Implementación de Azure AD Identity Protection

Exploración de Azure AD Identity Protection

Identity Protection es una herramienta que permite a las organizaciones realizar tres tareas clave:

- Automatizar la detección y corrección de riesgos basados en la identidad.
- Investigar los riesgos de usar los datos en el portal.
- Exportar los datos de detección de riesgos a utilidades de terceros para su posterior análisis.

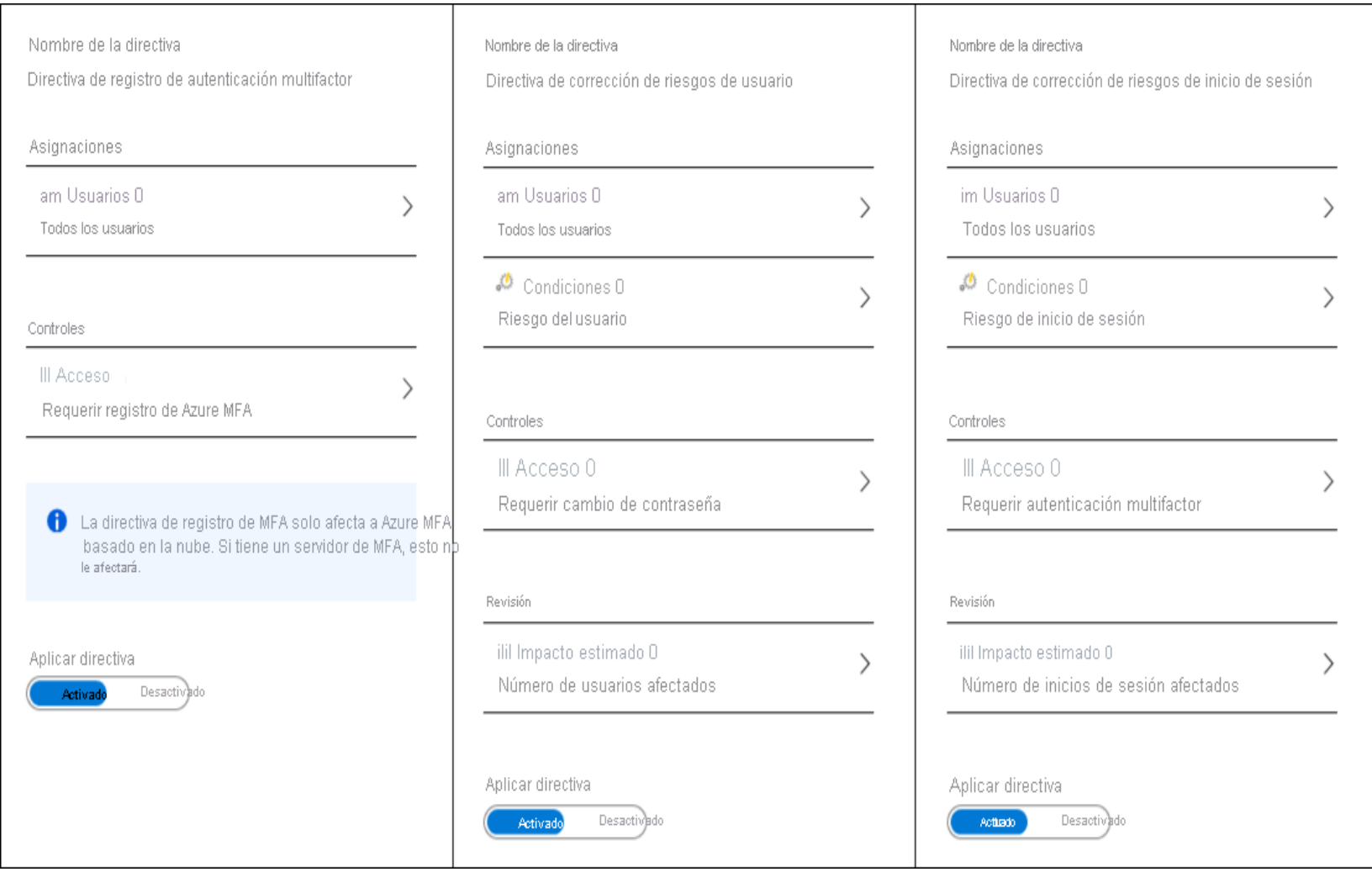
Identity Protection usa los aprendizajes que Microsoft ha adquirido de su puesto en organizaciones con Azure AD, el espacio de consumidor con cuentas de Microsoft y juegos con Xbox para proteger a los usuarios. Microsoft analiza 6,5 billones de señales al día para identificar y proteger a los clientes de las amenazas.

Las detecciones de riesgo en Azure AD Identity Protection incluyen todas las acciones sospechosas identificadas, relacionadas con las cuentas de usuario en el directorio. Las señales con las que se alimenta Identity Protection se pueden insertar en herramientas como Acceso condicional para tomar decisiones de acceso o alimentar una herramienta de información de seguridad y administración de eventos (SIEM) a fin de realizar una investigación más detallada en función de las directivas aplicadas.

Identity Protection proporciona a las organizaciones acceso a recursos eficaces para que puedan responder rápidamente a actividades sospechosas.

Directivas de Identity Protection

Azure Active Directory Identity Protection incluye tres directivas predeterminadas que los administradores pueden optar por habilitar. Estas directivas incluyen una personalización limitada, pero son aplicables a la mayoría de las organizaciones. Todas las directivas permiten excluir a los usuarios, como las cuentas de acceso o administrador de emergencia.



Directiva de registro de Azure MFA

Identity Protection puede ayudar a las organizaciones a implementar Multi-Factor Authentication (MFA) de Azure mediante una directiva de acceso condicional que requiere registro al iniciar sesión. La habilitación de esta directiva es una excelente manera de asegurarse de que los nuevos usuarios de la organización se hayan registrado en MFA el primer día. La autenticación multifactor es uno de los métodos de corrección automática para los eventos de riesgo dentro de Identity Protection. La autocorrección permite a sus usuarios actuar por sí mismos para reducir el volumen de llamadas al servicio de asistencia.

Directiva de riesgo de inicio de sesión

Identity Protection analiza las señales de cada inicio de sesión, tanto en tiempo real como sin conexión, y calcula una puntuación de riesgo en función de la probabilidad de que el usuario no haya realizado el inicio de sesión. Los administradores pueden decidir en función de esta señal de puntuación de riesgo para aplicar los requisitos organizativos. Los administradores pueden elegir bloquear el acceso, permitir el acceso o permitir el acceso pero requerir autenticación multifactor.

Si se detecta un riesgo, los usuarios pueden realizar el proceso de autenticación multifactor para solucionar automáticamente el evento de inicio de sesión peligroso y cerrarlo para evitar ruidos innecesarios para los administradores.

Directiva de acceso condicional personalizada

Los administradores también pueden optar por crear una directiva de acceso condicional personalizada que incluya el riesgo de inicio de sesión como una condición de asignación.

Configuración de detecciones de eventos de riesgo

Para proteger a los usuarios, puede configurar directivas basadas en el riesgo en Azure Active Directory (Azure AD) que respondan automáticamente a comportamientos de riesgo. Las directivas de Azure AD Identity Protection pueden bloquear automáticamente un intento de inicio de sesión o requerir una acción adicional como un cambio de contraseña, o bien solicitar una autenticación multifactor de Azure AD. Estas directivas funcionan con las directivas existentes de acceso condicional de Azure AD como una capa de protección adicional para la organización. Los usuarios podrían no desencadenar nunca un comportamiento de riesgo en una de estas directivas, pero la organización está protegida si se produce un intento de poner en peligro la seguridad.

Cada día, Microsoft recopila y analiza billones de señales anónimas como parte de los intentos de inicio de sesión de usuario. Estas señales ayudan a crear patrones de comportamiento correcto de inicio de sesión de usuario e identifican posibles intentos de inicio de sesión con riesgo. Azure AD Identity Protection puede revisar los intentos de inicio de sesión de los usuarios y tomar medidas adicionales si se produce un comportamiento sospechoso:

Algunas de las acciones siguientes pueden desencadenar la detección de riesgos de Azure AD Identity Protection:

- Usuarios con credenciales filtradas.
- Inicios de sesión desde direcciones IP anónimas.
- Viaje imposible a ubicaciones inusuales.
- Inicios de sesión desde dispositivos infectados.
- Inicios de sesión desde direcciones IP con actividad sospechosa.

Las tres directivas siguientes están disponibles en Azure AD Identity Protection para proteger a los usuarios y responder frente a actividades sospechosas. Puede optar por activar o desactivar la aplicación de directivas, seleccionar los usuarios o grupos a los que se aplicará la directiva y decidir si desea bloquear el acceso en el inicio de sesión o solicitar una acción adicional.

La perspectiva que se obtiene de una detección de riesgos identificada está asociada a su suscripción de Azure AD.

- **Directiva de riesgo de usuario**: identifica y responde a cuentas de usuario que pudieran tener credenciales en peligro. Puede solicitar al usuario que cree una nueva contraseña.

- **Directiva de riesgo de inicio de sesión**: identifica y responde a intentos de inicio de sesión sospechosos. Puede solicitar al usuario que utilice otras formas de verificación mediante Azure AD Multi-Factor Authentication.
- **Directiva de registro de MFA**: comprueba que los usuarios estén registrados en autenticación multifactor de Azure AD. Si una directiva de riesgo de inicio de sesión solicita MFA, el usuario debe estar previamente registrado en Azure AD Multi-Factor Authentication.

Cuando habilita una directiva usuario o de riesgo de inicio de sesión, también puede elegir el umbral para el nivel de riesgo: ***bajo y superiores***, *medio y superiores* o ***alto***. Esta flexibilidad le permite decidir cómo desea que se apliquen los controles a los eventos de inicio de sesión sospechosos.

Implementación de la directiva de riesgo de usuario

Identity Protection puede calcular los niveles normales del comportamiento de un usuario y usarlos para basar las decisiones de su riesgo. El riesgo del usuario es un cálculo de la probabilidad de que se haya puesto en peligro una identidad. Los administradores pueden decidir en función de esta señal de puntuación de riesgo para aplicar los requisitos organizativos. Los administradores pueden elegir bloquear el acceso, permitir el acceso o permitir el acceso pero requerir un cambio de contraseña mediante el autoservicio de restablecimiento de contraseña de Azure AD.

En la imagen anterior se muestra la configuración de la **directiva de riesgo de usuario** aplicada.

- Para inicios de sesión de usuario
- Responder automáticamente en función del nivel de riesgo de un usuario específico
- Proporcionar la condición (nivel de riesgo) y la acción (bloquear o permitir)
- Utilizar un umbral alto durante la implementación de la directiva
- Utilizar un umbral bajo para mayor seguridad

Usuarios de riesgo

Con la información que proporciona el informe de usuarios de riesgo, los administradores pueden buscar lo siguiente:

- ¿Qué usuarios están en riesgo, lo han corregido o lo han descartado?

- Detalles sobre las detecciones
- Historial de todos los inicios de sesión de riesgo
- Historial de riesgos

A continuación, los administradores pueden decidir actuar sobre estos eventos. Los administradores pueden optar por:

- Restablecer la contraseña del usuario
- Confirmar el peligro del usuario
- Descartar el riesgo del usuario
- Bloquear el inicio de sesión del usuario
- Investigar con más detalle con Azure ATP

Implementación de la directiva de riesgo de inicio de sesión

Un riesgo de inicio de sesión representa la probabilidad de que el propietario de la identidad no haya autorizado una solicitud de autenticación determinada. Para los usuarios de Azure Identity Protection, el riesgo de inicio de sesión se puede evaluar como parte de una directiva de acceso condicional. La directiva de riesgo de inicio de sesión admite las siguientes condiciones:

Ubicación

Al configurar la ubicación como una condición, las organizaciones pueden elegir incluir o excluir ubicaciones. Estas ubicaciones con nombre pueden incluir la información de red IPv4 pública, el país o la región, o incluso áreas desconocidas que no se asignan a países o regiones en concreto. Solo los intervalos IP se pueden marcar como una ubicación de confianza. Al incluir **cualquier ubicación**, esta opción incluye cualquier dirección IP en Internet, no solo en las ubicaciones con nombre configuradas. Al seleccionar **cualquier ubicación**, los administradores pueden optar por excluir **todas las ubicaciones de confianza** o **seleccionadas**.

Aplicaciones cliente

De forma predeterminada, las directivas de acceso condicional se aplican a aplicaciones basadas en explorador y aplicaciones que usan protocolos de autenticación modernos. Además de estas aplicaciones, los administradores pueden elegir incluir clientes de Exchange ActiveSync y otros clientes que utilicen protocolos heredados.

- **Explorador**: se trata de aplicaciones basadas en la web que utilizan protocolos como SAML, WS-Federation, OpenID Connect o servicios registrados como un cliente confidencial de OAuth.
- **Aplicaciones móviles y clientes de escritorio**: estas directivas de acceso se usan normalmente cuando se requiere un dispositivo administrado, se bloquea la autenticación

heredada y se bloquean las aplicaciones web, pero se permite la aplicación móvil o de escritorio.

Inicios de sesión no seguros

El informe de inicios de sesión de riesgo contiene datos que se pueden filtrar hasta los últimos 30 días (1 mes).

Con la información que proporciona el informe de inicios de sesión de riesgo, los administradores pueden buscar lo siguiente:

- Qué inicios de sesión están clasificados como de riesgo, confirmados en peligro, confirmados seguros, descartados o corregidos.
- Niveles de riesgo agregado y en tiempo real asociado con los intentos de inicio de sesión.
- Tipos de detección desencadenados.
- Directivas de acceso condicionales aplicadas.
- Detalles de MFA.
- Información del dispositivo
- Información de la aplicación
- Información de la ubicación.

A continuación, los administradores pueden elegir tomar medidas en estos eventos. Los administradores pueden optar por:

- Confirmar el peligro del inicio de sesión
- Confirmar la seguridad del inicio de sesión

Implementación de la autenticación multifactor en Azure

Multi-Factor Authentication (MFA) de Azure Active Directory ayuda a proteger el acceso a los datos y las aplicaciones, al tiempo que mantiene la simplicidad para los usuarios. Proporciona seguridad adicional al requerir una segunda forma de autenticación y ofrece una autenticación segura a través de una variedad de métodos de autenticación fáciles de usar.

En el caso de las organizaciones que necesitan cumplir los estándares del sector, como la versión 3.2 del Estándar de Seguridad de Datos (DSS) para la Industria de Tarjeta de Pago (PCI), MFA debe tener la capacidad de autenticar a los usuarios. Además de cumplir los estándares del sector, la aplicación de MFA para autenticar a los usuarios también puede ayudar a las organizaciones a mitigar los ataques de robo de credenciales.

La seguridad de la verificación en dos pasos de MFA radica en su enfoque por capas. El uso de varias fases de autenticación supone un reto importante para los atacantes. Aunque un atacante consiga descifrar la contraseña de usuario, no servirá de nada si no dispone también del método de autenticación adicional. Los métodos de autenticación incluyen:

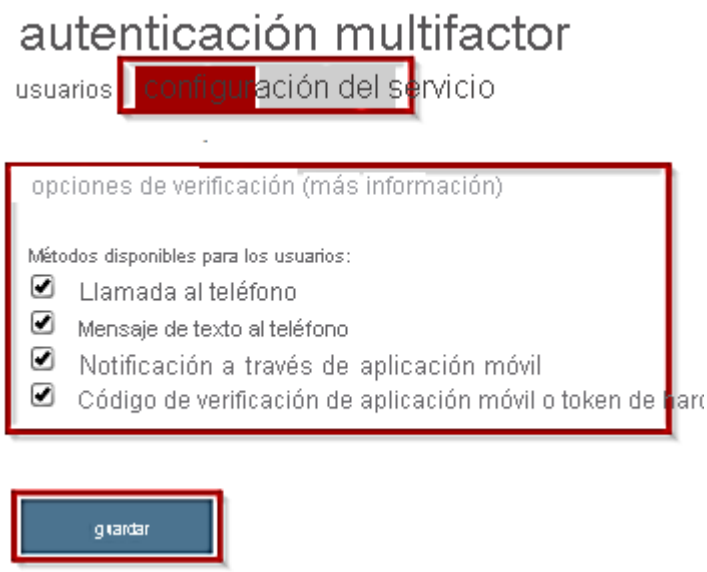
- Un elemento que conoce (normalmente una contraseña).
- Un elemento del que dispone (un dispositivo de confianza que no se puede duplicar con facilidad, como un teléfono).
- Un elemento físico que le identifica (biométrica).

Características de MFA

- **Obtenga más seguridad con menos complejidad**. Azure MFA ayuda a proteger el acceso a datos y aplicaciones y ayuda a satisfacer la demanda de los usuarios de un proceso de inicio de sesión sencillo. Obtenga autenticación segura con una variedad de opciones de verificación sencillas (llamada telefónica, mensaje de texto o notificación de aplicación móvil) y permita a los clientes elegir el método que prefieran.
- **Mitigue las amenazas con alertas y supervisión en tiempo real**. MFA ayuda a proteger su empresa con la supervisión de la seguridad y los informes basados en el aprendizaje automático que identifican los patrones de inicio de sesión incoherentes. Para ayudar a mitigar posibles amenazas, las alertas en tiempo real informan a su departamento de TI de las credenciales de cuenta sospechosas.
- **Úselo con Microsoft 365, Salesforce y mucho más**. MFA para Microsoft 365 ayuda a asegurar el acceso a las aplicaciones de Microsoft 365 sin coste adicional. La autenticación multifactor también está disponible con Azure Active Directory Premium y miles de aplicaciones de software como servicio (SaaS), incluido Salesforce, Dropbox y otros servicios populares.
- **Agregue protección para las cuentas de administrador de Azure**. MFA agrega una capa de seguridad a la cuenta de administrador de Azure sin costo adicional. Cuando está activada,

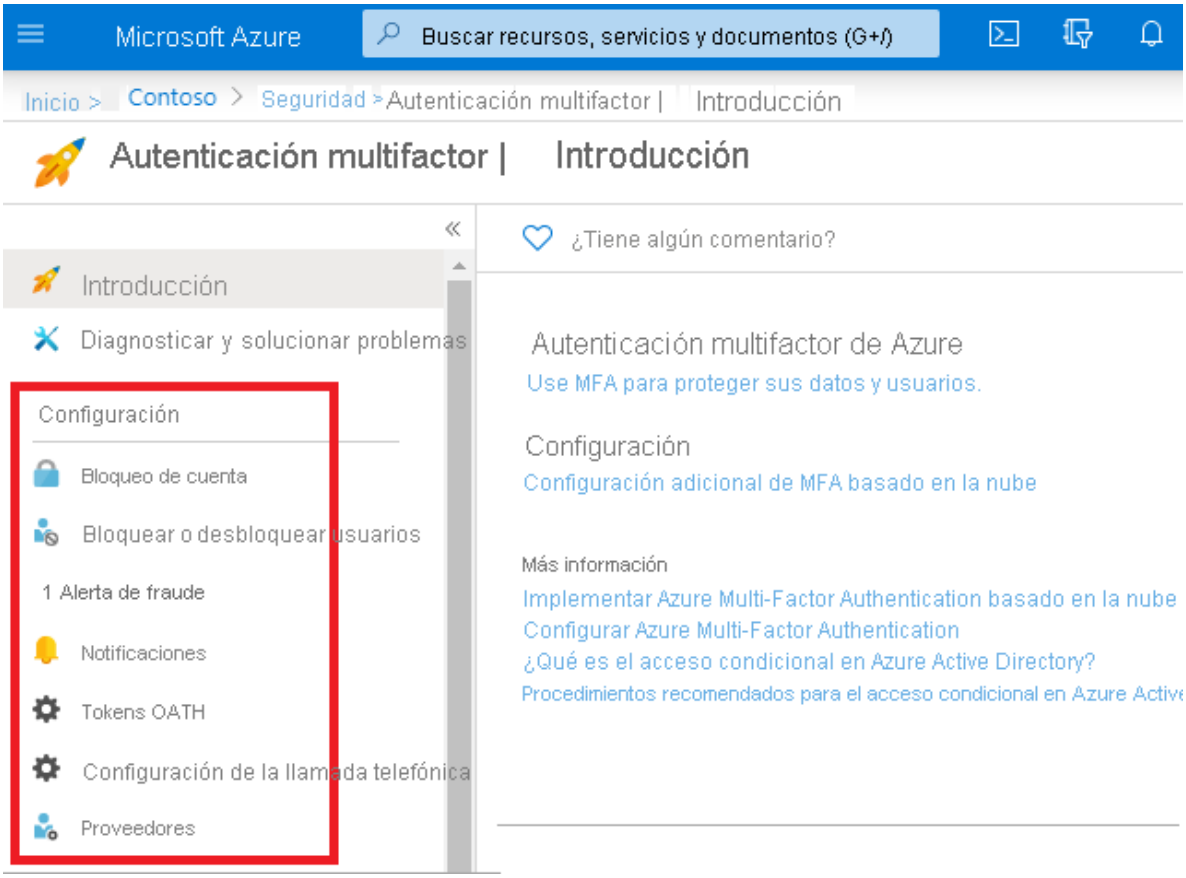
debe confirmar su identidad para crear una máquina virtual, administrar el almacenamiento o usar otros servicios de Azure.

Opciones de autenticación de MFA



Método	Descripción
Llamada al teléfono	Hace una llamada de voz automática. El usuario responde a la llamada y pulsa la # del teclado del teléfono para autenticarse. El número de teléfono no se sincroniza con Active Directory local. Una llamada de voz al teléfono es importante porque se mantiene después de una actualización del terminal telefónico, lo que permite al usuario registrar la aplicación móvil en el nuevo dispositivo.
Mensaje de texto al teléfono	Envía un mensaje de texto que contiene un código de verificación. Se pide al usuario que escriba el código de verificación en la interfaz de inicio de sesión. Este proceso se llama "SMS unidireccional". SMS bidireccional significa que el usuario debe devolver un mensaje de texto con un código determinado. SMS bidireccional se encuentra en desuso y no se admitirá después del 14 de noviembre de 2018. Los usuarios configurados para usar SMS bidireccional pasarán automáticamente a la verificación de llamada telefónica en ese momento.
Notificación a través de aplicación móvil	Envía una notificación push a su teléfono o dispositivo registrado. El usuario ve la notificación y selecciona Aprobar para completar la comprobación. La aplicación Microsoft Authenticator está disponible para Windows Phone, Android e IOS. Las notificaciones de inserción a través de la aplicación móvil proporcionan la mejor experiencia de usuario.
Código de verificación desde aplicación móvil	La aplicación Microsoft Authenticator genera un nuevo código de verificación de OATH cada 30 segundos. El usuario escribe el código de verificación en la interfaz de inicio de sesión. La aplicación Microsoft Authenticator está disponible para Windows Phone, Android e IOS. El código de verificación de la aplicación móvil se puede usar cuando el teléfono no tiene conexión de datos ni señal de telefonía móvil.

Exploración de la configuración de la autenticación multifactor



Bloqueo de cuenta

Para evitar intentos repetidos de MFA como parte de un ataque, la configuración de bloqueo de cuenta le permite especificar el número de intentos erróneos que se permiten antes de que la cuenta quede bloqueada durante un período de tiempo. La configuración de bloqueo de la cuenta solo se aplica cuando se especifica un código PIN para el aviso de MFA. Las siguientes configuraciones están disponibles:

- Número de denegaciones de MFA para desencadenar el bloqueo de cuenta
- Minutos hasta que se restablezca el contador de bloqueos de cuenta
- Minutos hasta que la cuenta se desbloquee automáticamente

Bloqueo y desbloqueo de usuarios

Si el dispositivo de un usuario se ha perdido o ha sido robado, puede bloquear los intentos de autenticación para la cuenta asociada.

Alertas de fraude

- **Bloquear usuario al notificarse fraudes**: configure la característica de alerta de fraude para que los usuarios puedan notificar intentos fraudulentos de acceder a sus recursos.

Los usuarios pueden informar de los intentos de fraude con la aplicación móvil o mediante su teléfono. Bloquear al usuario si se notifican fraudes: si se informa de que un usuario ha cometido fraude, su cuenta se bloquea durante 90 días o hasta que un administrador la desbloquee. Un administrador puede revisar los inicios de sesión mediante el informe de inicio de sesión y tomar las medidas adecuadas para evitar futuros fraudes. El administrador puede, a continuación, desbloquear la cuenta de usuario.

- **Código para notificar fraudes durante el saludo inicial**: cuando los usuarios reciben una llamada telefónica para realizar la verificación en dos pasos, normalmente presionan # para confirmar su inicio de sesión. Para notificar fraudes, el usuario escribe un código antes de presionar #. De manera predeterminada, dicho código es 0, pero se puede personalizar.

Notificaciones

Las notificaciones por correo electrónico se pueden configurar cuando los usuarios notifican alertas de fraude. Normalmente, estas notificaciones se envían a los administradores de identidad, ya que es probable que las credenciales de la cuenta del usuario estén en peligro.

Tokens OATH

Azure AD admite el uso de tokens TOTP SHA-1 de OATH, que actualizan los códigos cada 30 o 60 segundos. Los clientes pueden adquirir estos tokens a través del proveedor de su elección.

IP de confianza

Las direcciones IP de confianza son una característica que permite a los usuarios federados o a los intervalos de direcciones IP omitir la autenticación en dos pasos. Observe que hay dos selecciones en esta captura de pantalla.

Las selecciones que puede realizar dependen de si tiene inquilinos administrados o federados.

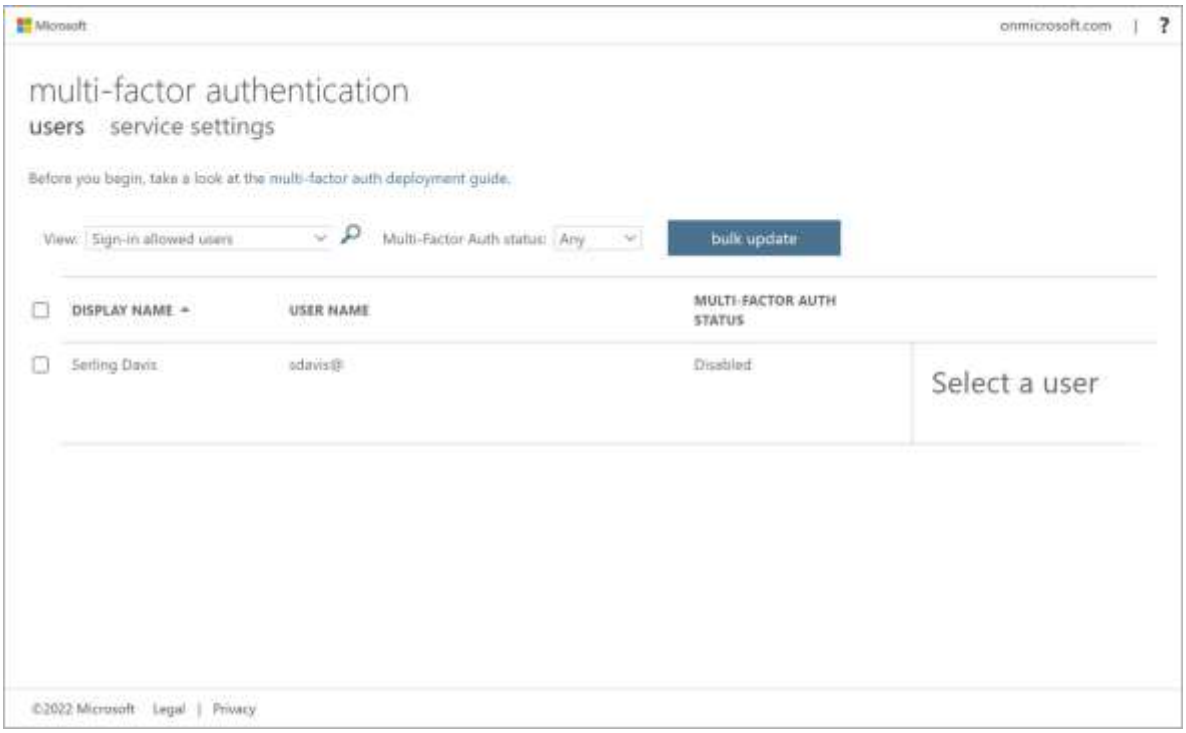
- **Inquilinos administrados**. Para los inquilinos administrados, puede especificar intervalos IP que pueden omitir MFA.
- **Inquilinos federados**. Para los inquilinos federados, puede especificar intervalos IP, y también puede excluir a los usuarios de las notificaciones de AD FS.

Importante

La omisión de las direcciones IP de confianza solo funciona desde dentro de la intranet de la empresa. Si selecciona la opción Todos los usuarios federados y un usuario inicia sesión desde fuera de la intranet de la empresa, el usuario debe autenticarse mediante la verificación en dos pasos. El proceso es el mismo, incluso si el usuario presenta una notificación de AD FS.

Habilitación de la autenticación multifactor

Para habilitar MFA, vaya a Propiedades del usuario en Azure Active Directory y, a continuación, a la opción Multi-Factor Authentication. Desde allí, puede seleccionar los usuarios que desea modificar y habilitar MFA. También puede habilitar grupos de usuarios de forma masiva con PowerShell. Los estados de los usuarios pueden ser **Habilitado**, **Aplicado** o **Deshabilitado**.



Nota

Al iniciar la sesión por primera vez, después de que se haya activado la MFA, se pide a los usuarios que configuren sus ajustes de MFA. Por ejemplo, si habilita MFA para que los usuarios deban usar un dispositivo móvil, se le pedirá a los usuarios que configuren su dispositivo móvil para MFA. Los usuarios deben completar esos pasos o no se les permitirá iniciar sesión, y así seguirán hasta que hayan validado que su dispositivo móvil es compatible con MFA.

Todos los usuarios comienzan con el estado Deshabilitado. Cuando se inscribe a los usuarios en Azure AD Multi-Factor Authentication por usuario, su estado cambia a Habilitado. Cuando los usuarios habilitados inician sesión y completan el proceso de registro, el estado cambia a Aplicado. Los administradores pueden mover a los usuarios entre estados, por ejemplo, de Enforced (Aplicado) a Habilitado o a Deshabilitado.

Habilitación de MFA para administradores globales

Azure MFA se incluye de forma gratuita para la seguridad del administrador global. La habilitación de MFA para administradores globales proporciona un nivel de seguridad adicional al administrar y crear recursos de Azure, como máquinas virtuales, administrar el almacenamiento o usar otros

servicios de Azure. La autenticación secundaria incluye llamadas telefónicas, mensajes de texto y la aplicación de autenticador.

Importante

Recuerde que solo puede habilitar MFA para las cuentas organizativas almacenadas en Active Directory. También se denominan cuentas profesionales o educativas.

Implementación del acceso condicional de Azure AD

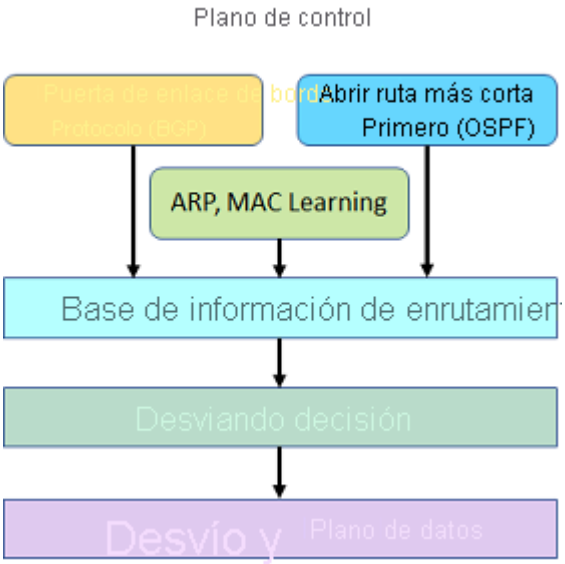
El viejo mundo de la seguridad detrás de un firewall corporativo, con su perímetro de red seguro, ya no funciona, no con personas que quieren trabajar desde cualquier lugar y conectarse a todo tipo de aplicaciones en la nube.

El acceso condicional es la herramienta que usa Azure Active Directory para reunir las señales, tomar decisiones y aplicar las directivas de la organización. El acceso condicional es el corazón del nuevo **plano de control controlado por identidades**.

La directiva de acceso condicional es realmente una directiva de próxima generación creada para la nube. Es capaz de tener en cuenta grandes cantidades de datos, así como los datos contextuales de un flujo de inicio de sesión de usuarios, y asegurarse de que se aplican los controles adecuados.

Identidad como servicio: el nuevo plano de control

¿Cuál es la base para afirmar que la administración de identidades es el nuevo plano de control? En primer lugar, ¿qué es el plano de control? En un conmutador o enrutador, el plano de control es la parte que controla dónde debe ir el tráfico, pero no es responsable del movimiento del tráfico. El plano de control aprende las rutas, ya sea estáticas o dinámicas. La parte responsable de mover el tráfico es el plano de reenvío. En la ilustración siguiente se muestra un diagrama de conmutador simple.



La identidad de un usuario es como un plano de control, porque controla con qué protocolos interactuará el usuario, a qué programas organizativos puede acceder el usuario y qué dispositivos puede emplear el usuario para acceder a esos programas. La identidad es lo que ayuda a proteger los datos corporativos y de usuario. Por ejemplo, ¿deben cifrarse, eliminarse u omitirse los datos cuando se produce un problema?

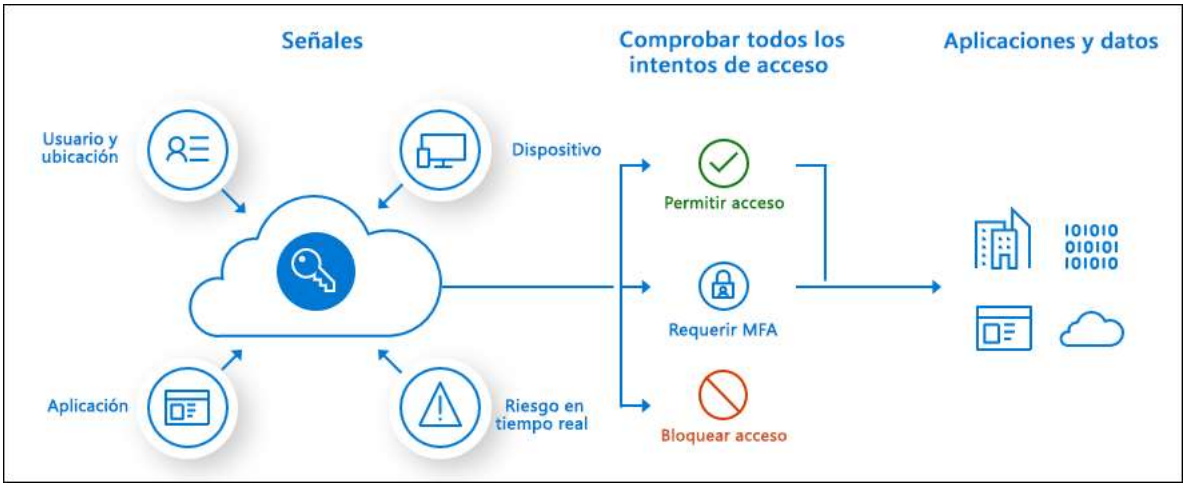
Ahora, todo gira en torno a esa identidad de usuario. Sabe cuáles son sus actividades y dónde se encuentran. Sabe qué dispositivos usan. A continuación, aprovechamos esa información en la directiva de acceso condicional para aplicar elementos como la autenticación multifactor o requerir un dispositivo compatible.

Están las **condiciones**, que indican cuándo se va a aplicar la directiva. Puede ser, de nuevo, la ubicación, el tipo de aplicación en la que se encuentra, cualquier **riesgo detectado**. ¿Cómo se determina el riesgo? Se determina a partir de todo el análisis y la información que tenemos entre organizaciones que usan Azure Active Directory, así como las ofertas de identidad de consumidor de Microsoft. El acceso condicional es la herramienta que usa Azure Active Directory para reunir las señales, tomar decisiones y aplicar las directivas de la organización. Las directivas de acceso condicional, en su forma más simple, son declaraciones **if-then**, si un usuario quiere acceder a un recurso (if), entonces debe completar una acción (then). Por ejemplo, un responsable de nóminas quiere acceder a la aplicación de nóminas y para ello es obligatorio realizar la autenticación multifactor.

Los administradores se enfrentan a dos objetivos principales:

- Capacitar a los usuarios para ser productivos donde sea y cuando sea.
- Proteger los recursos de la organización.

Mediante el uso de directivas de acceso condicional puede aplicar los controles de acceso correctos cuando sea necesario para mantener la organización segura y no interferir con los usuarios cuando no se necesita.



Las directivas de acceso condicional se aplican una vez que se completa la autenticación en una fase. El acceso condicional no pretende ser la primera línea de defensa de una organización para

escenarios como los ataques por denegación de servicio (DoS), pero puede utilizar las señales de estos eventos para determinar el acceso.

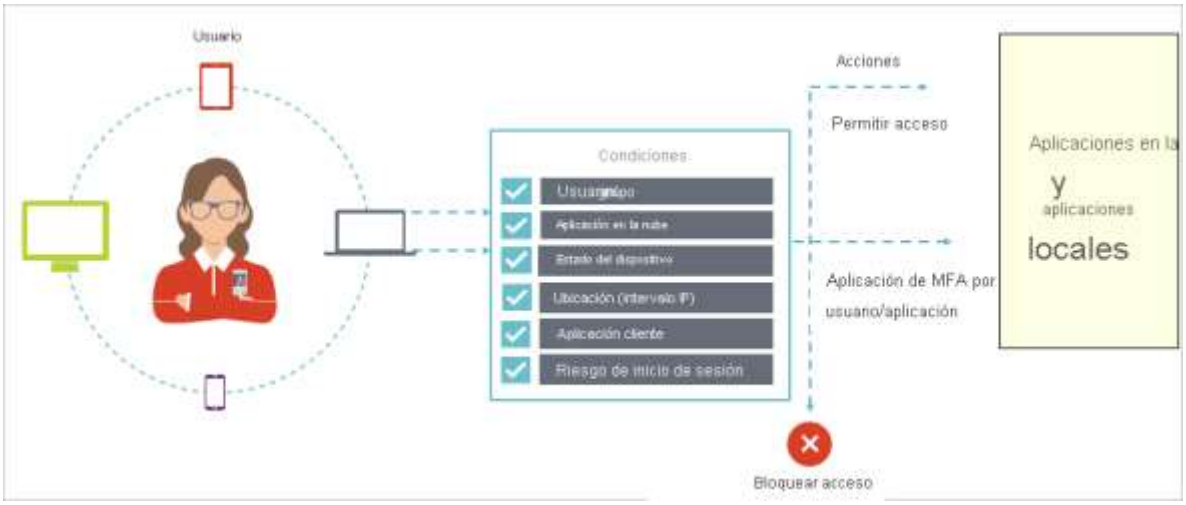
Importante

El acceso condicional es una manera eficaz de habilitar el acceso a los recursos una vez que se cumplen condiciones específicas.

Configuración de las condiciones de acceso condicional

El acceso condicional es una funcionalidad de Azure AD (con una licencia de Azure AD Premium) que le permite aplicar controles sobre el acceso a las aplicaciones en su entorno en función de condiciones específicas desde una ubicación central. Con el acceso condicional de Azure AD, puede tener en cuenta cómo se accede a un recurso en una decisión de control de acceso. Mediante el uso de directivas de acceso condicional, puede aplicar los controles de acceso correctos en las condiciones necesarias.

El acceso condicional incluye seis condiciones: usuario/grupo, aplicación en la nube, estado del dispositivo, ubicación (intervalo IP), aplicación cliente y riesgo de inicio de sesión. Puede usar combinaciones de estas condiciones para obtener la directiva de acceso condicional exacta que necesita. Observe en esta imagen que las condiciones determinan el control de acceso del tema anterior.



Con los controles de acceso, puede bloquear el acceso por completo o conceder acceso con más requisitos seleccionando los controles deseados. Puede tener varias opciones:

- Requerir MFA desde Azure AD o un proceso de MFA local (combinado con AD FS).
- Conceder acceso solo a dispositivos de confianza.
- Requerir un dispositivo unido a un dominio.
- Requerir que los dispositivos móviles usen directivas de protección de aplicaciones de Intune.

Exigir una mejor comprobación de la cuenta mediante MFA es un escenario de acceso condicional común. Aunque es posible que los usuarios puedan iniciar sesión en la mayoría de las aplicaciones en la nube de su organización, es posible que desee una mejor comprobación de aspectos como el sistema de correo electrónico o las aplicaciones que contienen registros de personal o información confidencial. En Azure AD, puede hacerlo con una directiva de acceso condicional.

Importante

La condición de usuarios y grupos es obligatoria en una directiva de acceso condicional. En la directiva, puede seleccionar Todos los usuarios o bien usuarios y grupos específicos.

Implementación de revisiones de acceso

Las revisiones de acceso de Azure Active Directory (Azure AD) permiten a las organizaciones administrar de forma eficiente la pertenencia a grupos, el acceso a las aplicaciones empresariales y las asignaciones de roles. El acceso de los usuarios se puede revisar de forma periódica para asegurarse de que solo las personas adecuadas tengan acceso continuado.

¿Por qué son importantes las revisiones de acceso?

Azure AD le permite colaborar internamente dentro de su organización y con usuarios de organizaciones externas, como los asociados. Los usuarios pueden unirse a grupos, invitar a otros usuarios, conectarse a aplicaciones en la nube y trabajar de forma remota desde sus dispositivos de trabajo o personales. La comodidad de aprovechar el potencial del autoservicio ha llevado a una necesidad de mejores funcionalidades de administración del acceso.

- Cuando se unen nuevos empleados, ¿cómo se asegura de que tengan el acceso adecuado para que sean productivos?
- A medida que las personas cambian de equipo o abandonan la empresa, ¿cómo se asegura de que se quite su antiguo acceso, especialmente cuando hay invitados involucrados?
- Los derechos de acceso excesivos pueden provocar malos resultados en las auditorías y riesgos, ya que indican una falta de control sobre el acceso.
- Debe interactuar proactivamente con los propietarios de recursos para asegurarse de que revisan periódicamente quién tiene acceso a sus recursos.

Use revisiones de acceso en los casos siguientes:

- **Demasiados usuarios con roles con privilegios**: es recomendable comprobar cuántos usuarios tienen acceso administrativo, cuántos de ellos son administradores globales y si hay invitados o asociados que no se han quitado después de que se les haya asignado la realización de una tarea administrativa. Puede volver a certificar los usuarios con asignación de roles en roles de Azure AD, por ejemplo, administradores globales, o roles de recursos de Azure, por ejemplo, administrador de acceso de usuario, en la experiencia Azure AD Privileged Identity Management (PIM).
- **Cuando la automatización es inviable**: puede crear reglas para la pertenencia dinámica en grupos de seguridad o grupos de Microsoft 365, pero ¿qué ocurre si los datos de los

RR. HH. no están en Azure AD o si los usuarios siguen necesitando acceso después de abandonar el grupo para entrenar a su sustituto? Luego puede crear una revisión en ese grupo para asegurarse de que los usuarios que aún necesiten acceso sigan teniendo acceso.

- **Cuando un grupo se utiliza para un nuevo propósito**: si tiene un grupo que se va a sincronizar con Azure AD, o si tiene previsto habilitar una aplicación de administración de ventas para todos los miembros del grupo del equipo de ventas, sería útil pedir al propietario del grupo que revise sus integrantes antes de que se utilice en un contenido de riesgo diferente.
- **Acceso a datos críticos para la empresa**: para determinados recursos, podría ser necesario pedir a personas ajenas a TI que cerraran sesión periódicamente y proporcionaran una justificación sobre por qué necesitan acceso con fines de auditoría.
- **Para mantener la lista de excepciones de una directiva**: en un mundo ideal, todos los usuarios seguirían las directivas de acceso para proteger el acceso a los recursos de la organización. A veces, sin embargo, hay casos empresariales en los que hay que hacer excepciones. Como administrador de TI, puede administrar esta tarea, evitar las excepciones de omisiones de la directiva y proporcionar a los auditores prueba de que estas excepciones se revisan normalmente.
- **Pida a los propietarios de los grupos que confirmen que siguen necesitando invitados en estos**: el acceso de los empleados se puede automatizar con algunos IAM locales, pero no invitados. Si un grupo proporciona a los invitados acceso a contenido empresarial confidencial, es responsabilidad del propietario del grupo confirmar que los invitados todavía tienen una necesidad empresarial legítima de acceso.
- **Hacer que las revisiones se repitan periódicamente**: puede configurar revisiones de acceso periódicas de los usuarios con una frecuencia establecida, como semanal, mensual, trimestral o anual, y los revisores recibirán una notificación al inicio de cada revisión. Los revisores pueden aprobar o denegar el acceso con una interfaz sencilla y con la ayuda de recomendaciones inteligentes.

En función de lo que quiera revisar, creará la revisión de acceso en las revisiones de acceso de Azure AD, las aplicaciones empresariales de Azure AD (**en versión preliminar**) o en Azure AD Privileged Identity Management. Necesita una licencia de Azure AD Premium P2 para usar esta característica.

Importante

Las licencias de Azure AD Premium P2 **no son necesarias** para los usuarios con los roles de administrador global o administrador de usuarios que establecen revisiones de acceso, configuran ajustes o aplican las decisiones de las revisiones.