**Introducción**

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para administrar la autenticación de forma eficaz a través de Microsoft Entra ID, garantizando un acceso seguro a los recursos y una mejora de la experiencia de usuario.

**Escenario**

Imagine que es un administrador de TI responsable de administrar los métodos de autenticación y garantizar el acceso seguro a los recursos de su organización. Su organización se basa en Microsoft Entra ID para la autenticación de usuario y debe configurar y aplicar métodos de autenticación modernos, al tiempo que mantiene la seguridad.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes pueden:

* Configure el id. verificado de Microsoft Entra para establecer un proceso de comprobación de identidad de confianza.
* Implemente la autenticación multifactor (MFA) para agregar una capa adicional de seguridad a la autenticación de usuarios.
* Implemente la autenticación sin contraseña para proporcionar una experiencia de inicio de sesión más cómoda y segura.
* Implemente medidas de protección de contraseñas para proteger contra los riesgos de seguridad relacionados con contraseñas.
* Implemente el inicio de sesión único (SSO) para simplificar el acceso de usuarios a varias aplicaciones y servicios.
* Integre el inicio de sesión único con proveedores de identidades para facilitar que el acceso sea fluido en varias plataformas.
* Recomiende y aplique protocolos de autenticación modernos para mejorar la seguridad y experiencia de los usuarios.

**Objetivos**

El módulo tiene como objetivo equipar a los participantes con los conocimientos y aptitudes necesarios para administrar la autenticación de forma eficaz en Microsoft Entra ID. Los participantes aprenden a configurar y aplicar métodos de autenticación modernos, proteger la autenticación de los usuarios y simplificar el acceso a recursos, lo que mejora en última instancia la seguridad y la comodidad de los usuarios.

**¿Qué es la autenticación de Microsoft Entra?**

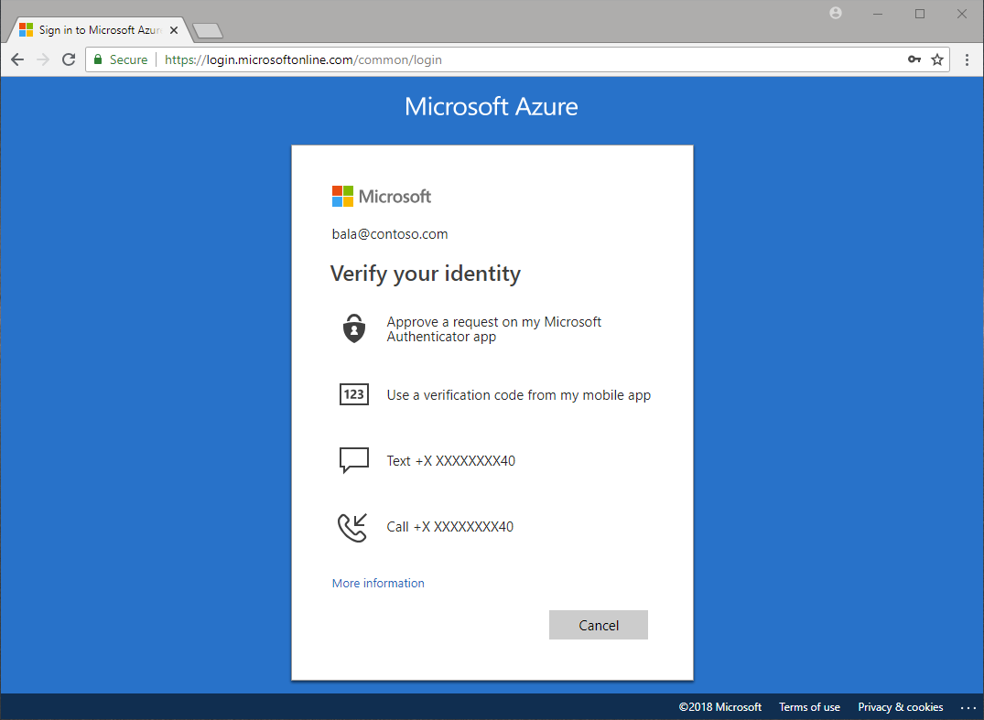
Una de las principales características de una plataforma de identidad es comprobar, o *autenticar*, las credenciales cuando un usuario inicia sesión en un dispositivo, una aplicación o un servicio. En Microsoft Entra ID, la autenticación supone algo más que comprobar un nombre de usuario y una contraseña. Para mejorar la seguridad y reducir la necesidad de asistencia del departamento de soporte técnico, la autenticación de Microsoft Entra ID incluye los siguientes componentes:

* Restablecimiento de la contraseña de autoservicio
* Autenticación multifactor de Microsoft Entra
* Integración híbrida para reescribir los cambios de contraseña en el entorno local
* Integración híbrida para aplicar directivas de protección de contraseñas en un entorno local
* Autenticación sin contraseñas

**Mejora de la experiencia del usuario final**

Microsoft Entra ID ayuda a proteger la identidad de un usuario y a simplificar su experiencia de inicio de sesión. Características como el autoservicio de restablecimiento de contraseña permiten a los usuarios actualizar o cambiar sus contraseñas mediante un explorador web desde cualquier dispositivo. Esta característica es especialmente útil cuando el usuario ha olvidado su contraseña o se ha bloqueado su cuenta, ya que puede desbloquearse y seguir trabajando sin tener que esperar a que el departamento de soporte técnico o el administrador le ayuden.

La autenticación multifactor de Microsoft Entra permite a los usuarios elegir una forma adicional de autenticación durante el inicio de sesión, como una llamada de teléfono o una notificación de la aplicación móvil. Esta capacidad reduce el requisito de una única forma fija de autenticación secundaria, como un token de hardware. Si el usuario no dispone actualmente de una forma de autenticación adicional, puede elegir un método diferente y seguir trabajando.



La autenticación sin contraseña elimina la necesidad de que el usuario cree y recuerde una contraseña segura. Funcionalidades como las claves de seguridad de Windows Hello para empresas o FIDO2 permiten a los usuarios iniciar sesión en un dispositivo o una aplicación sin necesidad de una contraseña. Esta capacidad puede reducir la complejidad de administrar contraseñas en diferentes entornos.

**Restablecimiento de la contraseña de autoservicio**

El autoservicio de restablecimiento de contraseña ofrece a los usuarios la posibilidad de 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 su contraseña, puede seguir las indicaciones para desbloquearse 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:

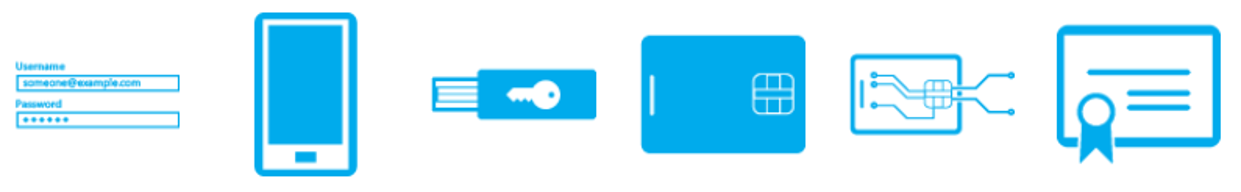
* Cambio de contraseña: el usuario conoce la contraseña pero desea cambiarla por una nueva.
* Restablecimiento de contraseña: el usuario no puede iniciar sesión, por ejemplo, ha olvidado la contraseña y quiere restablecerla.
* Desbloqueo de cuenta: el usuario no puede iniciar sesión porque su cuenta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

Cuando un usuario actualiza o restablece su contraseña mediante el autoservicio de restablecimiento de contraseña, esa contraseña también puede reescribirse en un entorno de Active Directory local. La escritura diferida de contraseñas garantiza que un usuario puede usar inmediatamente sus credenciales actualizadas en aplicaciones y dispositivos locales.

**Autenticación multifactor de Microsoft Entra**

La autenticación multifactor es un procedimiento en el que durante el proceso de inicio de sesión se solicita a un usuario una forma adicional de identificación, como especificar un código en su teléfono móvil o escanear su huella digital.

Si solo usa una contraseña para autenticar a un usuario, deja un vector desprotegido frente a los ataques. Si la contraseña es débil o se ha expuesto en otro lugar, ¿cómo saber si es el usuario quien inicia sesión realmente con el nombre de usuario y la contraseña y no un atacante? Al exigir una segunda forma de autenticación, aumenta la seguridad, ya que este factor adicional no es algo que resulte fácil de obtener o duplicar para un atacante.

 La autenticación multifactor de Microsoft Entra exige dos o más de los siguientes métodos de autenticación:

* Algo que conoce, normalmente una contraseña.
* Algo que tiene, como un dispositivo de confianza que no se puede duplicar con facilidad (por ejemplo, un teléfono o una clave de hardware).
* Algo que forma parte de usted, información biométrica como una huella digital o una detección de rostro.

Los usuarios pueden registrarse para el autoservicio de restablecimiento de contraseña y la autenticación multifactor de Microsoft Entra en un solo paso a fin de simplificar la experiencia de incorporación. Los administradores pueden definir qué formas de autenticación secundaria se pueden usar. También se puede exigir la autenticación multifactor de Microsoft Entra cuando los usuarios realizan un autoservicio de restablecimiento de contraseña para proteger mejor ese proceso.

**Implementación de la autenticación multifactor (MFA)**

Para personalizar la experiencia de usuario final de la autenticación multifactor de Microsoft Entra, puede configurar opciones para valores como los umbrales de bloqueo de cuentas o las alertas y notificaciones de fraude.

La siguiente configuración de autenticación multifactor de Microsoft Entra está disponible en Azure Portal:

| **Característica** | **Descripción** |
| --- | --- |
| Bloqueo de cuenta | Evite temporalmente que las cuentas usen la autenticación multifactor de Microsoft Entra si hay demasiados intentos de autenticación denegados en una fila. Esta característica solo se aplica a los usuarios que escriben un PIN para autenticarse. (Solo servidor de MFA) |
| Bloqueo y desbloqueo de usuarios | Impida que usuarios específicos puedan recibir solicitudes de la autenticación multifactor de Microsoft Entra. Todos los intentos de autenticación para los usuarios bloqueados se denegarán automáticamente. Los usuarios permanecen bloqueados durante 90 días a partir del momento en que se bloquean o cuando se desbloquean manualmente. |
| Notificar actividad sospechosa | Defina configuraciones que permitan a los usuarios notificar solicitudes de comprobación fraudulentas. |
| Notificaciones | Permite notificaciones de eventos desde el Servidor MFA. |
| Tokens de autorización abierta (OATH) | Se usa en entornos de autenticación multifactor de Microsoft Entra basados en la nube para administrar tokens de tipo OATH para los usuarios. |
| Configuración de las llamadas telefónicas | Configure valores relacionados con llamadas de teléfono y saludos para entornos locales y en la nube. |
| Proveedores | Se mostrarán los proveedores de autenticación existentes que pueden haberse asociado con su cuenta. La adición de nuevos proveedores estará deshabilitada a partir del 1 de septiembre de 2018. |

**Bloqueo de cuenta (solo servidor de autenticación multifactor de Microsoft Entra)**

**Nota**

El bloqueo de cuenta solo afecta a los usuarios que inician sesión mediante el servidor MFA local.

Para evitar intentos repetidos de autenticación multifactor 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 cuenta solo se aplica cuando se escribe un código PIN para el símbolo del sistema de autenticación multifactor.

Están disponibles las siguientes opciones de configuración:

* Número de denegaciones de autenticación multifactor que desencadenan un bloqueo de cuenta
* Minutos hasta que se restablezca el contador de bloqueos de la cuenta
* Minutos hasta que la cuenta se desbloquee automáticamente

Para configurar las opciones de bloqueo de cuenta, complete los siguientes pasos:

1. Inicie sesión en **Azure Portal** como administrador.
2. Vaya a **Microsoft Entra ID**, **Seguridad**, **Autenticación multifactor**, **Bloqueo de cuenta**.
3. Escriba los valores necesarios para el entorno y seleccione **Guardar**.

**Bloqueo y desbloqueo de usuarios**

Si el dispositivo de un usuario se ha perdido o ha sido robado, puede bloquear los intentos de autenticación multifactor de Microsoft Entra de la cuenta asociada. Todos los intentos de autenticación multifactor de Microsoft Entra de usuarios bloqueados se deniegan automáticamente. Los usuarios **permanecen bloqueados durante 90 días a partir del momento en que se bloqueen**.

**Bloquear a un usuario**

Para bloquear a un usuario, complete los siguientes pasos.

1. Vaya a **Microsoft Entra ID**, **Seguridad**, **Autenticación multifactor**, **Bloquear y desbloquear usuarios**.
2. Seleccione Agregar para bloquear a un usuario.
3. Escriba el nombre de usuario del usuario bloqueado en el formato username@domain.com y, a continuación, proporcione un comentario en el cuadro Motivo.
4. Seleccione Aceptar para bloquear al usuario.

**Desbloquear un usuario**

Para desbloquear a un usuario, complete los siguientes pasos:

1. Vaya a **Microsoft Entra ID, Seguridad**, **Autenticación multifactor, Bloquear y desbloquear usuarios**.
2. En la columna Acción junto al usuario, **seleccione Desbloquear**.
3. Escriba un comentario en el cuadro Motivo del desbloqueo.
4. Seleccione **Aceptar** para desbloquear al usuario.

**Notificar actividad sospechosa**

Ya está disponible una vista previa de Informar de actividad sospechosa, la función actualizada de **Alerta de fraude de autenticación multifactor**. Cuando se recibe un mensaje de autenticación multifactor desconocido y sospechoso, los usuarios pueden notificar el intento de fraude mediante Microsoft Authenticator o por teléfono. Estas alertas están integradas en Identity Protection para una cobertura y funcionalidad más completas.

Los usuarios que notifican un aviso de autenticación multifactor como sospechoso se establecen en Alto riesgo de usuario. Los administradores pueden usar directivas basadas en riesgos para limitar el acceso a estos usuarios o habilitar **autoservicio de restablecimiento de contraseña (SSPR)** para que los usuarios corrijan problemas por sí mismos. Si usó anteriormente la característica de bloqueo automático de alertas de fraude y no tiene una licencia de **Microsoft Entra ID** P2 para las directivas basadas en riesgos, puede usar eventos de detección de riesgos para identificar y deshabilitar usuarios afectados y evitar automáticamente su inicio de sesión. Para obtener más información sobre el uso de directivas basadas en riesgos, consulte Directivas de acceso basadas en riesgos.

Para habilitar Notificar actividad sospechosa desde la configuración de Métodos de autenticación:

1. En Azure Portal, haga clic en **Microsoft Entra ID**, **Seguridad**, **Métodos de autenticación**, **Configuración**.
2. Establezca Notificar actividad sospechosa en Habilitado.
3. Seleccione Todos los usuarios o un grupo específico.

**Visualización de eventos de actividad sospechosos**

Cuando un usuario informa de un mensaje de autenticación multifactor como sospechoso, el evento se muestra en el informe Inicios de sesión (**como un inicio de sesión rechazado por el usuario**), en los **registros de auditoría** y en el informe de **Detecciones de riesgos**.

Para ver el informe de detección de riesgo, seleccione Azure **Microsoft Entra ID**, **Seguridad, Protección de identidad, Detección de riesgo**. El evento de riesgo forma parte del informe estándar de Detecciones de riesgo y aparecerá como Tipo de detección Actividad sospechosa notificada por el usuario, Nivel de riesgo alto, Usuario final de origen notificado.

Seleccione **Microsoft Entra ID**, **Registros de inicio de sesión**, **Detalles de autenticación** para ver los informes de fraude en el informe de inicio de sesión. El informe de fraude forma parte del informe estándar de inicios de sesión de Microsoft Entra ID y aparece en el detalle del resultado como MFA denegado, Código de fraude especificado.

Para ver los informes de fraude en los registros de auditoría, seleccione **Microsoft Entra ID**, **registros de auditoría**. El informe de fraude aparece en Tipo de actividad Fraude notificado: el usuario está bloqueado para la autenticación multifactor o Fraude notificado: no se realiza ninguna acción en función de la configuración de nivel de inquilino para un informe de fraude.

**Administración de eventos de actividad sospechosa**

Una vez que un usuario ha denunciado una solicitud como sospechosa, el riesgo debe investigarse y corregirse con Identity Protection.

**Notificación de alertas de fraude y actividad sospechosa**

**Notificar actividad sospechosa** y la implementación heredada de **Alerta de fraude** pueden funcionar en paralelo. Puede mantener la funcionalidad Alerta de fraude en todo el inquilino mientras empieza a usar **Notificar actividad sospechosa** con un grupo de pruebas dirigido.

Si Alerta de fraude está habilitada con el bloqueo automático y Notificar actividad sospechosa está habilitada, el usuario se agregará a la lista de bloqueos y se establecerá como de alto riesgo y en el ámbito de cualquier otra directiva configurada. Se deberá quitar estos usuarios de la lista de bloqueados y se deberá corregir su riesgo para permitirles iniciar sesión con MFA.

**Notificaciones**

Puede configurar Microsoft Entra ID para enviar notificaciones por correo electrónico cuando los usuarios informen de alertas de fraude. Normalmente, estas notificaciones se envían a los administradores de identidades porque es probable que las credenciales de la cuenta del usuario estén en peligro. En el ejemplo siguiente se muestra el aspecto de un correo electrónico de notificación de alerta de fraude:

**Tokens OATH**

Microsoft Entra ID admite el uso de tokens **OATH TOTP (contraseña única basada en tiempo)** tokens SHA-1 que actualizan los códigos cada **30** o **60** segundos. Puede adquirir estos tokens a través del proveedor de su elección.

Los tokens de hardware TOTP de OATH suelen incluir una clave secreta, o valor de inicialización, programada previamente en el token. Necesita introducir esas claves en Microsoft Entra ID tal como se describe en los pasos siguientes. Las claves secretas se limitan a 128 caracteres lo que puede no ser compatible con todos los tokens. La clave secreta solo puede contener los caracteres a-z o A-Z y los dígitos 1-7. Debe estar codificada en Base32.

Los tokens de hardware OATH TOTP programables que pueden volver a sembrarse también pueden configurarse con Microsoft Entra ID en el flujo de configuración de tokens de software.

Los tokens de hardware OATH se admiten como parte de una versión preliminar pública.

Después de adquirir tokens, debe cargarlos en un formato de archivo de valores separados por comas (CSV). Incluya el **nombre principal de usuario (UPN)**, **número de serie**, **clave secreta**, **intervalo de tiempo**, **fabricante**, y **modelo**.

CSV

upn,serial number,secret key,time interval,manufacturer,model Helga@contoso.com,1234567,1234567abcdef1234567abcdef,60,Contoso,HardwareKey

**Nota**

Asegúrese de incluir la fila de encabezado en el archivo CSV.

Un administrador puede iniciar sesión en Azure Portal, ir a **Microsoft Entra ID, Seguridad**, **Autenticación multifactor**, **Tokens OATH**y **cargar el archivo CSV**.

En función del tamaño del archivo CSV, puede tardar unos minutos en procesarse. Seleccione Actualizar para obtener el estado. Si hay algún error en el archivo, puede descargar un archivo CSV que enumere los errores. Los nombres de campo del archivo CSV descargado son diferentes de los de la versión cargada.

Una vez solucionados los errores, el administrador puede activar cada clave seleccionando Activar para el token e introduciendo las **contraseñas de un solo uso (OTP)** que aparecen en el token.

Los usuarios pueden tener una combinación de hasta cinco tokens de hardware OATH o aplicaciones de autenticación, como la aplicación Microsoft Authenticator, que está configurada para utilizarse en cualquier momento.

**Implementación de la autenticación sin contraseña**

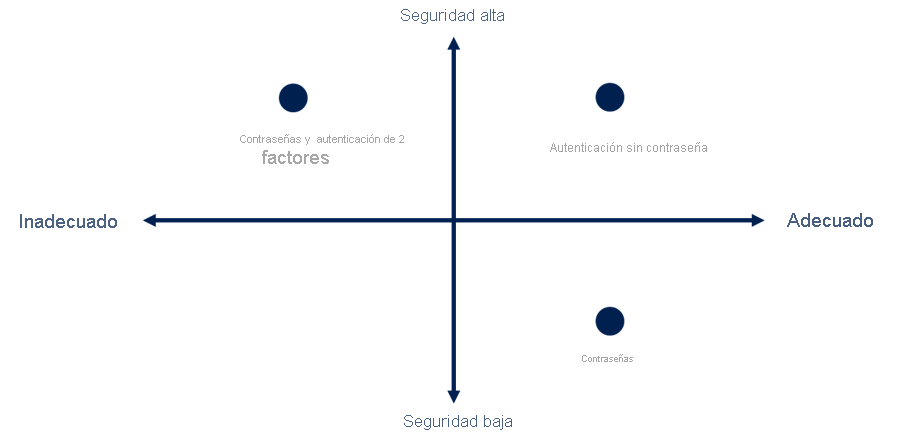
El uso de características como la **autenticación multifactor (MFA)** constituye una excelente manera de proteger una organización. Pero esta capa de seguridad adicional sumada al hecho de tener que recordar las contraseñas suele frustrar a los usuarios. Los métodos de autenticación sin contraseña resultan más cómodos, ya que la contraseña se quita y se reemplaza por algo que se tiene más algo que se es o se sabe.

Expandir tabla

| **Autenticación** | **Algo que se tiene** | **Algo que se es o se sabe** |
| --- | --- | --- |
| Inicio de sesión sin contraseña | Dispositivo, teléfono o clave de seguridad con Windows 10 | PIN o biométrica |

Cada organización tiene diferentes necesidades en cuanto a la autenticación. Microsoft Azure global y Azure Government ofrecen las siguientes **tres** opciones de autenticación sin contraseña que se integran con Microsoft Entra ID:

* Windows Hello para empresas.
* Microsoft Authenticator.
* Claves de seguridad de Fast Identity Online2 (**FIDO2**).



**Windows Hello para empresas**

Windows Hello para empresas resulta muy conveniente para los trabajadores de la información que tienen su propio equipo con Windows designado. La información biométrica y las credenciales de PIN están vinculadas directamente al equipo del usuario, lo que impide el acceso de cualquier persona que no sea el propietario. Con la integración de la infraestructura de clave pública (PKI) y la compatibilidad integrada con el inicio de sesión único (SSO), Windows Hello para empresas ofrece un método sencillo y práctico de acceder directamente a los recursos corporativos del entorno local y la nube.

**Microsoft Authenticator**

También puede permitir que el teléfono del empleado se convierta en un método de autenticación sin contraseña. Es posible que ya esté utilizando la aplicación Authenticator como una opción de autenticación multifactor idónea, además de una contraseña. También puede usar la aplicación Authenticator como una opción sin contraseña.

**Claves de seguridad de Fast Identity Online2 (FIDO2)**

FIDO (Fast IDentity Online) Alliance ayuda a promover los estándares de autenticación abiertos y a reducir el uso de contraseñas como forma de autenticación. FIDO2 es el estándar más reciente que incorpora el estándar de autenticación web (WebAuthn).

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. 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 sin un nombre de usuario o una contraseña mediante una clave de seguridad externa o una clave de plataforma integrada en un dispositivo.

Los usuarios pueden registrarse y luego seleccionar una llave de seguridad de FIDO2 en la interfaz de inicio de sesión como medio principal de autenticación. Estas claves de seguridad FIDO2 suelen ser dispositivos USB, pero también podrían usar Bluetooth o NFC (transmisión de datos en proximidad). 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.

Las claves de seguridad FIDO2 se pueden usar para iniciar sesión en los dispositivos Windows 10 de Microsoft Entra ID o los dispositivos híbridos unidos a Microsoft Entra ID, y para obtener el inicio de sesión único en sus recursos locales y en la nube. 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.

**Introducción a Id. verificada por Microsoft Entra**

En el mundo actual, nuestras vidas digitales y físicas están cada vez más entrelazadas con las aplicaciones, servicios y dispositivos que usamos. Esta revolución digital ha abierto un mundo de posibilidades, lo que nos permite conectarnos con innumerables empresas e individuos de maneras antes imaginables.

Esta mayor conectividad presenta más riesgo de robo de identidad e infracciones de datos. Estas infracciones pueden tener un impacto devastador en nuestras vidas personales y profesionales. Pero hay esperanza. Microsoft está trabajando con una comunidad diversa para crear una solución de identidad descentralizada que ponga a los individuos en control de sus propias identidades digitales, proporcionando una manera segura y privada de administrar los datos de identidad sin depender de autoridades centralizadas ni intermediarios

**Por qué es necesaria una identidad descentralizada**

Hoy en día utilizamos nuestra identidad digital en el trabajo, en casa y en todas las aplicaciones, servicios y dispositivos que usamos. Dicha identidad se compone de todo lo que decimos, hacemos y vivimos (comprar entradas para un evento, registrarnos en un hotel o incluso pedir comida a domicilio). En la actualidad, son otras partes las que poseen y controlan tanto nuestra identidad como todas nuestras interacciones digitales, en algunos casos, incluso sin nuestro conocimiento.

Cada día, los usuarios conceden a las aplicaciones y los dispositivos acceso a sus datos. Sería necesario un gran esfuerzo para que realicen un seguimiento de quién tiene acceso a qué partes de información. En lo que se refiere a la empresa, la colaboración con consumidores y asociados requiere una orquestación de alto nivel para intercambiar datos de forma segura de manera que se mantenga la privacidad y la seguridad de todos los implicados.

Creemos que un sistema de identidad descentralizada basado en estándares puede desbloquear un nuevo conjunto de experiencias que proporcionen a los usuarios y las organizaciones un mayor control sobre sus datos y que, además, ofrezcan un mayor grado de confianza y seguridad tanto a las aplicaciones como a los dispositivos y proveedores de servicios.

**¿Qué son los identificadores descentralizados?**

Para llegar a comprender lo que son los identificadores descentralizados, resulta de gran ayuda establecer una comparación con otros sistemas de identidad. Tanto las direcciones de correo electrónico como los identificadores de las redes sociales son alias descriptivos que para la colaboración, pero ahora están sobrecargados, porque sirven como puntos de control para el acceso a datos en muchos escenarios que van más allá de la colaboración. Esto crea un posible problema, ya que el acceso a estos identificadores se podría quitar en cualquier momento.

Los identificadores descentralizados (DID) son diferentes, Los DID son identificadores únicos a escala mundial, generados por los propios usuarios y arraigados en sistemas descentralizados de confianza. Poseen características únicas, como una mayor garantía de inmutabilidad, resistencia a la censura y evasión de la alteración. Estos atributos son fundamentales para cualquier sistema de identificadores destinado a proporcionar control de usuario y autopropiedad.

La solución de credenciales verificables de Microsoft usa credenciales descentralizadas (DID) para firmar de forma criptográfica como prueba de que un usuario de confianza (verificador) está atestiguando la información que demuestra que son los propietarios de una credencial verificable. Se recomienda que todos aquellos que deseen crear una solución de credenciales verificables mediante la oferta de Microsoft tengan un conocimiento básico de los identificadores descentralizados.

**¿Qué son las credenciales verificables?**

A diario usamos distintas formas de identificarnos. Tenemos carnet de conducir, que usamos como evidencia de somos capaces de manejar un automóvil. Las universidades expiden diplomas que demuestran que hemos logrado cierto nivel de educación. Usamos pasaportes para demostrar a las autoridades quiénes somos cuando viajamos a otros países o regiones. El modelo de datos describe cómo podemos controlar estos tipos de escenarios cuando se trabaja en Internet, pero de una forma segura que respete la privacidad del usuario.

En resumen, las credenciales verificables son objetos de datos que se componen de las notificaciones realizadas por el emisor que da fe de la información sobre un sujeto. Estas notificaciones se identifican por esquema e incluyen el emisor y el asunto del identificador descentralizado. La identidad descentralizada del emisor crea una firma digital como prueba de que da fe de esta información.

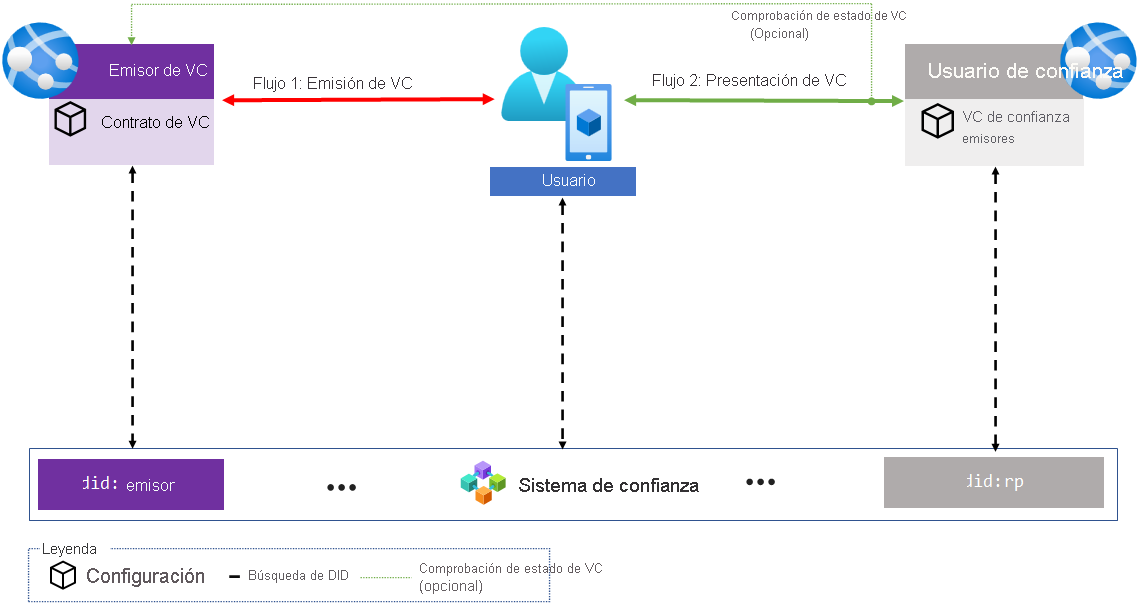
**Enfoques relativos a la identidad**

En la actualidad, la mayoría de las organizaciones usan sistemas de identidad centralizados para proporcionar credenciales de empleados. También usan distintos métodos para llevar clientes, asociados, proveedores y usuarios de confianza a los límites de confianza de la organización. Estos métodos incluyen la federación, la creación y administración de cuentas de invitado con sistemas como Microsoft Entra B2B y la creación de confianzas explícitas con usuarios de confianza. La mayoría de las relaciones empresariales tienen un componente digital, por lo que la habilitación de cierta forma de confianza entre organizaciones requiere un gran esfuerzo.

**Funcionamiento de los sistemas de identidad descentralizada**

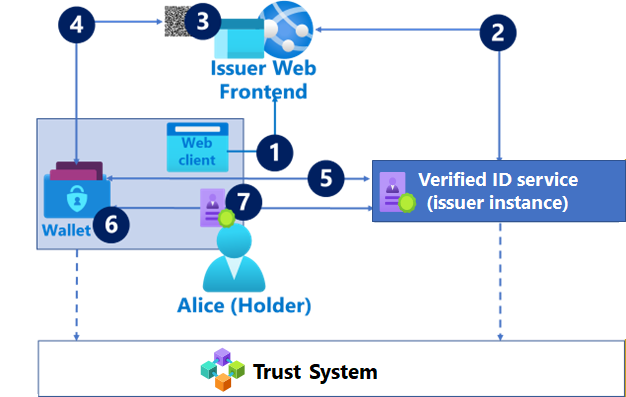
En las arquitecturas de identidad descentralizada, el emisor, el usuario y el usuario de confianza (RP) tienen cada uno un rol para establecer y garantizar el intercambio de confianza continuo de las credenciales de los demás. Las claves públicas de los DID de los actores se pueden resolver mediante el sistema de confianza, lo que permite la validación de firmas y, por tanto, la confianza de cualquier artefacto, incluida una credencial verificable. Los usuarios de confianza pueden consumir credenciales verificables sin tener que establecer relaciones de confianza con el emisor. En su lugar, el emisor proporciona al sujeto una credencial que este puede presentar como prueba a los usuarios de confianza. Todos los mensajes entre los actores se firman con el DID del actor; los DID de los emisores y comprobadores también deben ser propietarios de los dominios DNS que generaron las solicitudes.

Por ejemplo: cuando los titulares de una credencial verificable necesitan acceder a un recurso, deben presentar la credencial a ese usuario de confianza. Para ello, usan una aplicación de cartera para leer la solicitud del usuario de confianza para presentar una credencial verificable. Como parte de la lectura de la solicitud, la aplicación de cartera usa el DID del usuario de confianza para buscar las claves públicas de dicho usuario mediante el sistema de confianza y valida que la solicitud para presentar la credencial verificable no se haya alterado. Para demostrar la propiedad del dominio, la cartera también comprueba que se haga referencia al DID en un documento de metadatos hospedado en el dominio DNS del usuario de confianza.



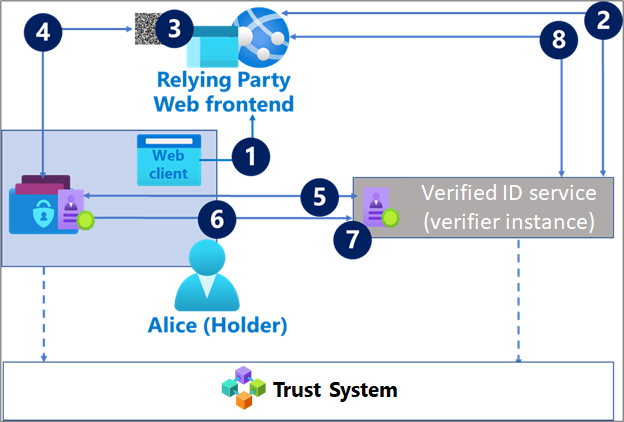
**Flujo 1: emisión de una credencial verificable**

En este flujo, el titular de la credencial interactúa con el emisor para solicitar una credencial verificable, como se muestra en el diagrama siguiente.



1. El titular inicia el flujo mediante un explorador o una aplicación nativa para acceder al front-end web del emisor. Allí, el sitio web del emisor lleva al usuario a recopilar datos y ejecuta la lógica específica del emisor para determinar si se puede emitir la credencial y su contenido.
2. La interfaz web del emisor llama al servicio de Verified ID de Microsoft Entra para generar una solicitud de emisión de VC.
3. El front-end web representa un vínculo a la solicitud en forma de código QR o un vínculo profundo específico del dispositivo (según el dispositivo).
4. El titular lee el código QR o el vínculo profundo del paso 3 mediante una aplicación de cartera, como Microsoft Authenticator
5. La cartera descarga la solicitud del vínculo. La solicitud incluye:
   * DID del emisor. La aplicación de cartera usa el DID del emisor que se va a resolver mediante el sistema de confianza para buscar las claves públicas y los dominios vinculados.
   * Dirección URL con el manifiesto de credencial verificable, que especifica los requisitos del contrato para emitir la credencial. Los requisitos del contrato pueden incluir id\_token, los atributos de atestiguación automática que se deben proporcionar o la presentación de otra credencial verificable.
   * Aspecto de la credencial verificable (dirección URL del archivo de logotipo, colores, etc.)
6. La cartera valida las solicitudes de emisión y procesa los requisitos del contrato:
   * Valida que el mensaje de solicitud de emisión se haya firmado con las claves del emisor que se encuentran en el documento DID resuelto mediante el sistema de confianza. Validar la firma garantiza que el mensaje no se haya alterado.
   * Valida que el emisor posea el dominio DNS al que se hace referencia en el documento DID del emisor.
   * En función de los requisitos del contrato de VC, la cartera puede requerir que el titular recopile información adicional, como por ejemplo, solicitar atributos de emisión automática o navegar por un flujo de OIDC para obtener id\_token.
7. Envía los artefactos requeridos por el contrato al servicio Verified ID de Microsoft Entra. El servicio Verified ID de Microsoft Entra devuelve el VC, firmado con la clave DID del emisor y la cartera almacena de forma segura el VC.

**Flujo 2: presentación de credenciales verificables**



En este flujo, un titular interactúa con un usuario de confianza para presentar una credencial verificable como parte de sus requisitos de autorización.

1. El titular inicia el flujo mediante un explorador o una aplicación nativa para acceder al front-end web del usuario de confianza.
2. El frontend web llama al servicio Verified ID de Microsoft Entra para generar una solicitud de presentación VC.
3. El front-end web representa un vínculo a la solicitud en forma de código QR o un vínculo profundo específico del dispositivo (según el dispositivo).
4. El titular lee el código QR o el vínculo profundo del paso 3 mediante una aplicación de cartera, como Microsoft Authenticator
5. La cartera descarga la solicitud del vínculo. La solicitud incluye:
   * Solicitud basada en estándares para las credenciales de un esquema o tipo de credencial.
6. La cartera valida la solicitud de presentación y encuentra las credenciales verificables almacenadas que satisfacen la solicitud. En función de las credenciales verificables necesarias, la cartera guía al sujeto para seleccionar y dar su consentimiento para usar las credenciales verificables.
   * Una vez que el sujeto consiente el uso de la credencial verificable, la cartera genera un DID único en pares entre el sujeto y el usuario de confianza.

Luego, la cartera envía una carga de respuesta de presentación al servicio de Verified ID de Microsoft Entra firmada por el sujeto. Contiene:

* + Las credenciales verificables que el sujeto consintió.
  + El DID en pares generado como "sujeto" de la carga.
  + El DID del usuario de confianza como "audiencia" de la carga.

1. El servicio Verified ID de Microsoft Entra valida la respuesta enviada por la cartera. En algunos casos, el emisor de la credencial verificable puede revocar la credencial verificable. Para asegurarse de que la credencial verificable siga siendo válida, el comprobador debe comprobar con el emisor de la credencial verificable. Esto depende de cómo haya solicitado el comprobador la credencial verificable en el paso 2.
2. Tras la validación, el servicio Verified ID de Microsoft Entra devuelve la llamada al RP con el resultado.

**Puntos clave**

Las arquitecturas descentralizadas se pueden usar para mejorar las soluciones existentes y proporcionar nuevas funcionalidades.

Para cumplir las aspiraciones de la fundación Decentralized Identity Foundation (DIF) y los objetivos de diseño de W3C, se deben tener en cuenta los siguientes elementos al crear una solución de credenciales verificables:

* No hay puntos centrales de establecimiento de confianza entre los actores del sistema. En otras palabras, los límites de confianza no se expanden a través de la federación porque los actores confían en credenciales verificables concretas.
  + El sistema de confianza permite la detección del identificador descentralizado (DID) de cualquier actor.
  + La solución permite a los comprobadores validar las credenciales verificables de cualquier emisor.
  + La solución no permite al emisor controlar la autorización del sujeto o del comprobador (usuario de confianza).
* Los actores operan de forma desacoplada, cada uno de ellos puede completar las tareas de sus roles.
  + Los emisores atienden todas las solicitud de credenciales verificables y no discriminan las solicitudes atendidas.
  + Los sujetos poseen su credencial verificable una vez emitida y pueden presentar su credencial verificable a cualquier comprobador.
  + Los comprobadores pueden validar cualquier credencial verificable de cualquier asunto o emisor.

**Configuración de la id. verificada por Microsoft Entra**

En un escenario real, donde el emisor y el verificador son organizaciones separadas, el verificador utiliza su propio inquilino de Microsoft Entra para realizar la verificación de la credencial que fue emitida por la otra organización. Como comprobador, desbloqueará privilegios para las personas que tengan tarjetas de experto en credenciales verificadas.

**Requisitos previos**

* Configure un inquilino para Verified ID de Microsoft Entra.
* Si quiere clonar el repositorio que hospeda la aplicación de ejemplo, instale Git.
* Visual Studio Code u otro editor de código similar.
* .NET 5.0.
* Descargue ngrok y regístrese para obtener una cuenta gratuita. Si no es posible usar ngrok en la organización, lea estas preguntas frecuentes.
* Un dispositivo móvil con Microsoft Authenticator:
  + Se ha instalado la versión 6.2206.3973 de Android o una posterior.
  + Se ha instalado la versión 6.6.2 de iOS o una posterior.

**Recopilación de detalles del inquilino para configurar la aplicación de ejemplo**

Ahora que ha configurado Verified ID de Microsoft Entra, va a recopilar información sobre el entorno y las credenciales verificables que ha establecido. Estos fragmentos de información los usará al configurar la aplicación de ejemplo.

**Descarga del código de ejemplo**

La aplicación de ejemplo está disponible en .NET y el código se mantiene en un repositorio de GitHub.

**Configure la aplicación de credenciales verificables**

Cree un secreto de cliente para la aplicación registrada que ha creado. La aplicación de ejemplo usa el secreto de cliente para demostrar su identidad al solicitar tokens.

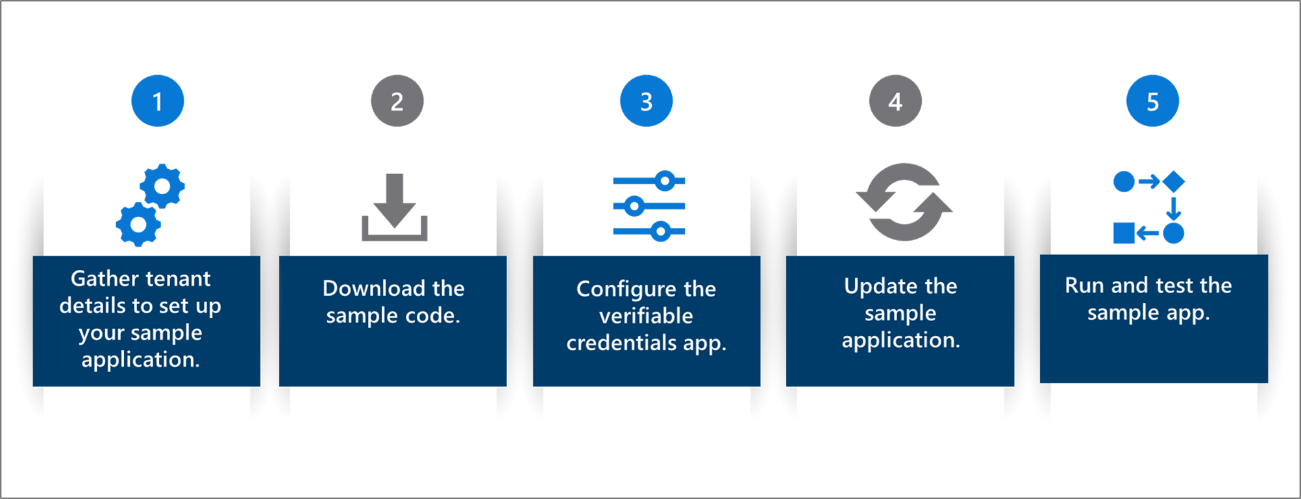
**Actualización de la aplicación de ejemplo**

Ahora realice modificaciones en el código del emisor de la aplicación de ejemplo para actualizarlo con la dirección URL de credencial verificable. Este paso le permite emitir credenciales verificables mediante su propio inquilino.

**Ejecución y prueba de la aplicación de ejemplo**

Ahora está listo para presentar y comprobar su primera tarjeta de experto en credenciales verificadas mediante la ejecución de la aplicación de ejemplo.

**Ejemplo**: Complete los pasos siguientes para **presentar** y **comprobar** el id. verificado de Microsoft Entra para una aplicación de ejemplo:



**Implementación de la protección de contraseñas**

La característica Protección con contraseña de Microsoft Entra detecta y bloquea las contraseñas no seguras conocidas y sus variantes, y también puede bloquear otros términos poco seguros específicos de una organización. La implementación local de Protección con contraseña de Microsoft Entra utiliza las mismas listas de contraseñas prohibidas personalizadas y globales que se almacenan en Microsoft Entra ID y realiza las mismas comprobaciones de los cambios de contraseña locales que hace Microsoft Entra ID de los cambios basados en la nube. Estas comprobaciones se realizan durante los cambios de contraseña y los eventos de restablecimiento de contraseña en los controladores de dominio de Microsoft Entra local.

**Principios de diseño**

Protección con contraseña de Microsoft Entra se ha diseñado teniendo en cuenta estos principios:

* Los controladores de dominio (DC) nunca tienen que comunicarse directamente con Internet.
* No hay ningún puerto de red nuevo abierto en los controladores de dominio.
* No se requieren cambios en el esquema de Microsoft Entra Domain Services. El software usa los objetos de esquema *container* y *serviceConnectionPoint* de dominio de Microsoft Entra existentes.
* Se puede usar cualquier nivel funcional de dominio o bosque de Microsoft Entra Domain Services compatible.
* El software no crea ni necesita ninguna cuenta en los dominios de Microsoft Entra Domain Services que protege.
* Las contraseñas de usuario no cifradas nunca dejan el controlador de dominio, ya sea durante las operaciones de validación de contraseña o en cualquier otro momento.
* El software no depende de otras características de Microsoft Entra. Por ejemplo, la sincronización de hash de contraseñas (PHS) de Microsoft Entra no está relacionada con Protección con contraseña de Microsoft Entra ni es necesaria con funcionalidad.
* Se admite la implementación incremental, sin embargo, la directiva de contraseñas se aplicará solamente donde se instale el agente de controlador de dominio.

**Implementación incremental**

La protección con contraseña de Microsoft Entra admite la implementación incremental entre controladores de dominio de Microsoft Entra ID. Es importante comprender lo que esto significa realmente y cuáles son los inconvenientes.

El software agente de DC de Protección con contraseña de Microsoft Entra solo puede validar las contraseñas cuando está instalado en un controlador de dominio, y solo en el caso de los cambios de contraseña que se envían a ese controlador de dominio. No es posible controlar qué controladores de dominio eligen las máquinas cliente de Windows para procesar los cambios de contraseña de los usuarios. Para garantizar el comportamiento coherente y el cumplimiento de la seguridad universal de Protección con contraseña de Microsoft Entra, el software agente de DC debe estar instalado en todos los controladores de dominio de un dominio.

Muchas organizaciones quieren probar con precaución Protección con contraseña de Microsoft Entra en un subconjunto de sus controladores de dominio antes de realizar una implementación completa. Este escenario es posible gracias a que Protección con contraseña de Microsoft Entra admite la implementación parcial. El software de agente de DC de un controlador de dominio dado valida de forma activa las contraseñas incluso cuando otros controladores de dominio del dominio no tienen instalado dicho software. Las implementaciones parciales de este tipo no son seguras y solo se recomiendan con fines de prueba.

* El servicio de proxy de protección con contraseña de Microsoft Entra se ejecuta en cualquier máquina unida a un dominio del bosque de Microsoft Entra ID actual. La finalidad principal de este servicio es la de reenviar las solicitudes de descarga de la directiva de contraseñas de los controladores de dominio a Microsoft Entra ID y, luego, devolver las respuestas de Microsoft Entra ID al controlador de dominio.
* La DLL del agente de controlador de dominio del filtro de contraseña recibe las solicitudes de validación de contraseña de usuario desde el sistema operativo. El filtro las reenvía al servicio DC Agent que se ejecuta localmente en el controlador de dominio.
* El servicio DC Agent de Protección con contraseña de Microsoft Entra recibe solicitudes de validación de contraseña del archivo DLL del filtro de contraseñas de DC Agent. Este servicio las procesa mediante la directiva de contraseñas (disponible localmente) actual y devuelve el resultado de *correcta* o *error*.

**Funcionamiento de Protección con contraseña de Microsoft Entra**

Los componentes de Protección con contraseña de Microsoft Entra local funcionan de la siguiente manera:

1. Cada instancia del servicio proxy de protección con contraseña de Microsoft Entra se anuncia en los controladores de dominio del bosque mediante la creación de un objeto serviceConnectionPoint en Microsoft Entra ID. Cada servicio del agente de controlador de dominio para la protección con contraseña de Microsoft Entra también crea un objeto serviceConnectionPoint en Microsoft Entra ID. Este objeto se utiliza principalmente para los informes y diagnósticos.
2. El servicio DC Agent es responsable de iniciar la descarga de una nueva directiva de contraseñas de Microsoft Entra ID. El primer paso es localizar un servicio de proxy de Protección con contraseña de Microsoft Entra consultando en el bosque los objetos serviceConnectionPoint del proxy.
3. Cuando se encuentra un servicio de proxy disponible, el agente de controlador de dominio envía una solicitud de descarga de la directiva de contraseña al servicio de proxy. A su vez, el servicio de proxy envía la solicitud a Microsoft Entra ID para, posteriormente, devolver la respuesta al servicio DC Agent.
4. Una vez que el servicio DC Agent recibe una nueva directiva de contraseña de Microsoft Entra ID, la almacena en una carpeta dedicada en la raíz de su recurso compartido de carpeta sysvol de dominio. El servicio DC Agent también supervisa esta carpeta en caso de que las directivas más recientes se repliquen desde otros servicios DC Agent en el dominio.
5. El servicio siempre solicita una nueva directiva al inicio del servicio. Una vez iniciado el servicio DC Agent, comprueba la antigüedad de la directiva actual disponible de forma local cada hora. Si la directiva es anterior a una hora, el agente de controlador de dominio solicita una nueva directiva de Microsoft Entra ID a través del servicio de proxy, como se describió anteriormente. Si la directiva actual no es anterior a una hora, el agente de controlador de dominio sigue usando esa directiva.
6. Cuando un controlador de dominio recibe los eventos de cambio de contraseña, la directiva almacenada en caché se usa para determinar si la nueva contraseña se acepta o se rechaza.

**Principales consideraciones y características**

* Cada vez que se descarga una directiva de contraseñas de Protección con contraseña de Microsoft Entra, esa directiva es específica de un inquilino. En otras palabras, las directivas de contraseñas son siempre una combinación de la lista global de contraseñas prohibidas de Microsoft y la lista de contraseñas prohibidas por inquilino personalizada.
* El agente de controlador de dominio se comunica con el servicio de proxy por RPC a través de TCP. El servicio de proxy escucha estas llamadas en un puerto RPC dinámico o estático, según esté configurado.
* El agente de controlador de dominio nunca escucha en un puerto de red disponible.
* El servicio de proxy nunca llama al servicio DC Agent.
* El servicio de proxy es sin estado. Nunca almacena en caché las directivas ni cualquier otro estado descargado de Azure.
* El servicio DC Agent siempre usa la directiva de contraseña localmente disponible más reciente para evaluar una contraseña de usuario. Si no hay ninguna directiva de contraseña disponible en el controlador de dominio local, la contraseña se acepta automáticamente. Cuando esto ocurre, se registra un mensaje de evento para advertir al administrador.
* Protección con contraseña de Microsoft Entra no es un motor de aplicación de directivas en tiempo real. Puede haber un retraso desde que se realiza un cambio en la configuración de la directiva de contraseñas en Microsoft Entra ID hasta que el cambio llega y se aplica a todos los controladores de dominio.
* Protección con contraseña de Microsoft Entra funciona como un complemento a las directivas de contraseña de Microsoft Entra ID existentes, no las sustituye. Esto incluye las demás DLL de filtro de contraseña de terceros que puedan estar instaladas. En Microsoft Entra ID, es necesario siempre que todos los componentes de validación de contraseñas estén de acuerdo antes de aceptar una contraseña.

**Implementación del inicio de sesión único (SSO)**

Al planear la implementación del SSO con sus aplicaciones de Microsoft Entra ID, debe tener en cuenta las siguientes preguntas:

* ¿Cuáles son los roles administrativos necesarios para administrar la aplicación?
* ¿Es necesario renovar el certificado de aplicación de Lenguaje de marcado de aserción de seguridad (SAML)?
* ¿Quién debe recibir una notificación de los cambios relacionados con la implementación del inicio de sesión único?
* ¿Qué licencias son necesarias para garantizar una administración eficaz de la aplicación?
* ¿Se usan cuentas de usuario invitado y compartidas para acceder a la aplicación?
* ¿Conozco las opciones de implementación del SSO?

**Roles administrativos**

Use siempre el rol con los permisos mínimos disponibles para realizar la tarea requerida en Microsoft Entra ID. Revise los distintos roles disponibles y elija el correcto para resolver las necesidades para cada rol de la aplicación. Es posible que algunos roles se tengan que aplicar temporalmente y quitar una vez completada la implementación.

| **Rol** | **Roles** | **Rol de Microsoft Entra (si procede)** |
| --- | --- | --- |
| Administrador del departamento de soporte técnico | El nivel 1 admite la visualización de los registros de inicio de sesión para resolver problemas. | None |
| Administración de identidades | Configuración y depuración cuando los problemas implican Microsoft Entra ID | Administrador de aplicaciones en la nube |
| Administrador de aplicaciones | Atestación de usuarios en la aplicación, configuración en usuarios con permisos | None |
| Administradores de infraestructura | Propietario de sustitución del certificado | Administrador de aplicaciones en la nube |
| Propietario de la empresa o parte interesada | Atestación de usuarios en la aplicación, configuración en usuarios con permisos | None |

**Certificate**

Al habilitar la federación en la aplicación de SAML, Microsoft Entra ID crea un certificado con una validez predeterminada de tres años. Si es necesario, puede personalizar la fecha de expiración de ese certificado. Asegúrese de que tiene procesos implantados para renovar los certificados antes de que caduquen.

Puede cambiar la duración del certificado en el centro de administración de Microsoft Entra. Asegúrese de documentar la expiración y saber cómo administrará la renovación de certificados. Es importante identificar los roles adecuados y las listas de distribución de correo electrónico encargadas de administrar el ciclo de vida del certificado de firma. Se recomiendan los siguientes roles:

* Propietario para actualizar las propiedades de usuario en la aplicación
* Propietario de guardia para proporcionar asistencia para la solución de problemas de la aplicación
* Lista de distribución de correo electrónico supervisada con detalle para notificaciones de cambios relacionados con el certificado

Configure un proceso para controlar un cambio de certificado entre Microsoft Entra ID y la aplicación. Este proceso puede ayudar a evitar o minimizar una interrupción debido a la expiración de un certificado o a una sustitución forzada de certificados.

**Comunicaciones**

La comunicación es fundamental para el éxito de cualquier servicio nuevo. Comuníquese de forma proactiva con los usuarios sobre cómo cambiará su experiencia. Comuníqueles cuándo cambiará y cómo obtener soporte técnico si tienen problemas. Revise las opciones sobre cómo accederán los usuarios a sus aplicaciones habilitadas para el inicio de sesión único y elabore las comunicaciones de forma que coincidan con la selección.

Implemente el plan de comunicación. Asegúrese de que permite a los usuarios saber que se va a producir un cambio, cuándo se ha producido y qué hacer a continuación. Además, asegúrese de proporcionar información sobre cómo obtener ayuda.

**Licencias**

Asegúrese de que la aplicación está cubierta por los siguientes requisitos de licencia:

* **Licencias de Microsoft Entra**: el inicio de sesión único para las aplicaciones empresariales preintegradas es gratuito. Pero es posible que el número de objetos en el directorio y las características que quiere implementar requieran licencias adicionales.
* **Licencias de aplicaciones**: necesitará las licencias adecuadas para las aplicaciones con el fin de satisfacer las necesidades empresariales. Trabaje con el propietario de la aplicación para determinar si los usuarios asignados a la aplicación tienen las licencias adecuadas para sus roles dentro de ella. Si Microsoft Entra ID administra el aprovisionamiento automático en función de los roles, los roles asignados en Microsoft Entra ID se deben alinear con el número de licencias que posee dentro de la aplicación. Un número incorrecto de las licencias que se poseen en la aplicación puede dar lugar a errores durante el aprovisionamiento o la actualización de una cuenta de usuario.

**Cuentas compartidas**

Desde la perspectiva del inicio de sesión, las aplicaciones con cuentas compartidas no son diferentes de las aplicaciones empresariales en las que se usa el inicio de sesión único con contraseña para usuarios individuales. Pero es necesario realizar más pasos al planear y configurar una aplicación diseñada para usar cuentas compartidas.

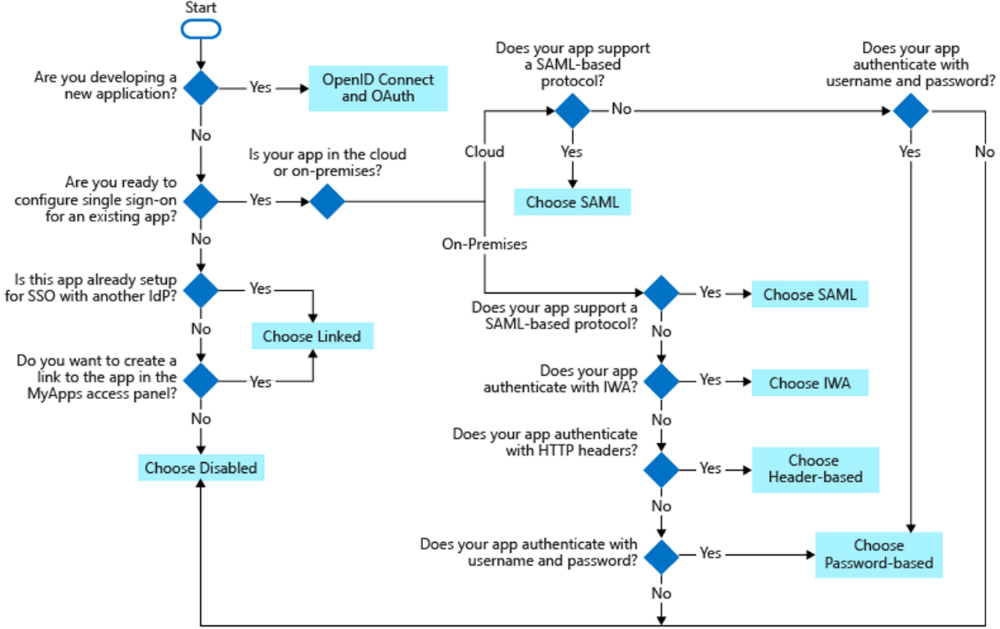
* Trabaje con los usuarios para documentar la siguiente información:
  + El conjunto de usuarios de la organización que van a usar la aplicación.
  + El conjunto existente de credenciales en la aplicación asociadas con el conjunto de usuarios.
* Para cada combinación de conjunto de usuarios y credenciales, cree un grupo de seguridad local en la nube según los requisitos.
* Restablezca las credenciales compartidas. Una vez implementada la aplicación en Microsoft Entra ID, los usuarios no necesitan la contraseña de la cuenta compartida. Microsoft Entra ID almacena la contraseña, por lo que debería considerar la posibilidad de establecer una contraseña larga y compleja.
* Si la aplicación lo admite, configure la sustitución automática de la contraseña. De ese modo, ni siquiera el administrador que ha realizado la instalación inicial conoce la contraseña de la cuenta compartida.

**Opciones de inicio de sesión único**

Hay varias maneras de configurar una aplicación para el inicio de sesión único. La elección de un método de SSO depende de cómo esté configurada la aplicación para la autenticación.

* Las aplicaciones en la nube pueden usar los métodos OpenID Connect, OAuth, SAML, basado en contraseña o vinculado para el inicio de sesión único. El inicio de sesión único también se puede deshabilitar.
* Las aplicaciones locales pueden usar métodos de inicio de sesión único basado en contraseña, de Autenticación integrada de Windows, basado en encabezados o vinculado para el inicio de sesión único. Las opciones locales funcionan si las aplicaciones están configuradas para Application Proxy.

Este diagrama de flujo puede ayudarle a decidir qué método de inicio de sesión único es el mejor en su caso.



Los siguientes protocolos de SSO están disponibles:

* **OpenID Connect y OAuth**: elija OpenID Connect y OAuth 2.0 si la aplicación a la que se va a conectar lo admite.
* **SAML**: elija SAML siempre que sea posible para las aplicaciones existentes que no usan OpenID Connect o OAuth.
* **Basado en contraseña**: elija el inicio de sesión basado en contraseña cuando la aplicación tenga una página de inicio de sesión HTML. El SSO basado en contraseña también se conoce como almacenamiento de contraseñas. El SSO basado en contraseña permite administrar el acceso y las contraseñas de los usuarios en aplicaciones web que no admiten la federación de identidades. También es útil cuando varios usuarios necesitan compartir una sola cuenta, como las cuentas de aplicaciones de redes sociales de la organización. El SSO basado en contraseña admite aplicaciones que requieren varios campos de inicio de sesión para aplicaciones que no solo requieren los campos de nombre de usuario y contraseña para iniciar sesión. Puede personalizar las etiquetas de los campos de nombre de usuario y contraseña que los usuarios ven en la página Aplicaciones cuando escriben sus credenciales.
* **Vinculado**: elija el inicio de sesión vinculado si la aplicación está configurada para el SSO en otro servicio de proveedor de identidades. La opción Vinculado permite configurar la ubicación de destino cuando un usuario selecciona la aplicación de los portales de usuario final de la organización. Puede agregar un vínculo a una aplicación web personalizada que actualmente use la federación, como Microsoft Entra Domain Federation Services. También puede agregar vínculos a páginas web específicas que quiera que aparezcan en los paneles de acceso de su usuario y a una aplicación que no requiera autenticación. La opción Vinculado no proporciona la funcionalidad de inicio de sesión a través de las credenciales de Microsoft Entra.
* **Deshabilitado**: elija el SSO deshabilitado cuando la aplicación no esté lista para configurarse para el inicio de sesión único.
* **Autenticación integrada de Windows (IWA)** : elija el inicio de sesión único de IWA para aplicaciones que usen IWA o aplicaciones compatibles con notificaciones. Para obtener más información, consulte Delegación restringida de Kerberos para el inicio de sesión único (SSO) para las aplicaciones con Application Proxy.
* **Basado en encabezados**: use el inicio de sesión único basado en encabezados si la aplicación usa encabezados para la autenticación.

**Integrar el inicio de sesión único (SSO) y los proveedores de identidades**

Puede integrar las aplicaciones de software como servicio (SaaS) habilitadas para la nube con Microsoft Entra ID. Consulte Microsoft Entra ID Marketplace para obtener una lista de todas las aplicaciones SaaS que se han integrado previamente en Microsoft Entra ID. Use el portal de red de aplicaciones para solicitar que se agregue una aplicación habilitada para System for Cross-Domain Identity Management (SCIM) a la galería para el aprovisionamiento automático o la aplicación habilitada para SAML/OpenID Connect (OIDC) para agregarse a la galería para el inicio de sesión único. Una vez que agregue la aplicación desde la galería, configure y pruebe el inicio de sesión único de Microsoft Entra ID para la aplicación.

**Proveedores de software como servicio (SaaS) habilitados para la nube**

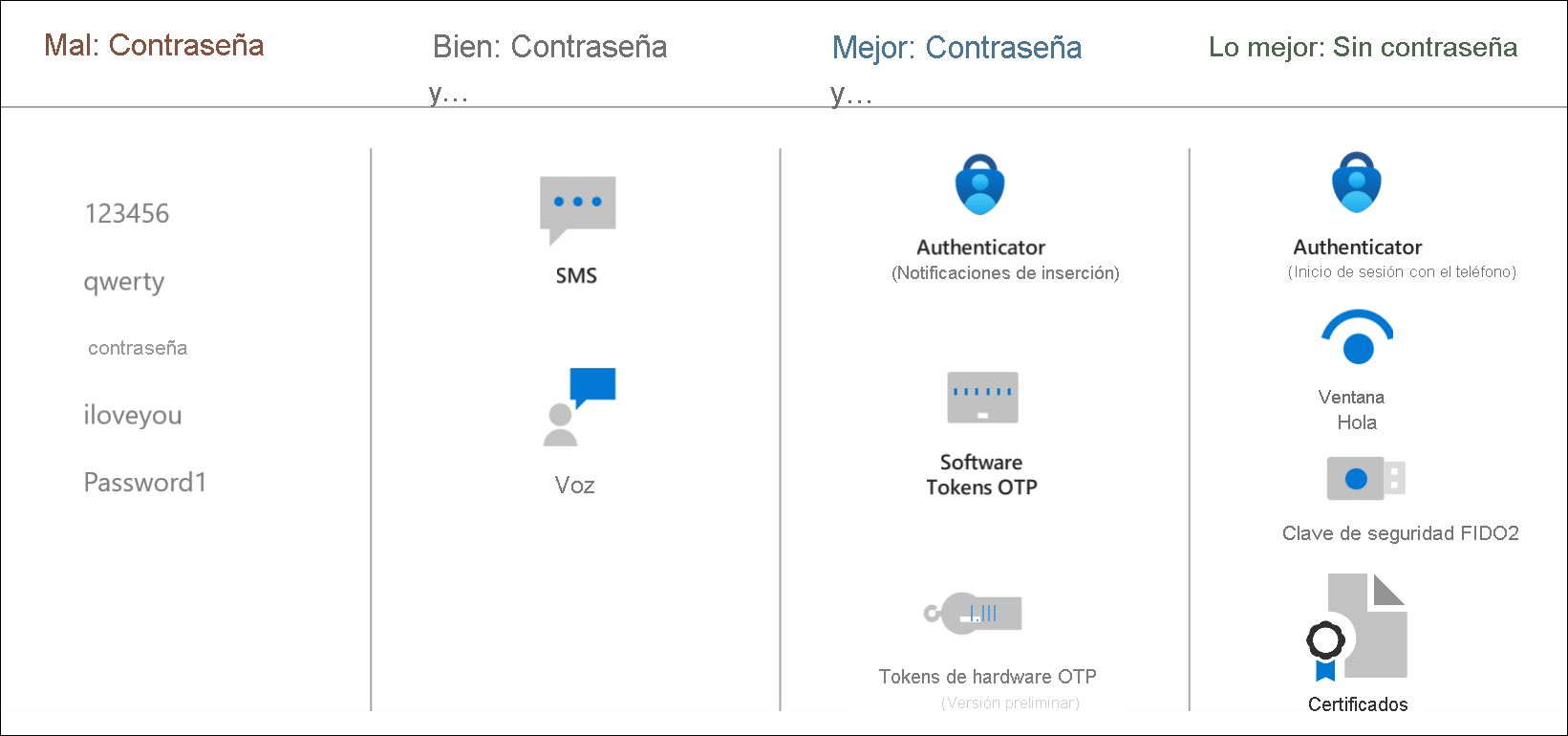
* Atlassian Cloud
* ServiceNow
* Slack
* SuccessFactors
* Workday

**Integraciones en la nube**

* Consola de Amazon Web Services (AWS)
* Alibaba Cloud (SSO basado en roles)
* Google Cloud Platform
* Salesforce
* Plataforma de identidad en la nube de SAP (Sistemas, aplicaciones y productos de procesamiento de datos)

**Recomendación y aplicación de protocolos de autenticación modernos**

Microsoft recomienda los métodos de autenticación sin contraseña, como Windows Hello, las claves de seguridad FIDO2 y la aplicación Microsoft Authenticator, ya que son los proporcionan un inicio de sesión más seguro. Aunque los usuarios pueden iniciar sesión con otros métodos comunes, como un nombre de usuario y una contraseña, las contraseñas deben reemplazarse por métodos de autenticación más seguros.



La autenticación multifactor de Microsoft Entra agrega seguridad adicional con respecto al uso exclusivo de una contraseña cuando un usuario inicia sesión. Se pueden solicitar al usuario formas adicionales de autenticación, como responder a una notificación push, especificar un código de un token de software o hardware, o responder a un SMS o a una llamada de teléfono.

Para simplificar la experiencia de incorporación de los usuarios y registrarse tanto para MFA como para el autoservicio de restablecimiento de contraseña (SSPR), se recomienda habilitar el registro de información de seguridad combinada. Para mejorar la resistencia, se recomienda exigir a los usuarios que registren varios métodos de autenticación. Así, si un usuario no tiene disponible un método durante el inicio de sesión o el autoservicio de restablecimiento de contraseña, puede elegir autenticarse con otro método.

**Seguridad del método de autenticación**

Cuando implemente características como la autenticación multifactor Microsoft Entra en su organización, revise los métodos de autenticación disponibles. Elija los métodos que cumplan o superen sus requisitos en cuanto a seguridad, facilidad de uso y disponibilidad. Siempre que sea posible, use métodos de autenticación con el nivel de seguridad más alto.

En la tabla siguiente se describen las consideraciones sobre seguridad que se deben tener en cuenta en los métodos de autenticación disponibles. La disponibilidad es una indicación de que el usuario puede usar el método de autenticación, no de la disponibilidad del servicio en Microsoft Entra ID:

| **Método de autenticación** | **Seguridad** | **Facilidad de uso** | **Disponibilidad** |
| --- | --- | --- | --- |
| Windows Hello para empresas | Alto | Alto | Alto |
| Microsoft Authenticator | Alto | Alto | Alto |
| Authenticator Lite | Alto | Alto | Alto |
| Clave de seguridad FIDO2 | Alto | Alto | Alto |
| Autenticación basada en certificados | Alto | Alto | Alto |
| Tokens de hardware OATH (versión preliminar) | Media | Media | Alto |
| Tokens de software OATH | Media | Media | Alto |
| Pase de acceso temporal (TAP) | Media | Alto | Alto |
| SMS | Media | Alto | Media |
| Voz | Media | Media | Media |
| Contraseña | Bajo | Alto | Alto |

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Cuál es la responsabilidad principal del servicio del agente de controlador de dominio en la protección con contraseña de Microsoft Entra?**

1. Descargar una nueva directiva de contraseñas de Microsoft Entra ID.
2. Crear un objeto serviceConnectionPoint en Microsoft Entra ID.
3. Procesar las solicitudes de validación de contraseñas desde el archivo DLL de filtro de contraseña del agente de controlador de dominio mediante la directiva de contraseñas actual disponible localmente y devolver el resultado de aprobada o denegada

**2. ¿Qué hace System for Cross-domain Identity Management (SCIM)?**

1. Proporciona una lista de todas las aplicaciones SaaS que se han integrado previamente en Microsoft Entra ID.
2. Permite la automatización y la validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables
3. Permite el aprovisionamiento automático de cuentas de usuario y grupos en distintos sistemas

**3. ¿Qué habilita Microsoft Entra Verified ID?**

1. Permite la automatización y la validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables
2. Habilita la creación de máquinas virtuales para la informática en la nube
3. Habilita la comprobación de credenciales emitidas por otras organizaciones

**4. Un comprobador usa su propio inquilino de Microsoft Entra para realizar la comprobación de la credencial emitida por otra organización. ¿Cuál es el propósito de usar el servicio de Microsoft Entra Verified ID para la comprobación?**

1. Emitir credenciales verificables mediante su propio inquilino
2. Descargar ngrok y registrarse para obtener una cuenta gratuita
3. Desbloquear privilegios a los sujetos que poseen tarjetas de expertos de credenciales comprobadas

**5.Una empresa planea implementar el inicio de sesión único con sus aplicaciones en Microsoft Entra ID. Deben tener en cuenta los roles administrativos, la renovación de certificados, la comunicación y las licencias. ¿Cuál de las siguientes afirmaciones se aplica al certificado de aplicación SAML?**

1. No se puede personalizar el certificado.
2. El certificado es válido durante un año de forma predeterminada.
3. El certificado debe renovarse antes de su expiración y la fecha de expiración se puede personalizar en el Centro de administración de Microsoft Entra.
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, los participantes aprenderán a configurar el id. comprobado de Entra, implementar MFA, autenticación sin contraseña, protección con contraseña, SSO, integración con proveedores de identidades y mejorar la seguridad a través de protocolos de autenticación modernos.