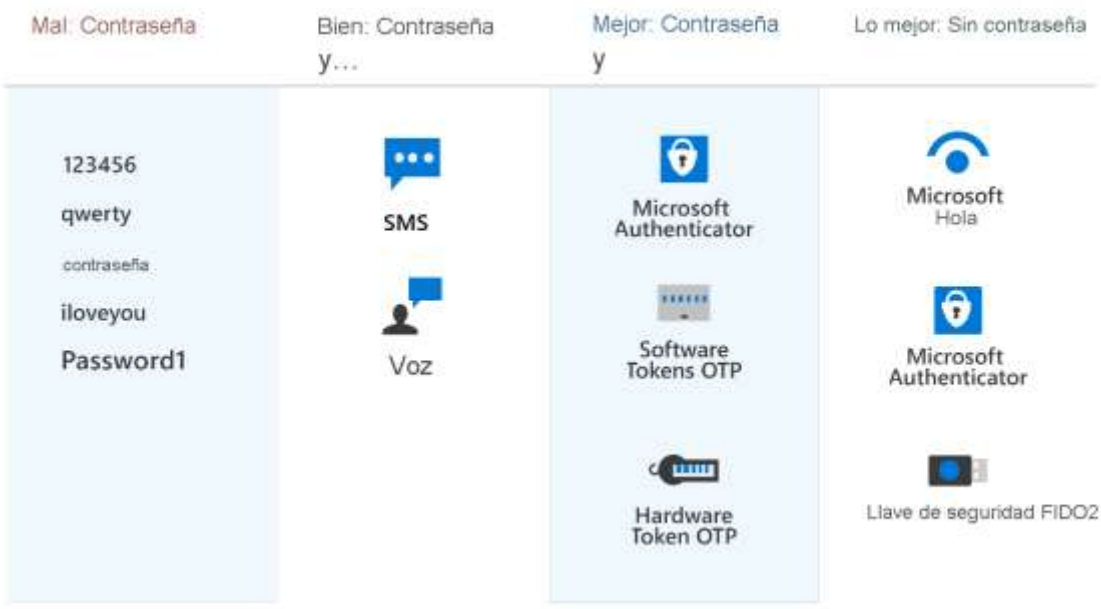
Describir los métodos de autenticación de Azure AD

Una de las principales características de una plataforma de identidad es comprobar, o autenticar, las credenciales cuando un usuario inicia sesión en un dispositivo, una aplicación o un servicio. Azure AD ofrece distintos métodos de autenticación.

Contraseñas

Las contraseñas son la forma más común de autenticación, pero tienen muchos problemas, especialmente si se usan en la autenticación de un solo factor, donde solo se usa una forma de autenticación. Si son bastante fáciles de recordar, un hacker podrá vulnerarlas fácilmente. Las contraseñas seguras que no son fáciles de atacar son difíciles de recordar, y afectan a la productividad de los usuarios cuando las olvidan.

El uso de contraseñas debe complementarse o reemplazarse por métodos de autenticación más seguros disponibles en Azure AD.



Teléfono

Azure AD admite dos opciones para la autenticación basada en teléfono.

- **Autenticación basada en SMS**. El servicio de mensajes cortos (SMS) usado en la mensajería de texto del dispositivo móvil se puede usar como forma principal de autenticación. Con el inicio de sesión basado en SMS, los usuarios no necesitan conocer un nombre de usuario y una contraseña para acceder a las aplicaciones y servicios. En su lugar, el usuario escribe su número de teléfono móvil registrado, recibe un mensaje de texto con un código de verificación, y escribe el código en la interfaz de inicio de sesión.

Los usuarios también pueden optar por comprobar su identidad a través de la mensajería de texto SMS en un teléfono móvil, como forma secundaria de autenticación durante el autoservicio de restablecimiento de contraseña (SSPR) o Azure AD Multi-Factor Authentication. Por ejemplo, los usuarios pueden complementar su contraseña mediante la mensajería de texto SMS. Se envía un SMS al número de teléfono móvil con un código de verificación. Para completar el proceso de inicio de sesión, el código de verificación entregado debe introducirse en la interfaz de inicio de sesión.

- **Comprobación por llamada de voz**. Los usuarios pueden usar llamadas de voz como forma secundaria de autenticación, para comprobar su identidad, durante el autoservicio de restablecimiento de contraseña (SSPR) o Azure AD Multi-Factor Authentication. Con la verificación por llamada telefónica, se hace una llamada de voz automatizada al número de teléfono registrado por el usuario. Para completar el proceso de inicio de sesión, se le pide al usuario que presione # en el teclado. Las llamadas de voz no se admiten como una forma principal de autenticación en Azure AD.

OATH

OATH (Open Authentication) es un estándar abierto que especifica cómo se generan los códigos de contraseña de un solo uso y duración definida (TOTP). Los códigos de contraseña de un solo uso se pueden usar para autenticar a un usuario. Los TOTP de OATH se implementan mediante software o hardware para generar los códigos.

- **Los tokens de software OATH** suelen ser aplicaciones. Azure AD genera la clave secreta, o valor de inicialización, que se introduce en la aplicación y se usa para generar cada OTP.
- **Los tokens de hardware OATH TOTP** (compatibles con la versión preliminar pública) son dispositivos de hardware pequeños que parecen un fob de clave que muestra un código que se actualiza cada 30 o 60 segundos. Los tokens de hardware TOTP de OATH suelen incluir una clave secreta, o valor de inicialización, programada previamente en el token. Estas claves y otra información específica de cada token deben introducirse en Azure AD y, a continuación, activarse para su uso por parte de los usuarios finales.

Los tokens de hardware y software OATH solo se admiten como formas secundarias de autenticación en Azure AD para comprobar una identidad durante el autoservicio de restablecimiento de contraseña (SSPR) o Azure AD Multi-Factor Authentication.

Autenticación sin contraseñas

En muchas organizaciones, el objetivo final es eliminar el uso de contraseñas como parte de los eventos de inicio de sesión. Cuando un usuario inicia sesión con un método sin contraseña, las credenciales se proporcionan mediante el uso de métodos como la información biométrica en Windows Hello para empresas o una clave de seguridad FIDO2. Un atacante no puede duplicar fácilmente estos métodos de autenticación.

Azure AD ofrece formas de autenticación nativa sin contraseña con el fin de simplificar la experiencia de inicio de sesión de los usuarios y reducir el riesgo de ataques.

En el vídeo siguiente se explica el problema de las contraseñas y por qué es tan importante la autenticación sin contraseña.

Windows Hello para empresas

Windows Hello para empresas reemplaza las contraseñas con una autenticación de dos factores sólida en dispositivos. Esta autenticación en dos fases es una combinación de una clave o un certificado vinculado a un dispositivo y algo que la persona conoce (un PIN) o algo que la persona es (biometría). La entrada de PIN y el gesto biométrico desencadenan el uso de la clave privada para firmar criptográficamente los datos que se envían al proveedor de identidades. El proveedor de identidades comprueba la identidad del usuario y autentica al usuario.

Windows Hello para empresas ayuda a protegerse contra el robo de credenciales, ya que un atacante debe tener tanto el dispositivo como la información biométrica o el PIN, lo que dificulta el acceso sin el conocimiento del empleado.

Como método de autenticación sin contraseña, Windows Hello para empresas actúa como forma principal de autenticación. Además, Windows Hello para empresas se puede usar como forma secundaria de autenticación para comprobar una identidad durante la autenticación multifactor.

FIDO2

Fast Identity Online (FIDO) es un estándar abierto para la autenticación sin contraseña. FIDO permite a los usuarios y a las organizaciones aprovechar el estándar para iniciar sesión en sus recursos mediante una clave de seguridad externa o una clave de plataforma integrada en un dispositivo, lo que elimina la necesidad de usar usuario y contraseña.

FIDO2 es el estándar más reciente que incorpora el estándar de autenticación web (WebAuthn) y es compatible con Azure AD. Las claves de seguridad FIDO2 son un método de autenticación sin contraseña basado en estándares que no permite la suplantación de identidad y que puede venir en cualquier factor de forma. Estas claves de seguridad FIDO2 suelen ser dispositivos USB, pero también pueden ser dispositivos basados en Bluetooth o comunicación de campo cercano (NFC), que se usan para la transferencia de datos inalámbricas de corto alcance. Con un dispositivo de hardware que controla la autenticación, se aumenta la seguridad de una cuenta, ya que no hay ninguna contraseña que pueda quedar expuesta ni adivinarse.

Con las claves de seguridad FIDO2, los usuarios pueden iniciar sesión en dispositivos Windows 10 unidos a Azure AD o Azure AD híbrido y lograr el inicio de sesión único en sus recursos de nube y locales. Los usuarios también pueden iniciar sesión en exploradores compatibles. Las claves de seguridad FIDO2 son una excelente opción para las empresas que son muy conscientes de la seguridad o tienen escenarios o empleados que no quieren o no pueden usar su teléfono como un segundo factor.

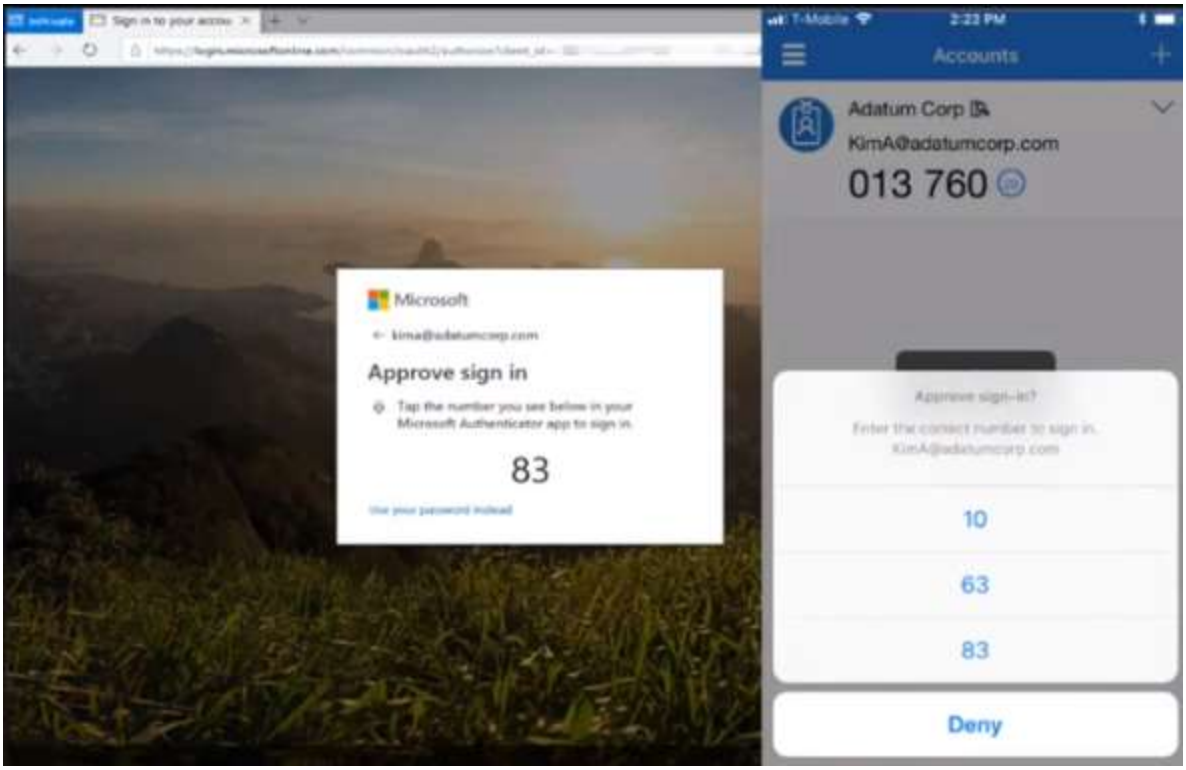
Como método de autenticación sin contraseña, FIDO2 actúa como forma principal de autenticación. Además, FIDO2 se puede usar como forma secundaria de autenticación para comprobar una identidad durante la autenticación multifactor.

Aplicación Microsoft Authenticator

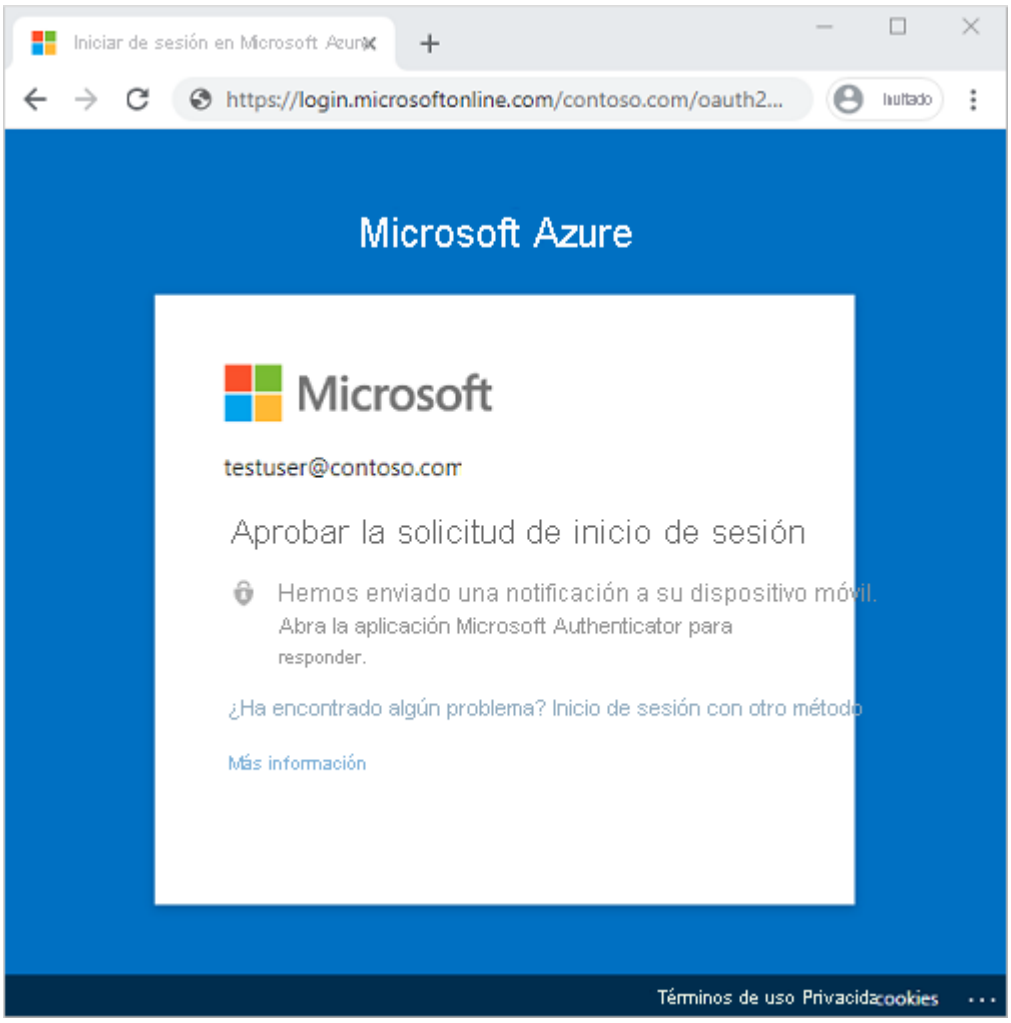
Como método de autenticación sin contraseña, la aplicación Microsoft Authenticator se puede usar como forma principal de autenticación para iniciar sesión en cualquier cuenta de Azure AD o como opción de verificación adicional durante el autoservicio de restablecimiento de contraseña (SSPR) o Azure AD eventos de Multi-Factor Authentication.

Para usar Microsoft Authenticator, un usuario debe descargar la aplicación de teléfono desde Microsoft Store y registrar su cuenta. Microsoft Authenticator está disponible para Android e iOS.

Con la información de inicio de sesión, la aplicación Authenticator convierte cualquier teléfono Android o iOS en una credencial segura sin contraseña. Para iniciar sesión en su cuenta de Azure AD, un usuario escribe su nombre de usuario, coincide con un número mostrado en la pantalla en el que se encuentra en su teléfono y, a continuación, usa su biométrica o PIN para confirmar.



Cuando un usuario elige Authenticator como método de autenticación secundario, para verificar su identidad, se envía una notificación push al teléfono o tableta. Si la notificación es legítima, el usuario selecciona **Aprobar**; de lo contrario, selecciona **Denegar**.



Describir la autenticación multifactor (MFA) en Azure AD

La autenticación multifactor requiere más de una forma de comprobación para demostrar que una identidad es legítima, como un dispositivo de confianza o una detección de huellas digitales. Esto implica que, aunque la contraseña de una identidad se haya puesto en peligro, un hacker no podrá acceder al recurso.

La autenticación multifactor mejora drásticamente la seguridad de las identidades, a la vez que sigue siendo simple para los usuarios. El factor de autenticación adicional debe ser algo difícil de obtener o duplicar para un atacante.

El funcionamiento de la autenticación multifactor de Azure Active Directory solicita lo siguiente:

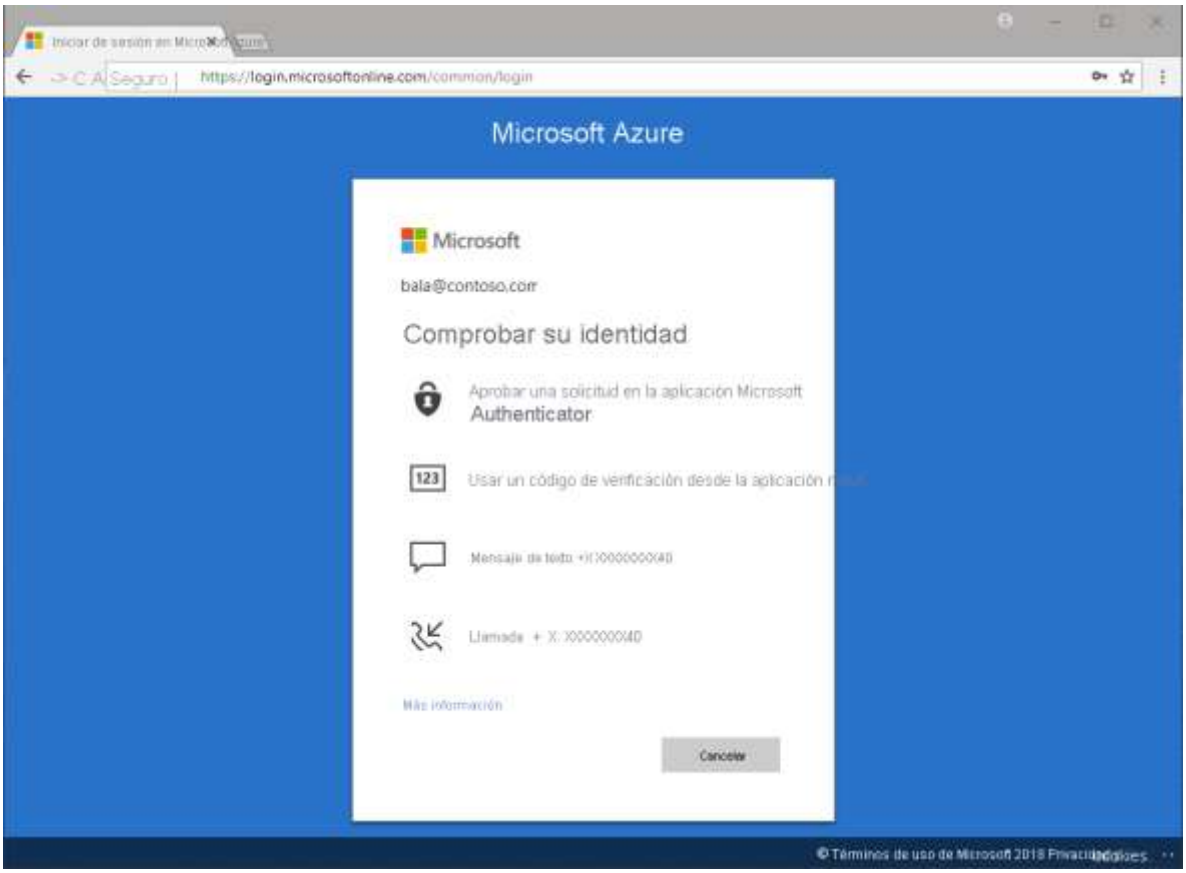
- **Algo que sabe**: normalmente una contraseña o un PIN **y**
- **Algo que tiene**: como un dispositivo de confianza que no se duplica fácilmente; por ejemplo, un teléfono o una clave de hardware, **o**
- **Algo que forma parte de usted**: información biométrica como una huella digital o una detección de rostro.

Las solicitudes de comprobación de la autenticación multifactor están configuradas para formar parte del evento de inicio de sesión en Azure AD. Azure AD solicita y procesa automáticamente la autenticación multifactor, sin realizar cambios en las aplicaciones o servicios. Cuando un usuario inicia sesión, recibe una solicitud de autenticación multifactor y puede elegir una de las formas de verificación adicionales que haya registrado.

Un administrador puede requerir ciertos métodos de comprobación, o el usuario puede acceder a la sección Mi cuenta para editar o agregar métodos de comprobación.

Las siguientes formas adicionales de verificación, descritas en la unidad anterior, se pueden usar con la autenticación multifactor de Azure AD:

- Aplicación Microsoft Authenticator
- Windows Hello para empresas
- Clave de seguridad FIDO2
- Token de hardware OATH (versión preliminar)
- Token de software OATH
- sms
- Llamada de voz



Valores predeterminados de seguridad y autenticación multifactor

Los valores predeterminados de seguridad son un conjunto de mecanismos de seguridad de identidad básicos recomendados por Microsoft. Cuando estén habilitadas, estas recomendaciones se aplicarán automáticamente en su organización. El objetivo es asegurarse de que todas las organizaciones gocen de un nivel básico de seguridad sin ningún costo adicional. Estos valores predeterminados habilitan algunas de las características y controles de seguridad más comunes, entre los que se incluyen los siguientes:

- Aplicar el registro de autenticación multifactor de Azure Active Directory para todos los usuarios.
- Forzar a los administradores a usar la autenticación multifactor.
- Requerir a todos los usuarios que realicen la autenticación multifactor cuando sea necesario.

Los valores predeterminados de seguridad son una excelente opción para las organizaciones que quieren aumentar su posición de seguridad, pero no saben por dónde empezar; o para las organizaciones que usan el nivel Gratis de licencias de Azure AD. Los valores predeterminados de seguridad podrían no ser adecuados para las organizaciones con licencias Premium de Azure AD, o con requisitos de seguridad más complejos. Para más información, visite ¿Cuáles son los valores de seguridad predeterminados?

Descripción del autoservicio de restablecimiento de contraseña (SSPR) en Azure AD

El autoservicio de restablecimiento de contraseña (SSPR) es una característica de Azure AD que permite a los usuarios cambiar o restablecer su contraseña, sin necesidad de que intervenga el administrador o el departamento de soporte técnico.

Si la cuenta de un usuario está bloqueada o se ha olvidado de la contraseña, puede seguir la indicación para restablecerla y volver al trabajo. Esta capacidad reduce las llamadas al departamento de soporte técnico y la pérdida de productividad cuando un usuario no puede iniciar sesión en su dispositivo o en una aplicación.

El autoservicio de restablecimiento de contraseña funciona en los siguientes escenarios:

- **Cambio de contraseña**: el usuario conoce la contraseña, pero quiere cambiarla por una nueva.
- **Restablecimiento de contraseña**: el usuario no puede iniciar sesión, por ejemplo, cuando ha olvidado la contraseña, y quiere restablecerla.
- **Desbloqueo de cuenta**: el usuario no puede iniciar sesión porque su cuenta está bloqueada.

Para usar el autoservicio de restablecimiento de contraseña, los usuarios deben cumplir lo siguiente:

- Tener asignada una licencia de Azure AD. Consulte la sección Más información de la unidad de resumen y recursos para obtener un vínculo a los requisitos de licencia para el autoservicio de restablecimiento de contraseña de Azure Active Directory.
- Estar habilitados para SSPR por un administrador.
- Estar registrado con los métodos de autenticación que quieren usar. Se recomiendan dos o más métodos de autenticación en caso de que uno no esté disponible.

Están disponibles los siguientes métodos de autenticación:

- Notificación en aplicación móvil
- Código de aplicación móvil
- Email
- Teléfono móvil
- Teléfono del trabajo
- Preguntas de seguridad

Cuando los usuarios se registren en SSPR, se les pedirá que elijan los métodos de autenticación que usarán. Si optan por usar preguntas de seguridad, pueden elegir entre un conjunto de preguntas para que se muestren y, a continuación, proporcionar sus propias respuestas. Las preguntas de seguridad se pueden usar solo durante el proceso de autoservicio de restablecimiento de contraseña (SSPR) para confirmar quién es. Las preguntas de seguridad no se usan como método de autenticación durante un evento de inicio de sesión. Las cuentas de administrador no pueden usar preguntas de seguridad como método de verificación con SSPR.

Nota

De manera predeterminada, las cuentas de administrador están habilitadas para el autoservicio de restablecimiento de contraseña y deben usar dos métodos de autenticación para restablecer su contraseña, como una dirección de correo electrónico, una aplicación de autenticador o un número de teléfono. Los administradores no tienen la posibilidad de usar preguntas de seguridad.

Cuando un usuario restablece su contraseña mediante el autoservicio de restablecimiento de contraseña, dicha contraseña también puede reescribirse en una instancia de Active Directory local. La reescritura de contraseñas permite a los usuarios usar sus credenciales actualizadas con las aplicaciones y dispositivos locales sin ninguna demora.

Para mantener a los usuarios informados sobre la actividad de la cuenta, los administradores pueden configurar las notificaciones de correo electrónico que se enviarán cuando se produzca un evento de SSPR. Estas notificaciones pueden abarcar tanto las cuentas de usuario normales como las cuentas de administrador. En el caso de las cuentas de administrador, esta notificación ofrece una capa adicional de reconocimiento cuando se restablece la contraseña de una cuenta de administrador con privilegios mediante SSPR. Todos los administradores globales recibirán una notificación cuando se utilice SSPR en una cuenta de administrador.

En esta guía interactiva, habilitará el autoservicio de restablecimiento de contraseña para los usuarios de Azure Active Directory. Seleccione la imagen siguiente para empezar y siga las indicaciones que aparecen en pantalla.

Descripción de las funcionalidades de administración y protección de contraseñas de Azure AD

La protección de contraseñas es una característica de Azure AD que reduce el riesgo de que los usuarios establezcan contraseñas no seguras. La característica Protección de contraseñas de Azure AD detecta y bloquea las contraseñas no seguras conocidas y sus variantes;además, puede bloquear otros términos poco seguros específicamente para la organización.

Con Protección con contraseña de Azure AD, se aplican automáticamente listas globales de contraseñas prohibidas a todos los usuarios de un inquilino de Azure AD. Para satisfacer sus necesidades empresariales y de seguridad, puede definir entradas en una lista personalizada de contraseñas prohibidas. Cuando los usuarios cambian o restablecen sus contraseñas, se consultan estas listas para exigir el uso de contraseñas seguras.

Debe usar características adicionales, como la autenticación multifactor de Azure Active Directory y no confiar solo en las contraseñas seguras aplicadas por Protección de contraseñas de Azure AD.

Lista global de contraseñas prohibidas

Microsoft actualiza y aplica automáticamente una lista global de contraseñas prohibidas que incluye contraseñas no seguras conocidas. Esta lista la mantiene el equipo de Azure AD Identity Protection, que analiza los datos de telemetría de seguridad para buscar contraseñas poco seguras o vulneradas. Algunos ejemplos de contraseñas que podrían estar bloqueadas son P@$$w0rd o Passw0rd1 y todas sus variaciones.

Las variaciones se crean mediante un algoritmo que transpone mayúsculas y minúsculas, así como letras a números; por ejemplo, "1" a "l". Las variaciones de Password1 pueden incluir a Passw0rd1,

Pass0rd1 y otras. A continuación, estas contraseñas se comprueban y se agregan a la lista global de contraseñas prohibidas y se ponen a disposición de todos los usuarios de Azure AD. La lista global de contraseñas prohibidas se aplica automáticamente y no se puede deshabilitar.

Si un usuario de Azure AD intenta usar como contraseña una de estas contraseñas no seguras, recibirá una notificación para elegir otra más segura. La lista global prohibida se crea a partir de ataques de difusión de contraseñas reales. Este enfoque mejora la seguridad y eficacia generales, y el algoritmo de validación de contraseñas también usa técnicas inteligentes de coincidencia aproximada que se usan para buscar cadenas que coincidan aproximadamente con un patrón. Protección de contraseñas de Azure AD detecta y bloquea de manera eficaz millones de las contraseñas poco seguras más comunes que se usan en su empresa.

Listas personalizadas de contraseñas prohibidas

Los administradores también pueden crear listas personalizadas de contraseñas prohibidas para satisfacer necesidades específicas de seguridad empresarial. La lista personalizada de contraseñas prohibidas impide el uso de contraseñas como el nombre o la ubicación de la organización. Las contraseñas agregadas a la lista personalizada de contraseñas prohibidas deben centrarse en términos específicos de la organización, como:

- Nombres de marca
- Nombres de producto
- Ubicaciones, por ejemplo, la oficina central de la empresa
- Términos internos específicos de la empresa
- Abreviaturas que tienen un significado específico en la empresa

La lista personalizada de contraseñas prohibidas se combina con la lista global de contraseñas prohibidas para bloquear las variaciones de todas las contraseñas.

Las listas de contraseñas prohibidas son una característica de Azure AD Premium 1 o 2.

Protección contra la difusión de contraseñas

Protección con contraseña de Azure AD le ayuda a defenderse contra los ataques de difusión de contraseña. La mayoría de los ataques de difusión de contraseñas envían solo algunas de las contraseñas menos seguras conocidas en cada una de las cuentas de una empresa. Esta técnica permite al atacante buscar rápidamente una cuenta en peligro y evitar posibles umbrales de detección.

Protección con contraseña de Azure AD bloquea de forma eficaz todas las contraseñas no seguras conocidas que se puedan usar en los ataques de difusión de contraseña. Esta protección se basa en los datos de telemetría de seguridad del mundo real que genera Azure AD, los cuales se usan para crear la lista global de contraseñas prohibidas.

Seguridad híbrida

Si busca seguridad híbrida, los administradores pueden integrar la Protección de contraseñas de Azure AD en un entorno de Active Directory local. Un componente instalado en el entorno local recibe la lista global de contraseñas prohibidas y las directivas personalizadas de protección de contraseñas de Azure AD. A continuación, los controladores de dominio las usan para procesar los eventos de cambio de contraseña. Este enfoque híbrido garantiza que, siempre que un usuario cambie su contraseña, se aplique la Protección de contraseñas de Azure AD.

Aunque la protección de contraseñas mejora la seguridad de las contraseñas, debe seguir usando las características recomendadas, como la autenticación multifactor de Azure Active Directory. Las contraseñas por sí solas, incluso las seguras, no lo protegerán tanto como varias capas de seguridad.