleccionado

Miembros
1 miembro seleccionado

Crear

- 5.
6. Cuando termine, compruebe que el grupo denominado **Northwest Sales** aparece en la lista **Todos los grupos**.
7. Es posible que tenga que actualizar **todos los grupos** un par de veces.

Configuración y administración del registro de dispositivos

Completado 100 XP

- 9 minutos

Con la proliferación de dispositivos de todas las formas y tamaños, así como las opciones que ofrece el concepto Bring Your Own Device (BYOD), los profesionales de TI se enfrentan con dos objetivos más o menos opuestos:

- Permitir que los usuarios finales sean productivos donde sea y cuando sea y en cualquier dispositivo.
- Proteger los recursos de la organización.

Para proteger los recursos, los profesionales de TI deben primero administrar las identidades de los dispositivos. Pueden compilar la identidad del dispositivo con herramientas como Microsoft Intune para garantizar que se respetan las normas de seguridad y cumplimiento.

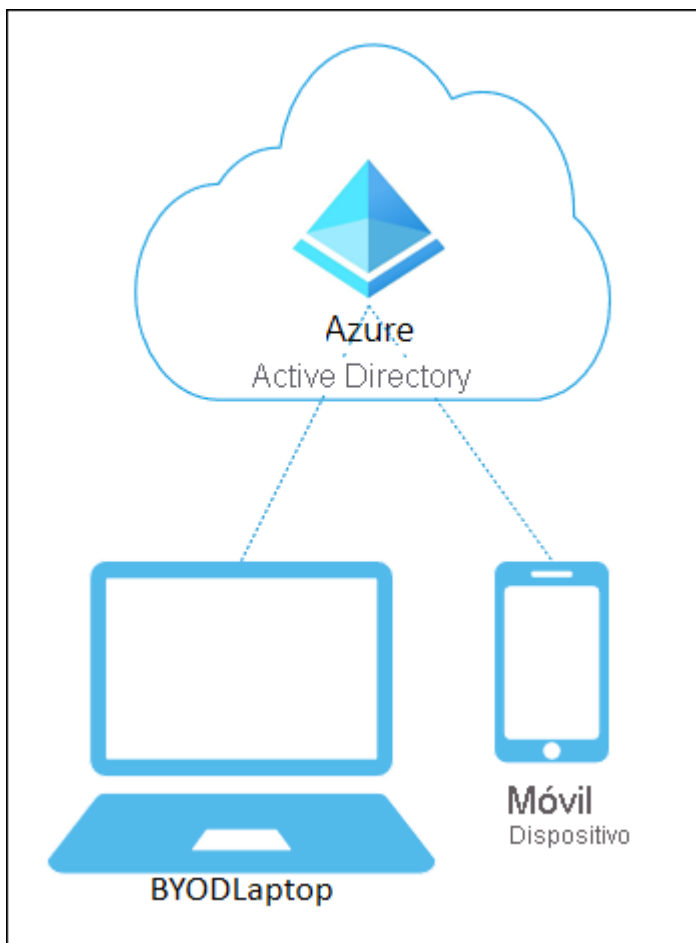
Azure Active Directory (Azure AD) habilita el inicio de sesión único en dispositivos, aplicaciones y servicios desde cualquier ubicación mediante estos dispositivos.

- Los usuarios obtienen acceso a los recursos de la organización que necesitan.
- Los profesionales de TI tienen el control de lo que necesitan proteger en la organización.

Dispositivos registrados en Azure AD

El objetivo de los dispositivos registrados de Azure AD es proporcionar a los usuarios compatibilidad con los escenarios de BYOD o dispositivos móviles. En estos escenarios, el usuario puede acceder a los recursos controlados de Azure Active Directory de la organización con un dispositivo personal.

Registrado en Azure AD	Descripción
Definición	Dispositivos registrados en Azure AD sin necesitar una cuenta de la organización en el dispositivo
Público principal	Aplicable a Bring your own device (BYOD) y dispositivos móviles
Propiedad del dispositivo	Usuario u organización
Sistemas operativos	Windows 10, Windows 11, iOS, Android y macOS
Opciones de inicio de sesión en el dispositivo	Credenciales locales de usuario final, contraseña, Windows Hello, biometría
Administración de dispositivos	Administración de dispositivos móviles (por ejemplo, Microsoft Intune)
Principales capacidades	Inicio de sesión único en recursos en la nube, acceso condicional



Los usuarios inician sesión en los dispositivos registrados en Azure AD con una cuenta local, como una cuenta de Microsoft en un dispositivo Windows 10 pero, además, tienen una cuenta de Azure AD adjunta para acceder a los recursos de la organización. Es posible limitar aún más el acceso a los recursos de la organización en función de esa cuenta de Azure AD y a las directivas de acceso condicional aplicadas a la identidad del dispositivo.

Los administradores pueden proteger y controlar aún más estos dispositivos registrados en Azure AD con herramientas para la Administración de dispositivos móviles (MDM), como Microsoft Intune. MDM proporciona una manera de aplicar las configuraciones que requiere la organización, como el cifrado del almacenamiento, la complejidad de las contraseñas y que el software de seguridad siempre esté actualizado.

El registro en Azure AD se puede realizar al acceder por primera vez a una aplicación de trabajo o si se usa manualmente el menú Configuración de Windows 10.

Escenarios para dispositivos registrados

Un usuario de la organización quiere acceder a herramientas para el correo electrónico, la generación de informes y la inscripción de beneficios desde su equipo doméstico. La organización tiene estas herramientas detrás de una directiva de acceso condicional que requiere acceso desde un dispositivo compatible con Intune. El usuario agrega su cuenta de organización, registra su

equipo doméstico con Azure AD y se aplican las directivas necesarias de Intune, lo que permite que el usuario acceda a sus recursos.

Otro usuario quiere acceder a su correo electrónico de la organización en su teléfono Android personal liberado. Su empresa exige un dispositivo compatible y ha creado una directiva de cumplimiento de Intune para bloquear los dispositivos liberados. El empleado no puede acceder a los recursos de la organización con este dispositivo.

Dispositivos unidos a Azure AD

La unión a Azure AD está pensada para las organizaciones en las que la nube es prioritaria o exclusiva. Cualquier organización puede implementar dispositivos unidos a Azure AD, sin importar tamaño ni sector. La unión a Azure AD habilita el acceso a aplicaciones y recursos de nube y locales.

Unido a Azure AD	Descripción
Definición	Dispositivos unidos solo a Azure AD que requieren una cuenta de la organización para iniciar sesión
Público principal	Adecuado tanto para organizaciones híbridas como para las que solo están en la nube
Propiedad del dispositivo	Organización
Sistemas operativos	Todos los dispositivos con Windows 10 y Windows 11, excepto Windows 10 Home
Administración de dispositivos	Administración de dispositivos móviles (por ejemplo, Microsoft Intune)
Principales capacidades	Inicio de sesión único en recursos locales y en la nube, acceso condicional, autoservicio de recuperación de contraseña y restablecimiento de PIN de Windows Hello

Los dispositivos unidos a Azure AD inician sesión con una cuenta organizativa de Azure AD. Es posible limitar aún más el acceso a los recursos de la organización en función de esa cuenta de Azure AD y a las directivas de acceso condicional aplicadas a la identidad del dispositivo.

Los administradores pueden proteger y controlar aún más los dispositivos unidos a Azure AD con herramientas de administración de dispositivos móviles (MDM), como Microsoft Intune o en escenarios de administración conjunta con Microsoft Endpoint Configuration Manager. Estas herramientas proporcionan una manera de aplicar las configuraciones que requiere la organización, como el cifrado del almacenamiento, la complejidad de las contraseñas y las instalaciones y actualizaciones de software. Los administradores pueden hacer que las aplicaciones de la organización estén disponibles en los dispositivos unidos a Azure AD con Configuration Manager.

La unión a Azure AD se puede lograr mediante opciones de autoservicio, como la configuración rápida (OOBE), la inscripción masiva o Windows Autopilot.

Los dispositivos unidos a Azure AD todavía puede mantener el acceso de inicio de sesión único a los recursos locales cuando están en la red de la organización. Los dispositivos que están unidos a

Azure AD todavía pueden autenticarse en los servidores locales como archivo, impresión y otras aplicaciones.

Escenarios para dispositivos unidos

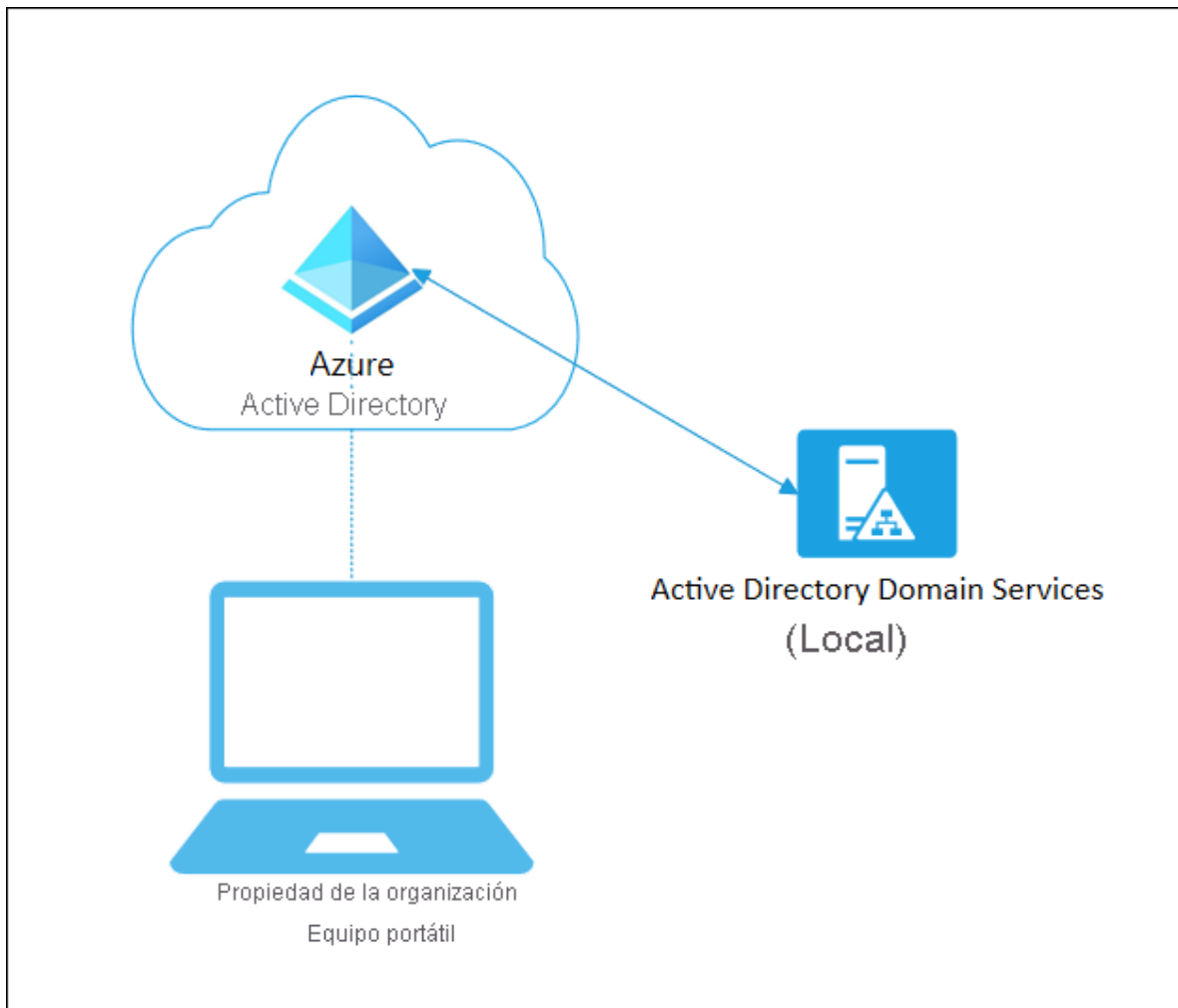
Aunque la unión a Azure AD esté pensada principalmente para aquellas organizaciones que no tengan una infraestructura de Windows Server Active Directory local, sin duda se puede utilizar en escenarios donde:

- Quiere realizar la transición a la infraestructura basada en la nube con Azure AD y un sistema MDM, como Intune.
- No puede usar una unión a un dominio local, por ejemplo, si tiene que controlar dispositivos móviles como tabletas y teléfonos.
- Los usuarios necesitan acceder sobre todo a Microsoft 365 u otras aplicaciones SaaS integradas con Azure AD.
- Desea administrar un grupo de usuarios en Azure AD en lugar de en Active Directory. Este escenario se puede aplicar, por ejemplo, a los trabajadores temporales, contratistas o alumnos.
- Desea proporcionar capacidades de unión a los trabajadores de sucursales remotas con infraestructura local limitada.

Puede configurar dispositivos Unidos a Azure AD para todos los dispositivos con Windows 10, con la excepción de Windows 10 Home.

El objetivo de los dispositivos unidos a Azure AD es simplificar:

- Las implementaciones de Windows de los dispositivos de trabajo
- El acceso a recursos y aplicaciones de la organización desde cualquier dispositivo Windows
- Administración basada en la nube de dispositivos de trabajo
- El inicio de sesión de los usuarios en sus dispositivos con sus cuentas profesionales o educativas de Azure AD o de Active Directory sincronizadas.



La unión a Azure AD se puede implementar mediante diferentes métodos:

Dispositivos híbridos unidos a Azure AD

Durante más de una década, muchas organizaciones han usado la unión a un dominio en su instancia de Active Directory local para permitir:

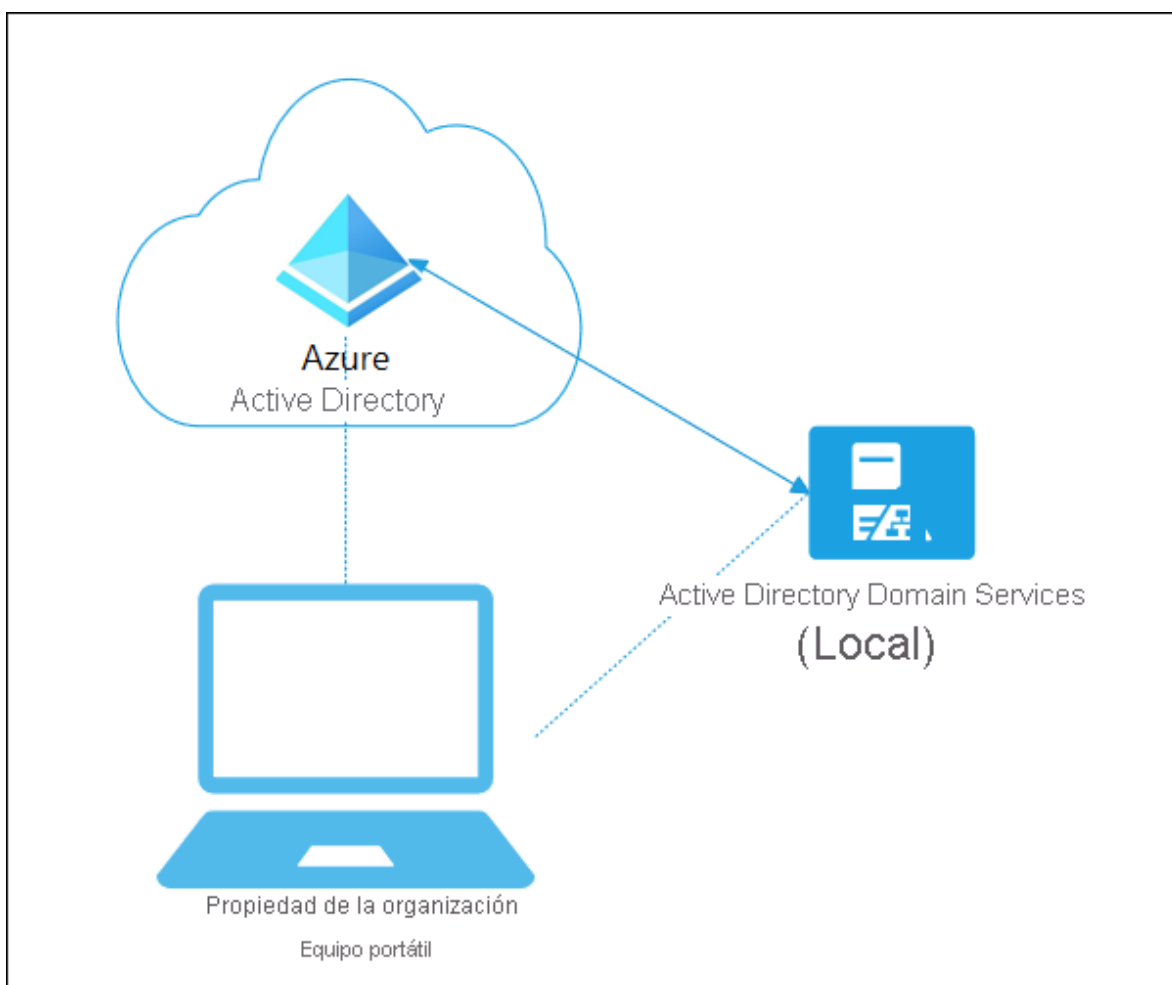
- A los departamentos de TI administrar los dispositivos de empresa desde una ubicación central.
- A los usuarios iniciar sesión en sus dispositivos con sus cuentas profesionales o educativas de Active Directory.

Normalmente, las organizaciones con un uso local confían en los métodos de creación de imágenes para aprovisionar los dispositivos y suelen usar **Configuration Manager** o la **directiva de grupo** para administrarlos.

Si su entorno tiene un uso local de AD y también desea aprovechar las funcionalidades proporcionadas por Azure Active Directory, puede implementar dispositivos híbridos unidos a

Azure AD. Estos dispositivos se han unido a Active Directory local y se han registrado en Azure Active Directory.

Híbrido unido a Azure AD	Descripción
Definición	Dispositivos unidos a AD local y a Azure AD que requieren una cuenta de la organización para el dispositivo
Público principal	Adecuados para organizaciones híbridas con infraestructura de AD local existente
Propiedad del dispositivo	Organización
Sistemas operativos	Windows 11, 10, 8.1 y 7, junto con Windows Server 2008/R2, 2012/R2, 2016 y 2019
Opciones de inicio de sesión en el dispositivo	Contraseña o Windows Hello para empresas
Administración de dispositivos	Política de grupo, administración independiente o conjunta de Configuration Manager
Principales capacidades	Inicio de sesión único en recursos locales y en la nube, acceso condicional, autoservicio de contraseña y restablecimiento de PIN de Windows Hello



Escenarios de unión híbrida

Use dispositivos híbridos unidos a Azure AD si:

- Tiene aplicaciones Win32 implementadas en estos dispositivos que se basan en la autenticación de máquina de Active Directory.
- Quiere seguir usando la directiva de grupo para administrar la configuración del dispositivo.
- Quiere seguir usando las soluciones existentes de creación de imágenes para implementar y configurar dispositivos.
- Además de Windows 10, debe admitir dispositivos de Windows 7 y 8.1 de nivel inferior.

Escritura diferida de dispositivos

En una configuración de Azure AD basada en la nube, los dispositivos solo se registran en Azure AD. Su instancia de AD local no tiene visibilidad de los dispositivos. Esto significa que el acceso condicional en la nube es fácil de configurar y mantener. Sin embargo, en esta sección se describen las configuraciones híbridas con Azure AD Connect. ¿Cómo se realiza el acceso condicional en el entorno local mediante dispositivos si solo existen en Azure AD? La escritura diferida de dispositivos le ayuda a realizar un seguimiento de los dispositivos registrados con Azure AD en AD. Verá una copia de los objetos de dispositivo en el contenedor "Dispositivos registrados".

Escenario: tiene una aplicación a la que desea conceder acceso a los usuarios siempre y cuando estos procedan de dispositivos registrados.

Nube: puede escribir directivas de acceso condicional para cualquier aplicación integrada de Azure AD con el fin de conceder autorizaciones en función de si el dispositivo está unido a Azure AD o no.

Local: esto no es posible sin escritura diferida de dispositivos. Si la aplicación está integrada con ADFS (2012 o superior), puede escribir reglas de notificación para comprobar el estado del dispositivo y, a continuación, proporcionar acceso solo si está presente la notificación que indica que es un dispositivo registrado. Para emitir esta notificación, ADFS comprobará el objeto del dispositivo en el contenedor "Dispositivos registrados" y, a continuación, emitirá la notificación.

Windows Hello para empresas (WHFB) requiere la escritura diferida de dispositivos en escenarios híbridos federados.

Administrar licencias

Los servicios en la nube de pago de Microsoft, como Microsoft 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 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 Microsoft 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 Microsoft 365, Enterprise Mobility + Security y Dynamics 365.

- Las licencias basadas en grupos actualmente solo están disponibles mediante [Azure Portal](#).
- 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.

Algunos servicios de Microsoft no están disponibles en todas las ubicaciones. Antes de asignar una licencia a un usuario, el administrador debe especificar la ubicación de uso en el perfil de usuario.

En el caso de la asignación de licencias de grupo, cualquier usuario sin una ubicación de uso especificada heredarán la ubicación del directorio. Si hay usuarios en varias ubicaciones, se recomienda establecer la ubicación de uso siempre como parte del flujo de creación de usuarios en Azure AD (por ejemplo, mediante la configuración de Azure AD Connect), que garantiza que el resultado de la asignación de licencias siempre es correcto y que los usuarios no reciben los servicios en ubicaciones que no están permitidas.

Ejercicio: Cambiar las asignaciones de licencias de grupo

Cambio de la asignación de licencia de grupo

1. Visite [Azure Portal](#) y vaya a la página Azure Active Directory.
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Grupos**.
3. Seleccione uno de los grupos disponibles. Por ejemplo, Marketing.
4. En el panel de navegación izquierdo, en **Administrar**, seleccione **Licencias**.
5. Revise las asignaciones actuales y, luego, seleccione **+ Asignaciones** en el menú.

Inicio > Contoso > Grupos > Marketing

Marketing | Licencias

Grupo

« **+ Asignaciones** Reprocesar Columnas ¿Tiene algún c...

Información general

Diagnosticar y solucionar problemas

Administrar

- Propiedades
- Miembros
- Propietarios
- Unidades administrativas
- Pertenencia a grupos
- Aplicaciones
- Licencias**
- Asignaciones de roles de Azure

Se aplicaron los cambios de la licencia a todos los usuarios.

Productos
Office 365 E5
Windows 10 Enterprise E3

Nota

Si no tiene licencias para agregar, puede optar por registrarse en una suscripción de prueba de Office 365 o Microsoft 365.

- En la página Actualizar asignaciones de licencia, seleccione otra licencia, desactive la selección de una licencia existente, agregue o quite opciones de licencia o la combinación que prefiera.
- Cuando haya terminado, seleccione **Guardar**.
- Revise el cambio en la página Licencias del grupo.

Identificación y resolución de problemas de asignación de licencias de un grupo en Azure Active Directory

Las licencias basadas en grupos de Azure Active Directory (Azure AD) incorpora el concepto de usuarios en estado de error de licencias. En esta sección, se explican los motivos por los que los usuarios pueden terminar en este estado.

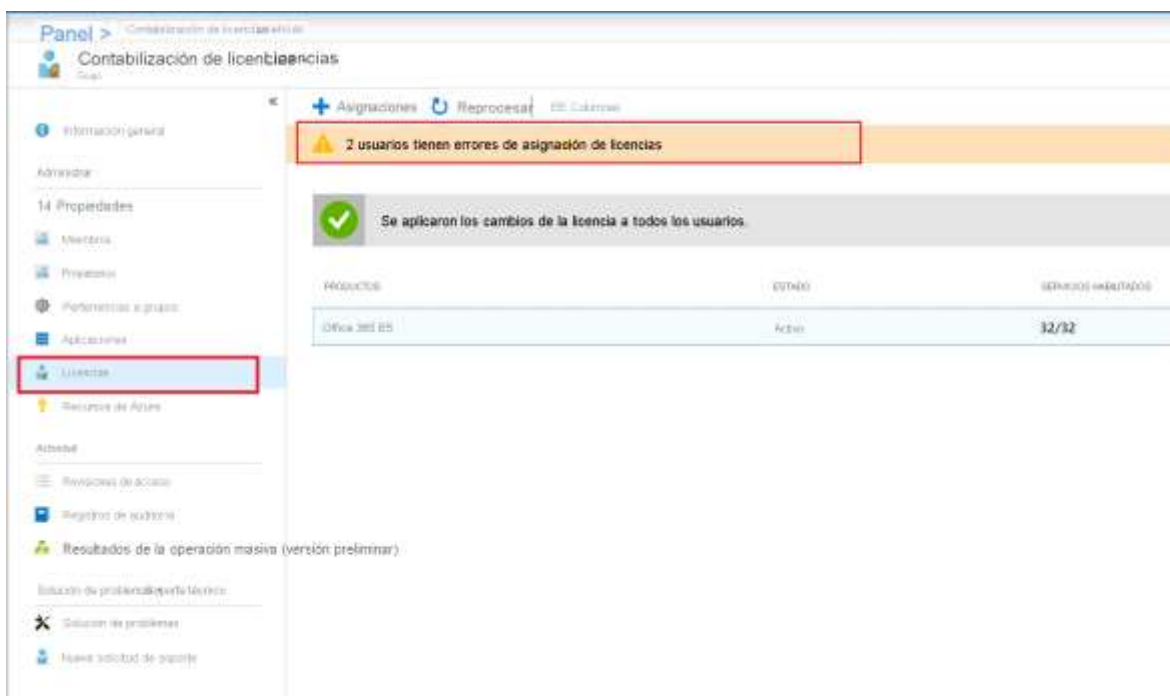
Cuando se asignan licencias directamente a usuarios individuales, sin usar las licencias basadas en grupos, la operación de asignación puede generar errores. Por ejemplo, al ejecutar el cmdlet de PowerShell Set-MsolUserLicense en un sistema del usuario, el cmdlet puede generar un error por diversos motivos relacionados con la lógica de negocios. Por ejemplo, podría haber un número insuficiente de licencias o un conflicto entre dos planes de servicio que no se puedan asignar al mismo tiempo. El problema se le notifica inmediatamente.

Cuando se usan licencias basadas en grupo, se pueden producir los mismos errores, pero ocurren en segundo plano mientras el servicio Azure AD está asignando las licencias. Por este motivo, los errores no se comunican inmediatamente. En su lugar, los errores se registran en el objeto de usuario y se notifican a través del portal de administración. Nunca se pierde la intención original de asignar la licencia al usuario, pero se registra en estado de error a efectos de futuras investigaciones y resoluciones.

Búsqueda de errores de asignación de licencias

Para buscar usuarios con estado de error en un grupo

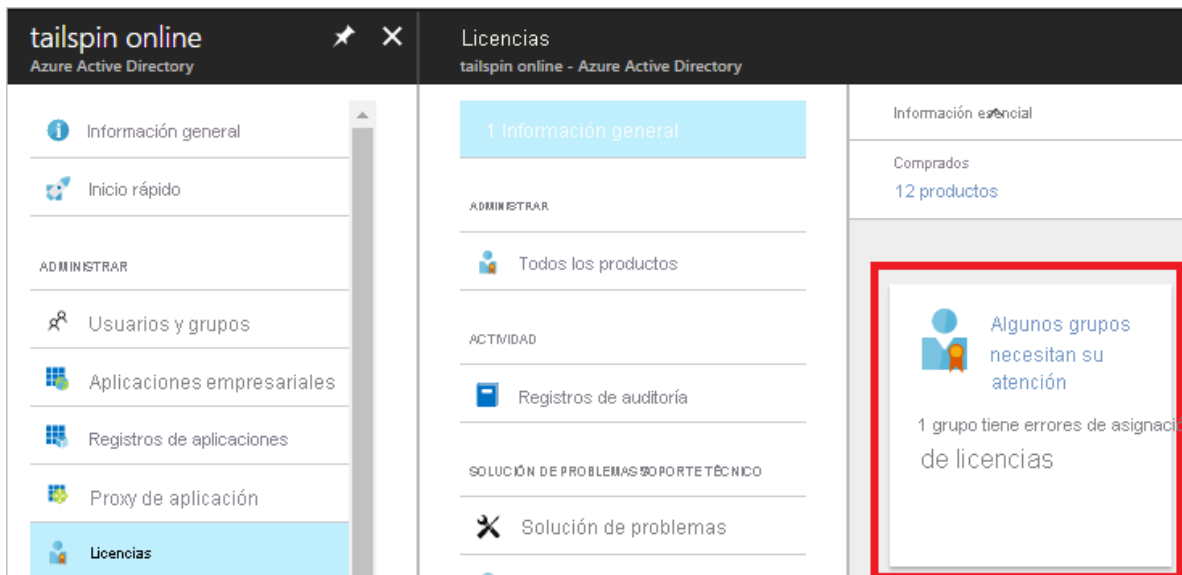
1. Abra el grupo en su página de información general y seleccione **Licencias**. Si hay usuarios con estado de error, aparece una notificación.



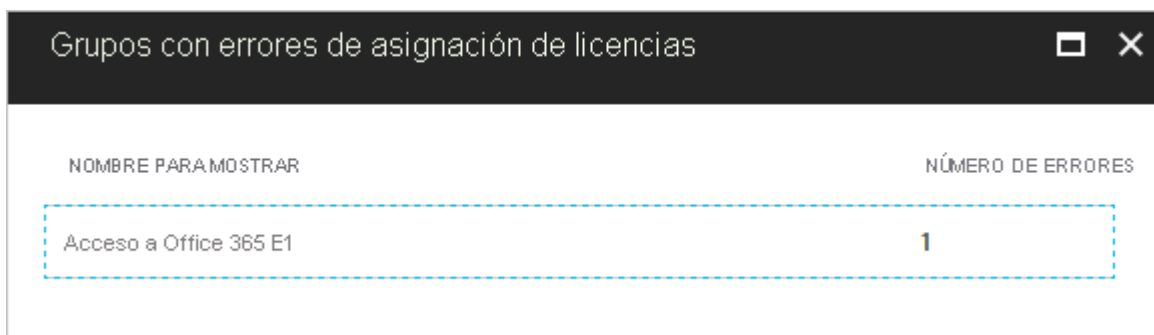
2. Seleccione la notificación para abrir una lista de todos los usuarios afectados. Puede seleccionar individualmente cada usuario para ver más detalles.

Errores de asignación de licencias			
USUARIOS	NOMBRE DE USUARIO	ASIGNACIONES CON ERRORES	MOTIVO PRINCIPAL DEL ERROR
Catherine Gibson	cgibson	1/1	Planes del servicio en conflicto

3. Para buscar todos los grupos que contienen al menos un error, en el menú de la página **Azure Active Directory** seleccione **Licencias** y, a continuación, seleccione **Información general**. Si algunos grupos requieren atención, aparece un cuadro de información.



4. Seleccione el cuadro para ver una lista de todos los grupos con errores. Puede seleccionar cada grupo para más detalles.



En las secciones siguientes se muestran descripciones de cada problema potencial y la manera de resolverlo.

No hay suficientes licencias

Problema: No hay suficientes licencias disponibles para uno de los productos especificados en el grupo. Necesita adquirir más licencias para el producto o liberar las licencias sin usar de otros usuarios o grupos.

Para ver cuántas licencias están disponibles, vaya a **Azure Active Directory**, luego a **Licencias** y, por último, a **Todos los productos**.

Para ver qué usuarios y grupos consumen las licencias, seleccione un producto. En **Usuarios con licencias**, puede ver una lista de todos los usuarios a los que se han asignado licencias directamente o a través de uno o varios grupos. En **Grupos con licencias**, puede ver todos los grupos que tienen ese producto asignado.

PowerShell: los cmdlets de PowerShell informan este error como *CountViolation*.

Planes de servicio en conflicto

Problema: uno de los productos especificados en el grupo contiene un plan de servicio que entra en conflicto con otro plan de servicio que ya está asignado al usuario a través de un producto diferente. Algunos planes de servicio se configuran de tal forma que no puedan asignarse al mismo usuario como otro plan de servicio relacionado.

Considere el ejemplo siguiente. Un usuario tiene una licencia de Office 365 Enterprise *E1* asignada directamente, con todos los planes habilitados. Se ha agregado el usuario a un grupo que tiene asignado el producto Office 365 Enterprise *E3*. El producto *E3* contiene planes de servicio que no pueden superponerse con los planes incluidos en *E1*, por lo que la asignación de licencia de grupo genera el error **Planes de servicio en conflicto**. En este ejemplo, los planes de servicio en conflicto son:

- SharePoint Online (Plan 2) entra en conflicto con SharePoint Online (Plan 1).
- Exchange Online (Plan 2) entra en conflicto con Exchange Online (Plan 1).

Para resolver este conflicto, debe deshabilitar dos de los planes. Puede deshabilitar la licencia de *E1* que se ha asignado directamente al usuario. O bien, debe modificar toda la asignación de licencias de grupo y deshabilitar los planes de la licencia de *E3*. Como alternativa, puede quitar la licencia de *E1* al usuario si es redundante en el contexto de la licencia de *E3*.

El administrador es la única persona competente para decidir cómo resolver el conflicto entre las licencias de productos. Azure AD no resuelve automáticamente los conflictos de licencias.

PowerShell: los cmdlets de PowerShell informan este error como *MutuallyExclusiveViolation*.

Otros productos dependen de esta licencia

Problema: uno de los productos que se especifica en el grupo contiene un plan de servicio que, para funcionar, debe estar habilitado para otro plan de servicio, en otro producto. Este error se produce cuando Azure AD intenta quitar el plan del servicio subyacente. Por ejemplo, esto puede ocurrir cuando se elimina el usuario del grupo.

Para solucionar este problema, debe asegurarse de que el plan necesario todavía está asignado a los usuarios a través de algún otro método o que los servicios dependientes están deshabilitados para esos usuarios. Después, puede quitar correctamente la licencia de grupo a esos usuarios.

PowerShell: los cmdlets de PowerShell informan este error como *DependencyViolation*.

No se permite la ubicación de uso

Problema: algunos servicios de Microsoft no están disponibles en todas las ubicaciones debido a las leyes y los reglamentos locales. Antes de poder asignar una licencia a un usuario, debe especificar la propiedad **Ubicación de uso** para el usuario. Puede especificar la ubicación en la sección **Usuario, Perfil** y luego **Editar** en Azure Portal.

Cuando Azure AD intenta asignar una licencia de grupo a un usuario cuya ubicación de uso no se admite, se produce un error y se registra en el usuario.

Para solucionar este problema, quite del grupo con licencia a los usuarios de las ubicaciones no admitidas. O bien, si los valores de ubicación de uso actual no representan la ubicación de los

usuarios reales, puede modificarlos para que la próxima vez las licencias se asignen correctamente (si se admite la nueva ubicación).

PowerShell: los cmdlets de PowerShell informan este error como *ProhibitedInUsageLocationViolation*.

Nota

Cuando Azure AD asigna licencias de grupo, los usuarios sin ubicación de uso especificada heredan la ubicación del directorio. Se recomienda que los administradores establezcan valores de ubicación de uso correctos en los usuarios antes de utilizar licencias basadas en grupo para cumplir con la normativa y la legislación local.

Direcciones proxy duplicadas

Si usa Exchange Online, es posible que algunos de los usuarios de la organización no estén configurados correctamente con el mismo valor de dirección de proxy. Cuando el sistema de licencias basadas en grupos intenta asignar una licencia a un usuario de este tipo, se produce un error y se muestra un mensaje que indica que la dirección proxy ya está en uso".

Después de resolver cualquier problema de direcciones proxy para los usuarios afectados, asegúrese de forzar el procesamiento de licencias en el grupo para asegurarse de que las licencias ahora se pueden aplicar.

Cambio de los atributos Mail y ProxyAddresses de Azure AD

Problema: al actualizar la asignación de licencias en un grupo o un usuario, es posible que vea que se han cambiado los atributos Mail y ProxyAddresses de Azure AD de algunos usuarios.

Si actualiza la asignación de licencias en un usuario, se desencadenará el cálculo de dirección proxy, lo que puede provocar un cambio en los atributos de usuario.

LicenseAssignmentAttributeConcurrencyException en registros de auditoría

Problema: el usuario tiene LicenseAssignmentAttributeConcurrencyException como asignación de licencia en los registros de auditoría. Cuando la licencia basada en grupos intenta procesar la asignación simultánea de la misma licencia para un usuario, se registra esta excepción en el usuario. Esto suele suceder cuando un usuario es miembro de más de un grupo con la misma licencia asignada. Azure AD reintentará procesar la licencia de usuario y resolverá el problema. No es necesario que el cliente tome ninguna medida para corregir este problema.

Más de una licencia de producto asignada a un grupo

Puede asignar más de una licencia de producto a un grupo. Por ejemplo, puede asignar Office 365 Enterprise E3 y Enterprise Mobility + Security a un grupo para habilitar fácilmente todos los servicios incluidos para los usuarios.

Azure AD intenta asignar todas las licencias especificadas en el grupo a cada usuario. Si Azure AD no puede asignar uno de los productos debido a problemas de lógica de negocio, tampoco asignará las otras licencias del grupo. Un ejemplo se da si no hay suficientes licencias para todos o si hay conflictos con otros servicios que están habilitados en el usuario.

Puede ver los usuarios con los que se han producido errores de asignación y comprobar a qué productos ha afectado esta situación.

Cuando se elimina un grupo con licencia

Debe quitar todas las licencias asignadas a un grupo antes de poder eliminar el grupo. Sin embargo, quitar las licencias de todos los usuarios en el grupo puede llevar tiempo. Pueden producirse errores si el usuario tiene asignada una licencia dependiente. Si un usuario tiene una licencia que depende de una licencia que se va a quitar debido a la eliminación del grupo, la asignación de la licencia para el usuario se convierte de heredada a directa.

Por ejemplo, piense en un grupo que tiene asignado Office 365 E3/E5 con un plan de servicio de Skype Empresarial habilitado. Imagine también que algunos miembros del grupo tienen licencias de Audioconferencia asignadas directamente. Cuando se elimina el grupo, las licencias basadas en el grupo intentarán quitar Office 365 E3/E5 de todos los usuarios. Dado que Audioconferencia depende de Skype Empresarial, para los usuarios con Audioconferencia asignada, las licencias basadas en grupos convierten las licencias de Office 365 E3/E5 a una asignación de licencias directa.

Administración de licencias para productos con requisitos previos

Algunos productos de Microsoft Online que puede tener son *complementos*. Los complementos precisan de un plan de servicio de requisitos previos habilitado para un usuario o un grupo antes de poder asignarles una licencia. Con las licencias basadas en grupos, el sistema requiere que los planes de servicio de requisitos previos y de complementos estén presentes en el mismo grupo a fin de garantizar que los usuarios que se agreguen al grupo puedan recibir el producto totalmente operativo. Vea el siguiente ejemplo:

Microsoft Workplace Analytics es un producto complementario. Contiene un plan de servicio único con el mismo nombre. Este plan de servicio solo se puede asignar a un usuario o grupo cuando uno de los siguientes requisitos previos se asignan también:

- Exchange Online (plan 1)
- Exchange Online (plan 2)

Si se intenta asignar este producto por sí solo a un grupo, el portal devuelve un mensaje de notificación. Al seleccionar los detalles del elemento, se muestra el siguiente mensaje de error:

Se produjo un error en la operación de licencia. Asegúrese de que el grupo tiene los servicios necesarios antes de agregar o quitar un servicio dependiente. **El servicio Microsoft Workplace Analytics necesita que Exchange Online (plan 2) también esté habilitado.**

Para asignar esta licencia de complemento a un grupo, es necesario asegurarse de que el grupo también contiene el plan de servicio de requisitos previos. Por ejemplo, es posible actualizar un grupo existente que ya contenga el producto Office 365 E3 completo y, a continuación, agregar al mismo el complemento.

También es posible crear un grupo independiente que contenga solo los productos mínimos necesarios para que el complemento funcione. Después se puede usar para proporcionar la

licencia del producto complementario solo a los usuarios seleccionados. Según el ejemplo anterior, asignaría los siguientes productos al mismo grupo:

- Office 365 Enterprise E3, solo con el plan de servicio Exchange Online (plan 2) habilitado
- Microsoft Workplace Analytics

De ahora en adelante, cualquier usuario que se agregue a este grupo utiliza una licencia del producto E3 y una licencia del producto Workplace Analytics. Al mismo tiempo, esos usuarios pueden formar parte de otro grupo que les proporcione acceso a todo el producto E3 y solo utilizan una licencia de ese producto.

Sugerencia

Puede crear varios grupos para cada plan de servicio de requisitos previos. Por ejemplo, si los usuarios usan las versiones Office 365 Enterprise E1 y Office 365 Enterprise E3, puede crear dos grupos para proporcionar licencias de Microsoft Workplace Analytics: una con E1 como requisito previo y la otra con E3. Esto le permite distribuir el complemento a los usuarios de E1 y E3 sin tener que usar licencias adicionales.

Forzado del proceso de licencias de grupo para resolver errores

Dependiendo de qué pasos haya dado para resolver los errores, puede ser necesario desencadenar manualmente el procesamiento de un grupo para actualizar el estado del usuario.

Por ejemplo, si libera algunas licencias quitando asignaciones de licencia directas de usuarios, debe desencadenar el procesamiento de grupos con los que anteriormente se produjeron errores por asignar licencias íntegramente a todos los miembros. Para volver a procesar un grupo, vaya al panel del grupo, abra **Licencias** y, a continuación, seleccione el botón **Volver a procesar** en la barra de herramientas.

Forzado del proceso de licencias de usuario para resolver errores

Dependiendo de qué pasos haya dado para resolver los errores, puede ser necesario desencadenar manualmente el procesamiento de un usuario para actualizar el estado del usuario.

Por ejemplo, después de resolver el problema con la dirección proxy duplicada en un usuario afectado, debe desencadenar el procesamiento del usuario. Para volver a procesar un usuario, vaya al panel del usuario, abra **Licencias** y, a continuación, seleccione el botón **Volver a procesar** en la barra de herramientas.

Migración de usuarios con licencias individuales a licencias de grupo

Puede que actualmente tenga licencias implementadas para usuarios de organizaciones mediante una asignación directa; es decir, mediante el uso de scripts de PowerShell u otras herramientas para asignar licencias de usuarios individuales. Antes de empezar a usar licencias basadas en grupos para administrar las licencias de su organización, puede usar este plan de migración para reemplazar con facilidad las soluciones existentes por licencias basadas en grupos.

Tenga en cuenta que debe evitar una situación en la que la migración a licencias basadas en grupos haga que los usuarios pierdan de manera temporal sus licencias actualmente asignadas. Se

debe evitar cualquier proceso que pueda dar lugar a la eliminación de licencias a fin de evitar el riesgo de que los usuarios pierdan el acceso a los servicios y a sus datos.

Proceso de migración recomendado

1. Cuenta actualmente con un sistema de automatización (por ejemplo, PowerShell) que administra la asignación y la retirada de licencias de los usuarios. Deje que se ejecute de la forma habitual.
2. Cree un grupo de licencias nuevo (o decida qué grupos utilizar de entre los existentes) y asegúrese de que todos los usuarios necesarios se agregan como miembros.
3. Asigne las licencias necesarias a esos grupos; el objetivo debe consistir en reflejar el mismo estado de licencia que el sistema de automatización (por ejemplo, PowerShell) aplica a dichos usuarios.
4. Verifique que dichas licencias se hayan aplicado a todos los usuarios de esos grupos. Para ello, compruebe el estado de procesamiento de cada grupo y los registros de auditoría.
 - Puede realizar una comprobación aleatoria de algunos usuarios individuales examinando los detalles de sus licencias. Observará que tienen las mismas licencias asignadas "directamente" o "heredadas" de los grupos.
 - Puede ejecutar un script de PowerShell para [verificar cómo se asignan las licencias a los usuarios](#).
 - Cuando se asigna la misma licencia de producto al usuario directamente y a través de un grupo, el usuario solo puede consumir una licencia. Por lo tanto, no se necesitan licencias adicionales para realizar la migración.
5. Compruebe si en algún grupo de usuarios aparece el estado de error, a fin de verificar que no se produzcan errores en las asignaciones de licencias.

Considere la posibilidad de quitar las asignaciones directas originales. Se recomienda hacerlo gradualmente y supervisar primero el resultado en un subconjunto de usuarios. Puede dejar las asignaciones directas originales de los usuarios pero, en ese caso, cuando el usuario deja los grupos con licencia, conserva las licencias asignadas directamente, y es posible que no sea esto lo que desee.

Un ejemplo

Una organización tiene 1.000 usuarios. Todos los usuarios necesitan licencias de Office 365 Enterprise E3. En la actualidad, la organización tiene un script de PowerShell que se ejecuta a nivel local mediante la adición y eliminación de licencias de usuarios a medida que se incorporan y se van. Pero la organización quiere reemplazar el script con licencias basadas en grupos, de forma que Azure AD administre las licencias automáticamente.

El proceso de migración podría ser similar al siguiente:

1. En Azure Portal, asigne la licencia de Office 365 E3 al grupo **Todos los usuarios** de Azure AD.

2. Confirme que se ha completado la asignación de licencia para todos los usuarios. Vaya a la página de información general del grupo, seleccione **Licencias** y compruebe el estado de procesamiento en la parte superior de la página **Licencias**.
 - Busque "Latest license changes have been applied to all users" (Los últimos cambios de licencia se han aplicado a todos los usuarios) para confirmar que el procesamiento se ha completado.
 - Busque si hay alguna notificación en la parte superior sobre algún usuario cuya licencia no se haya podido asignar correctamente. ¿Se han agotado las licencias para algunos usuarios? ¿Algunos usuarios tienen conflictos de planes de licencia que les impidan heredar las licencias de grupo?
3. Deberá revisar algunos usuarios para verificar que tengan aplicadas tanto licencias directas como de grupo. Vaya a la página de perfil de un usuario, seleccione Licencias y examine el estado de las licencias.
 - Este es el estado de usuario esperado durante la migración:

PRODUCTOS	ESTADO	SERVICIOS HABILITADOS	RUTAS DE ASIGNACIÓN
Azure Active Directory Premium P1	Activo con errores	3/3	Heredado (aad, Todos los usuarios)
Enterprise Mobility + Security E3	Activo	6/6	Directo, heredado (AniGroup, Todos los usuarios)
Microsoft Azure Active Directory Stand...	Activo	2/2	Directo, heredado (Todos los usuarios)
Microsoft Azure Multi-Factor Authentic...	Activo	1/1	Heredado (Todos los usuarios)
Microsoft Dynamics CRM Online	Activo	5/5	Directo
Office 365 E3	Activo	17/17	Directo, Directo, Heredado (AniGroup)
Power BI (gratis)	Activo	1/1	Directo

Nota

Esto confirma que el usuario tiene licencias directas y heredadas. Vemos que se ha asignado Office 365 E3.

Seleccione cada licencia para ver qué servicios están habilitados. Para comprobar que las licencias directas y de grupo habilitan exactamente los mismos servicios para el usuario, seleccione Asignaciones.

4. Después de confirmar que las licencias directas y de grupo son equivalentes, puede empezar a quitar a los usuarios las licencias directas. Para probarlo, quítelos para usuarios individuales en el portal y luego ejecute los scripts de automatización para quitarlos en masa. Este es un ejemplo del mismo usuario con las licencias directas quitadas a través del portal. Tenga en cuenta que el estado de licencia no varía, pero aún no se ven las asignaciones directas.

PRODUCTOS	ESTADO	SERVICIOS HABILITADOS	DETALLES DE ASIGNACIÓN
Azure Active Directory Premium P1	Activo con errores	3/3	Heredado (así, Todos los usuarios)
Enterprise Mobility + Security E3	Activo	6/6	Directo, Heredado (AniGroup, Todos los...
Microsoft Azure Active Directory Standa...	Activo	2/2	Directo, heredado (Todos los usuarios)
Microsoft Azure Multi-Factor Authentic...	Activo	1/1	Heredado (Todos los usuarios)
Microsoft Dynamics CRM Online	Activo	5/5	Directo
Office 365 E3	Activo	17/17	Heredado (AniGroup)
Power BI (gratuito)	Activo	1/1	Directo

Cambio de las asignaciones de licencia de un usuario o grupo en Azure Active Directory

En esta sección, se describe cómo trasladar usuarios y grupos entre planes de licencia de servicio en Azure Active Directory (Azure AD). El enfoque de Azure AD tiene como objetivo asegurarse de que no haya ninguna pérdida de servicio ni de datos durante el cambio de la licencia. Los usuarios deben cambiar entre los servicios sin problemas. Los pasos de la asignación del plan de licencia que aparecen en esta sección describen el cambio de un usuario o grupo en Office 365 E1 a Office 365 E3, pero se aplican a todos los planes de licencia. Al actualizar las asignaciones de licencia de un usuario o grupo, las supresiones de las asignaciones de licencia y las nuevas asignaciones se realizan simultáneamente; de este modo los usuarios no pierden el acceso a sus servicios durante los cambios de licencia ni se producen conflictos de licencia entre planes.

Antes de actualizar las asignaciones de licencia, debe comprobar que se cumplen ciertas suposiciones para todos los usuarios o grupos que se van a actualizar. Si las suposiciones no se cumplen para todos los usuarios de un grupo, se puede producir un error en la migración de alguno de ellos. Como resultado, algunos de los usuarios podrían perder el acceso a servicios o datos. Asegúrese de que:

- Los usuarios tienen el plan de licencia actual que se asigna a un grupo y hereda el usuario, y no uno asignado directamente.
- Dispone de suficientes licencias para el plan de licencia que va a asignar. Si no tiene suficientes licencias, es posible que no se asigne el nuevo plan a algunos usuarios. Puede comprobar el número de licencias disponibles.
- Confirme siempre que los usuarios no tengan otras licencias de servicio asignadas que puedan entrar en conflicto con la licencia deseada o impedir la eliminación de la licencia actual. Por ejemplo, una licencia de un servicio como Workplace Analytics o Project Online, que tienen una dependencia sobre otros servicios.
- Si administra grupos locales y los sincroniza en Azure AD a través de Azure AD Connect, agrega o quita los usuarios mediante su sistema local. Puede que los cambios tarden algún tiempo en sincronizarse con Azure AD para seleccionarlos en las licencias de grupo.

- Si utiliza la pertenencia dinámica a grupos de Azure AD, puede agregar o quitar usuarios cambiando sus atributos, pero el proceso de actualización de las asignaciones de licencia sigue siendo el mismo.

Ejercicio: Cambiar las asignaciones de licencias de usuario

Creación de un usuario en Azure Active Directory

1. Visite [Azure Portal](#) y vaya a la página Azure Active Directory.
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Usuarios**.
3. En el menú de la hoja Usuarios, seleccione **Nuevo usuario**.
4. Cree un usuario con esta información:

Configuración	Valor
Nombre de usuario	DominiqueK
Nombre	Dominique Koch
Nombre	Dominique
Apellido	Koch
Contraseña	Creación de una contraseña única para el usuario
Ubicación de uso	Seleccione la ubicación de uso preferida

5. Advertencia

6. Para asignar una licencia a un usuario, el usuario debe tener asignada una ubicación de uso.
7. Cuando haya terminado, abra Azure AD y haga clic en Usuarios para comprobar que la cuenta de Dominique Koch se muestra en la lista de todos los usuarios.

Actualización de las asignaciones de licencia de usuario

1. Vaya a la hoja [Azure Active Directory](#).
2. En el panel de navegación izquierdo, en **Administrar**, seleccione **Usuarios**.
3. En la hoja Usuarios, seleccione **Dominique Koch**.
4. En el panel de navegación izquierdo, seleccione **Licencias**.
5. En la hoja Actualizar asignaciones de licencia, active la casilla para una o varias licencias.

Actualizar asignaciones de licencia



i Cuando un usuario tiene licencias directas y heredadas y se desactiva la casilla de una licencia, solo se quita la asignación de licencia directa disponible para asignarla o quitarla directamente. El usuario también puede migrarse entre licencias.

Seleccionar licencias

- ☐ Dynamics 365 Business Central for WUs
- ☐ Dynamics 365 for Talent
- ☐ Enterprise Mobility + Security E5
- ☐ Microsoft 365 E5
- ☐ Microsoft 365 E5 Insider Risk Management
- ☐ Evaluación de usuario de Microsoft Dynamics 365
- ☒ Office 365 E5
- ☒ Windows 10 Enterprise E3

Revisar opciones de licencia

Seleccionar

Seleccionar

Office 365 E5

Windows 10 Enterprise E3

☒ Graph Connectors Search with Index

☒ Power Virtual Agents for Office 365

☒ Common Data Service for Teams

☒ Project for Office (Plan E5)

☒ Microsoft Excel Advanced Analytics

☒ Microsoft 365 Defender

☒ Common Data Service

☒ Microsoft Bookings

☒ Administración de registros de Microsoft

☒ Gobernanza de la información de Microsoft

☒ Investigaciones de datos de Microsoft

☒ Clave de cliente de Microsoft

Guardar

6. Cuando haya terminado, seleccione **Guardar**.

Creación de atributos de seguridad personalizados

¿Qué es un atributo de seguridad personalizado?

Los atributos de seguridad personalizados de Azure Active Directory son atributos específicos de la empresa (pares clave-valor) que puede definir y asignar a objetos de Azure AD. Estos atributos se pueden usar para almacenar información, clasificar objetos o aplicar un control de acceso detallado para recursos específicos de Azure.

¿Por qué usar atributos de seguridad personalizados?

- Amplíe los perfiles de usuario; p. ej., agregue la fecha de contratación de los empleados y el salario por hora, para todos los empleados.
- Asegúrese de que solo los administradores pueden ver el atributo de salario por hora en los perfiles de los empleados.
- Clasifique cientos o miles de aplicaciones para crear fácilmente un inventario filtrable para la auditoría.
- Conceda a los usuarios acceso a blobs de Azure Storage que pertenecen a un proyecto.

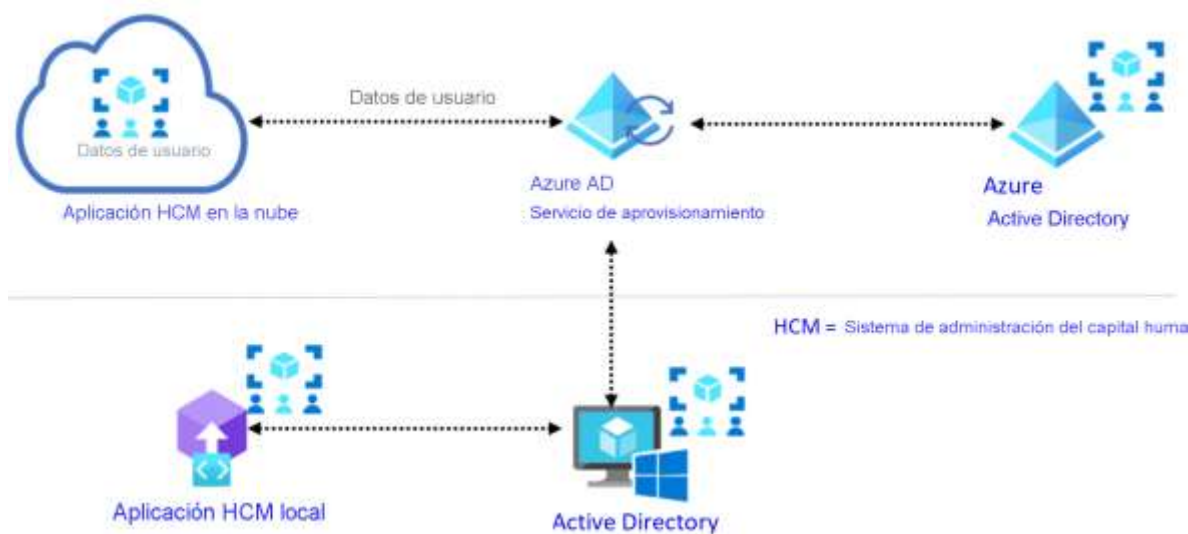
¿Qué puedo hacer con los atributos de seguridad personalizados?

- Defina información específica del negocio (atributos) para el inquilino.
- Agregue un conjunto de atributos de seguridad personalizados para los usuarios, aplicaciones, recursos de Azure AD o recursos de Azure.
- Administre objetos de Azure AD mediante atributos de seguridad personalizados con consultas y filtros.
- Proporcione gobernanza de atributos para que los atributos determinen quién puede obtener acceso.

Características de los atributos de seguridad personalizados

- Están disponibles para todo el inquilino
- Permiten incluir una descripción.
- Admiten distintos tipos de datos: booleanos, enteros, cadenas
- Admiten un valor único o varios valores.
- Admiten valores de formato libre definidos por el usuario o valores predefinidos
- Permiten asignar atributos de seguridad a los usuarios con sincronización de directorios desde un entorno local de Active Directory.

Exploración de la creación automática de usuarios



Componentes del sistema SCIM (sistema de administración de identidades entre dominios)

- **Sistema HCM:** aplicaciones y tecnologías que permiten el proceso y las prácticas de administración de capital humano que admiten y automatizan los procesos de recursos humanos a lo largo del ciclo de vida de los empleados.
- **Servicio de aprovisionamiento de Azure AD:** usa el protocolo SCIM 2.0 para el aprovisionamiento automático. El servicio se conecta al punto de conexión de SCIM para la aplicación y usa el esquema de objetos de usuario SCIM y las API de REST para automatizar el aprovisionamiento y el desaprovisionamiento de usuarios y grupos.
- **Azure AD:** repositorio de usuarios usado para administrar el ciclo de vida de las identidades y sus derechos.
- **Sistema de destino:** aplicación o sistema que tiene el punto de conexión de SCIM y funciona con el aprovisionamiento de Azure AD para habilitar el aprovisionamiento automático de usuarios y grupos.

¿Por qué usar SCIM?

System for Cross-domain Identity Management (SCIM) es un protocolo estándar abierto para automatizar el intercambio de información de la identidad de usuarios entre dominios de identidad y sistemas de TI. SCIM garantiza que se creen automáticamente cuentas en Azure Active Directory (Azure AD) o Windows Server Active Directory para los empleados que se agreguen al sistema de administración de capital humano (HCM). Los atributos y perfiles de usuario se sincronizan entre los dos sistemas, actualizando y eliminando usuarios en función del estado de usuario o el cambio de rol.

La clave es mantener los sistemas de identidad actualizados. Si se puede desaprovisionar automáticamente un usuario de Azure AD tan pronto como se elimine de sus sistemas de recursos humanos, se preocupará menos por una posible infracción.

Comprobación de conocimientos

1. Por lo general, Azure AD define a los usuarios de tres maneras. Dos de estas son las identidades de nube y los usuarios invitados. ¿De qué otra manera define Azure AD a los usuarios?

- ☐ Como usuarios no conectados.
- ☐ Como usuarios de transición.
- ☒ Como identidades sincronizadas con el directorio.

✓ Correcto: Azure AD define a los usuarios como identidades de nube, usuarios invitados y como identidades sincronizadas con el directorio.

2. Las licencias basadas en grupos de Azure AD facilitan la administración a gran escala. Por lo general, ¿cuánto tardan en entrar en vigor las modificaciones de licencia una vez que se modifica la pertenencia a grupos?

- ☐ Dentro del período en que se actualizan los controladores de dominio locales.
- ☒ En cuestión de minutos después de un cambio de pertenencia.

✓ Correcto: las modificaciones de licencia que se generan a partir de los cambios en la pertenencia a grupos suelen entrar en vigor en cuestión de minutos después de un cambio de pertenencia.

- ☐ En un plazo de 24 horas después de un cambio de pertenencia.

3. Azure AD permite la definición de dos tipos de grupos distintos; un tipo son los grupos de seguridad, que se usan para administrar el acceso de los miembros y los equipos equipo a los recursos compartidos. ¿Cuál es el otro tipo de grupo?

- ☐ Grupos de distribución, que se usan con fines de comunicaciones a través de aplicaciones como Teams y Exchange.
- ☐ Grupos de licencias, que se usan para facilitar la administración de las licencias de software.
- ☒ Grupos de Microsoft 365, que proporcionan acceso a buzones compartidos, calendarios, sitios de SharePoint, etc.

✓ Correcto: Azure AD permite la definición de grupos de seguridad y grupos de Microsoft 365.