

¿Qué es el autoservicio de restablecimiento de contraseña de Azure Active Directory?

Se le ha pedido que evalúe las maneras de reducir los costos del departamento de soporte técnico en la organización comercial. Se ha detectado que el personal de soporte técnico dedica gran parte de su tiempo a restablecer las contraseñas de los usuarios. A menudo, los usuarios se quejan de retrasos con este proceso y estos retrasos afectan a su productividad. Queremos saber cómo podemos configurar Azure para permitir que los usuarios administren sus propias contraseñas.

En esta unidad, veremos cómo funciona el autoservicio de restablecimiento de contraseña (SSPR) de Azure Active Directory (Azure AD).

¿Por qué usar SSPR?

En Azure AD, cualquier usuario puede cambiar su contraseña si ya ha iniciado sesión, pero si no ha iniciado sesión y ha olvidado su contraseña o ha expirado, deberá restablecer su contraseña. Con SSPR, los usuarios pueden restablecer sus contraseñas en un explorador web o en una pantalla de inicio de sesión de Windows para poder volver a acceder a Azure, Microsoft 365 y cualquier otra aplicación que use Azure AD para la autenticación.

SSPR reduce la carga de los administradores, ya que los usuarios pueden solucionar los problemas de contraseña por sí mismos, sin tener que acudir al departamento de soporte técnico. Además, reduce el impacto en la productividad que conlleva una contraseña olvidada o caducada. Los usuarios no tienen que esperar a que un administrador esté disponible para restablecer su contraseña.

Cómo funciona SSPR

El usuario inicia un restablecimiento de contraseña yendo directamente al portal de restablecimiento de contraseña o seleccionando el vínculo **No puede acceder a su cuenta** en una página de inicio de sesión. En el portal de restablecimiento se llevan a cabo estos pasos:

1. **Localización:** El portal comprueba la configuración regional del explorador y representa la página SSPR en el idioma correspondiente.
2. **Comprobación:** el usuario escribe su nombre de usuario y pasa un captcha para garantizar que es un usuario, y no un robot.
3. **Autenticación:** el usuario escribe los datos necesarios para autenticar su identidad; por ejemplo, podría escribir un código o responder preguntas de seguridad.
4. **Restablecimiento de contraseña:** Si el usuario pasa las pruebas de autenticación, puede escribir una nueva contraseña y confirmarla.
5. **Notificación:** se envía un mensaje al usuario para confirmar el restablecimiento.

Existen diversas formas de personalizar la experiencia de usuario de SSPR. Por ejemplo, podemos agregar el logotipo de la empresa a la página de inicio de sesión para que los usuarios sepan que están en el lugar adecuado para restablecer la contraseña.

Autenticación de un restablecimiento de contraseña

Antes de permitir un restablecimiento de contraseña, es fundamental confirmar la identidad de un usuario. Los usuarios malintencionados podrían aprovechar cualquier debilidad del sistema para suplantar a ese usuario. Azure admite seis maneras diferentes de autenticar solicitudes de restablecimiento.

Como administrador, debe elegir los métodos que se van a usar al configurar SSPR. Habilite dos o más de estos métodos para que los usuarios puedan elegir los que pueden usar con facilidad. Los métodos son los siguientes:

Método de autenticación	Cómo registrarse	Cómo autenticar un restablecimiento de contraseña
Notificación en aplicación móvil	Instale la aplicación Microsoft Authenticator en el dispositivo móvil y regístrela en la página Configuración de la autenticación multifactor.	Azure envía una notificación a la aplicación, que se puede confirmar o denegar.
Código de aplicación móvil	Este método también usa la aplicación Authenticator y se instala y registra de la misma manera.	Escriba el código de la aplicación.
Correo electrónico	Indique una dirección de correo electrónico que sea ajena a Azure y Microsoft 365.	Azure envía un código a la dirección, que hay que introducir en el asistente de restablecimiento.
Teléfono móvil	Indique un número de teléfono móvil.	Azure envía un código al teléfono en un mensaje SMS, que se escribe en el Asistente para restablecer. También se puede optar por recibir una llamada automatizada.
Teléfono del trabajo	Proporcione un número de teléfono no móvil.	Se recibirá una llamada automatizada a dicho número, y habrá que presionar #.
Preguntas de seguridad	Seleccione preguntas como "¿En qué ciudad nació su madre?" y guarde las respuestas.	Responda las preguntas.

En las organizaciones de Azure AD gratuitas y de prueba no se admiten las opciones de llamada de teléfono.

Requerimiento del número mínimo de métodos de autenticación

Se puede especificar un número mínimo de métodos que el usuario debe configurar: uno o dos. Por ejemplo, puede habilitar los métodos de código de aplicación móvil, correo electrónico, teléfono de la oficina y preguntas de seguridad y especificar un mínimo de dos métodos. Después, los usuarios pueden elegir los dos métodos que prefieran, como el correo electrónico y el código de la aplicación móvil.

En el caso del método de preguntas de seguridad, puede especificar un número mínimo de preguntas que el usuario debe configurar para registrarse para este método. También puede especificar un número mínimo de preguntas que deben responder correctamente para restablecer la contraseña.

Una vez que los usuarios registren la información necesaria para el número mínimo de métodos que ha especificado, se consideran registrados para SSPR.

Recomendaciones

- Habilite dos o más métodos de solicitud de restablecimiento de autenticación.
- Use códigos o notificaciones de aplicación móvil como método principal, pero habilite también los métodos de teléfono de la oficina o de correo electrónico para dar cabida a los usuarios que no tengan dispositivos móviles.
- El método del teléfono móvil no es un método recomendado, ya que se pueden enviar mensajes SMS fraudulentos.
- La opción de preguntas de seguridad es el método menos recomendable, porque existe la posibilidad de que otras personas conozcan las respuestas a esas preguntas. Use el método de preguntas de seguridad únicamente en combinación con al menos otro de los métodos.

Cuentas asociadas a roles de administrador

- Las cuentas con un rol de administrador siempre tienen aplicada una directiva de autenticación de dos métodos muy sólida, independientemente de la configuración de otros usuarios.
- El método de preguntas de seguridad no está disponible en las cuentas asociadas a un rol de administrador.

Configuración de notificaciones

Los administradores pueden elegir cómo se va a notificar a los usuarios de los cambios de contraseña. Se pueden habilitar dos opciones:

- **¿Quiere notificar a los usuarios los restablecimientos de contraseña?:** el usuario que restablezca su propia contraseña recibirá una notificación en sus direcciones de correo electrónico principal y secundaria. Si el restablecimiento lo ha realizado un usuario malintencionado, dicha notificación avisará al usuario, que puede tomar medidas de mitigación de riesgos.
- **¿Quiere notificar a todos los administradores cuando otros administradores restablezcan su contraseña?:** cuando un administrador restablezca su contraseña, se notificará a todos los demás administradores.

Requisitos de licencia

Las ediciones de Azure AD son gratis, Premium P1 y Premium P2. La funcionalidad de restablecimiento de contraseña que se puede usar dependerá de la edición.

Cualquier usuario que haya iniciado sesión puede cambiar su contraseña, independientemente de la edición de Azure AD que posea.

Si no ha iniciado sesión y ha olvidado la contraseña, o esta ha expirado, puede usar SSPR en Azure AD Premium P1 o P2. También está disponible con Aplicaciones de Microsoft 365 para negocios o Microsoft 365.

En una situación híbrida donde haya Active Directory en un entorno local y Azure AD en la nube, cualquier cambio de contraseña en la nube se debe volver a escribir en el directorio local. Esta compatibilidad con escritura diferida está disponible en Azure AD Premium, tanto P1 como P2. También está disponible con Aplicaciones de Microsoft 365 para negocios.

Opciones de implementación de SSPR

Puede implementar SSPR con escritura diferida de contraseñas mediante [Azure AD Connect](#) o [Cloud Sync](#) en la nube, en función de las necesidades de los usuarios. Cada opción se puede implementar en paralelo en dominios diferentes para dirigirse a distintos conjuntos de usuarios. Esto ayuda a los usuarios existentes locales a reescribir los cambios de contraseña al tiempo que se agrega una opción para los usuarios de dominios desconectados debido a una fusión o división de la empresa. Los usuarios de un dominio local existente pueden utilizar Azure AD Connect mientras que los nuevos usuarios de una fusión pueden utilizar la sincronización en la nube en otro dominio. La sincronización en la nube también puede proporcionar una mayor disponibilidad porque no se basa en una sola instancia de Azure AD Connect. Para obtener una comparación de características entre las dos opciones de implementación, consulte [Comparación entre Azure AD Connect y la sincronización en la nube](#).

1. ¿Cuándo se considera que un usuario está registrado en SSPR?

- ☐ Cuando hayan registrado al menos uno de los métodos de autenticación permitidos
- ☒ Cuando hayan registrado al menos el número de métodos necesarios para restablecer una contraseña

✓ Se considera que un usuario está registrado en SSPR si ha registrado como mínimo el número de métodos necesarios para restablecer una contraseña. Este número se establece en Azure Portal.

- ☐ Cuando hayan configurado el número mínimo de preguntas de seguridad

2. Cuando SSPR está habilitado en la organización de Azure AD...

- ☐ Los usuarios solo pueden cambiar su contraseña cuando han iniciado sesión
- ☐ Los administradores pueden restablecer sus contraseñas mediante un método de autenticación
- ☒ Los usuarios pueden restablecer sus contraseñas cuando no pueden iniciar sesión

✓ Si el usuario pasa las pruebas de autenticación, puede restablecer su contraseña.

Implementación del autoservicio de restablecimiento de contraseña de Azure AD

Ha decidido implementar el autoservicio de restablecimiento de contraseña (SSPR) en Azure Active Directory (Azure AD) de su organización. Queremos empezar a usar SSPR con un grupo de 20 usuarios del departamento de marketing a modo de implementación de prueba. Si todo va bien, habilitaremos SSPR en toda la organización.

En esta unidad, veremos cómo habilitar SSPR en Azure AD.

Requisitos previos

Antes de empezar a configurar SSPR, necesitamos estos elementos:

- Una organización de Azure AD. Esta organización debe tener al menos una licencia de prueba habilitada.
- Una cuenta de Azure AD con privilegios de administrador global. La usaremos para configurar SSPR.
- Una cuenta de usuario no administrativo. La usaremos para comprobar SSPR. Es importante que esta cuenta no sea un administrador, ya que Azure AD impone más requisitos en las cuentas administrativas de SSPR. Este usuario, y todas las cuentas de usuario, deben tener una licencia válida para usar SSPR.
- Un grupo de seguridad con el que probar la configuración. La cuenta de usuario no administrativo debe ser miembro de este grupo. Usaremos este grupo de seguridad para limitar en qué usuarios implementaremos SSPR.

Si aún no tenemos una organización de Azure AD que podamos usar en este módulo, configuraremos una en la unidad siguiente.

Ámbito de la implementación de SSPR

Hay tres opciones de configuración en la propiedad **Se habilitó el restablecimiento de contraseña del autoservicio**:

- **Deshabilitado**: ningún usuario de la organización de Azure AD puede usar SSPR. Este es el valor predeterminado.
- **Habilitado**: todos los usuarios de la organización de Azure AD pueden usar SSPR.
- **Seleccionado**: solo los miembros del grupo de seguridad especificado pueden usar SSPR. Esto permite habilitar SSPR en un grupo de usuarios concreto, que puede probarlo y comprobar que funciona según lo previsto. Cuando todo esté listo para llevar a cabo la implementación global, establezca la propiedad en **Habilitado**, así todos los usuarios tendrán acceso a SSPR.

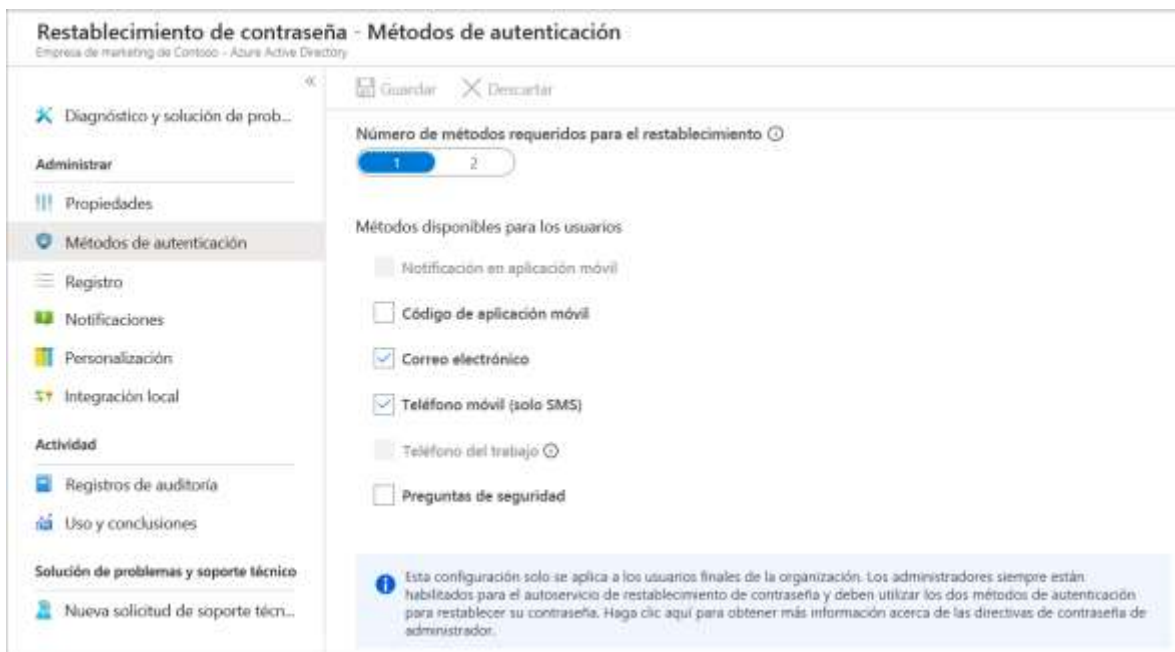
Configuración de SSPR

Estos son los pasos de alto nivel para configurar SSPR.

1. En [Azure Portal](#), vaya a **Active Directory>Restablecimiento de contraseña**.
2. Propiedades:
 - Habilite SSPR.
 - Puede habilitarlo para todos los usuarios de la organización de Azure AD o solo para determinados usuarios.
 - Para habilitarlo para determinados usuarios, debe especificar el grupo de seguridad. Los miembros de este grupo pueden usar SSPR.



3. Métodos de autenticación:
 - Elija si desea requerir uno o dos métodos de autenticación.
 - Elija los métodos de autenticación que los usuarios pueden usar.



4. Registro:

- Especifique si los usuarios deben registrarse en SSPR la próxima vez que inicien sesión.
- Especifique con qué frecuencia se va a pedir a los usuarios que vuelvan a confirmar su información de autenticación.

Restablecimiento de contraseña: registro
Empresa de marketing de Contoso - Azure Active Directory

« Guardar Descartar

Diagnóstico y solución de problemas

Administrar

Propiedades

Métodos de autenticación

Registro

Notificaciones

Personalización

On-premises integration

¿Es necesario que los usuarios se registren al iniciar sesión? ⓘ

☒ Sí ☐ No

Número de días antes de que se solicite a los usuarios que vuelvan a confirmar su información de autenticación ⓘ

180

ⓘ Esta configuración solo se aplica a los usuarios finales de la organización. Los administradores siempre están habilitados para el autoservicio de restablecimiento de contraseña y deben utilizar los dos métodos de autenticación para restablecer su contraseña. Haga clic aquí para obtener más información acerca de las directivas de contraseña de administrador.

5. Notificaciones: Elija si se va a notificar a los usuarios y a los administradores los restablecimientos de contraseñas.

Restablecimiento de contraseña - Notificaciones
Empresa de marketing de Contoso - Azure Active Directory

« Guardar Descartar

Diagnóstico y solución de prob...

Administración

Propiedades

Métodos de autenticación

Registro

Notificaciones

Personalización

Integración local

¿Quiere notificar a los usuarios los restablecimientos de contraseña? ⓘ

☒ Sí ☐ No

¿Quiere notificar a todos los administradores cuando otros administr... ⓘ

☐ Sí ☒ No

6. Personalización: Indique una dirección de correo electrónico o una dirección URL de página web donde los usuarios puedan obtener ayuda.

Restablecimiento de contraseña - Personalización
Empresa de marketing de Confianza · Azure Active Directory

Guardar Descartar

Personalizar el vínculo del departamento de soporte técnico ⓘ

☒ Sí ☐ No

Dirección URL o correo electrónico del departamento de soporte técnico personalizados ⓘ

https://helpdesk.organization.com ✓

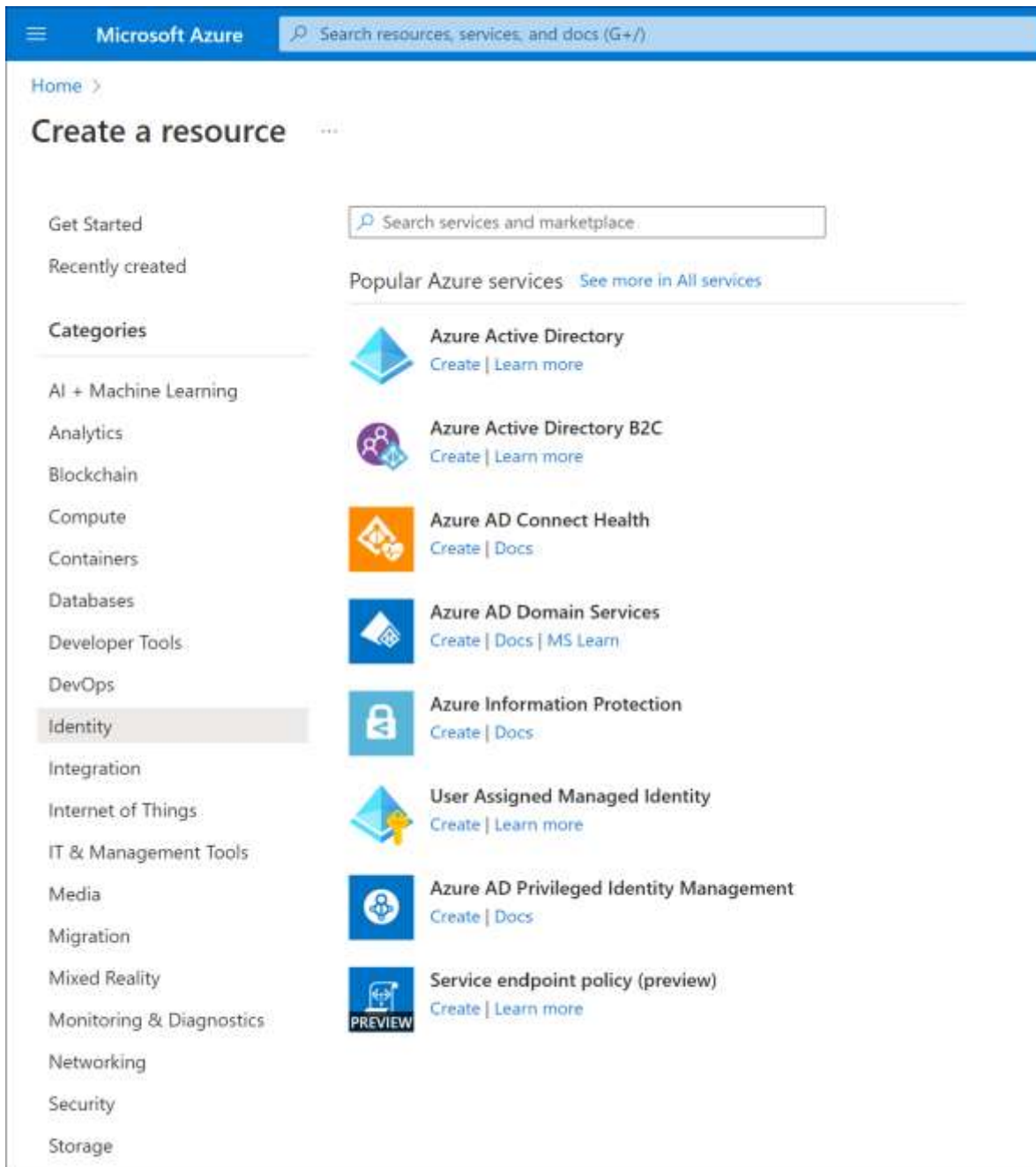
Ejercicio: configurar el autoservicio de restablecimiento de contraseña

En esta unidad, configuraremos y comprobaremos el autoservicio de restablecimiento de contraseña (SSPR) con un teléfono móvil. Deberá usar su teléfono móvil para completar el proceso de restablecimiento de contraseña en este ejercicio.

Creación de una organización de Azure AD

La organización de Azure Active Directory (Azure AD) predeterminada en el espacio aislado de Azure no es compatible con SSPR, por lo que en este ejercicio crearemos una segunda organización y cambiaremos a ella.

1. Inicie sesión en [Azure Portal](#) con la misma cuenta que ha usado para activar el espacio aislado.
2. Seleccione **Crear un recurso>Identidad>Azure Active Directory**.



3. Seleccione **Azure Active Directory** y, a continuación, seleccione **Siguiente: Configuración**.
4. En la página **Crear inquilino** use estos valores, seleccione **Revisar y crear** y, a continuación, seleccione **Crear**.

Propiedad

Valor

Nombre de la organización Elija cualquier nombre de organización.

Nombre de dominio inicial Elija un nombre de dominio que sea único en **.onmicrosoft.com**. Anote el n

Propiedad**Valor**

País o región

Estados Unidos.

5. Escriba los caracteres del captcha y, a continuación, seleccione **Enviar**.
6. Después de crear la organización, pulse la tecla F5 para actualizar la página. En la esquina superior derecha, seleccione su cuenta de usuario. A continuación, seleccione **Cambiar directorio**.
7. Seleccione la organización que acabamos de crear.

Creación de una suscripción de prueba de Azure AD Premium P2

Ahora vamos a activar una suscripción de prueba Premium para la organización para que podamos probar SSPR.

1. Vaya a **Azure Active Directory>Restablecimiento de contraseña**.
2. Seleccione **Obtener una prueba gratuita Premium para usar esta característica**.
3. En **AZURE AD PREMIUM P2**, expanda **Prueba gratuita** y después seleccione **Activar**.
4. Actualice el explorador para ver la página **Restablecimiento de contraseña: Propiedades**.

Creación de un grupo

Queremos implementar SSPR en un conjunto limitado de usuarios en primer lugar para asegurarnos de que la configuración de SSPR funciona según lo previsto. Vamos a comenzar creando un grupo de seguridad para esta implementación limitada.

1. En la organización de Azure AD que creamos, en **Administrar**, seleccione **Grupos**.
2. Seleccione **+ Nuevo grupo**.
3. Escriba los siguientes valores:

Configuración**Valor**

Tipo de grupo

Seguridad

Nombre del grupo

SSPRTesters

Descripción del grupo

Evaluadores de implementación de SSPR

Tipo de pertenencia

Asignada

4. Seleccione **Crear**.

Nuevo grupo

* Tipo de grupo

Seguridad

* Nombre de grupo ⓘ

SSPRTesters

Descripción del grupo ⓘ

Los miembros están probando la implementación de SSPR

* Tipo de pertenencia ⓘ

Asignado

Propietarios

>

Miembros

>

Crear

Creación de una cuenta de usuario

Para probar la configuración, cree una cuenta que no esté asociada a un rol de administrador.

1. En la organización de Azure AD, en **Administrar**, seleccione **Usuarios**.
2. Seleccione **+ Nuevo usuario** y use los siguientes valores:

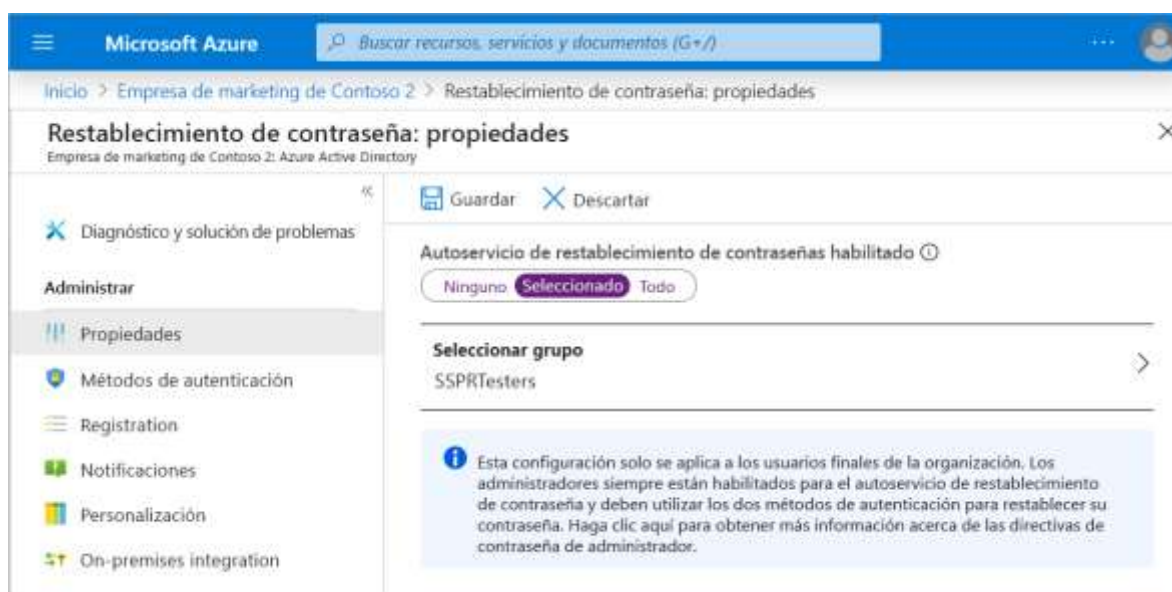
Opción	Valor
Nombre de usuario	balas
Nombre	Bala Sandhu
Contraseña	Seleccione Mostrar contraseña y anótela.
Grupos	Seleccione SSPRTesters.

3. Seleccione **Crear**.

Habilitación de SSPR

Ahora todo está listo para habilitar SSPR para el grupo.

1. En la organización de Azure AD, en **Administrar**, seleccione **Restablecimiento de contraseña**.
2. Si en la página **Restablecimiento de contraseña** se sigue mostrando el mensaje **Obtener una prueba gratuita Premium para usar esta característica**, espere unos minutos y actualice la página.
3. En la página **Propiedades**, seleccione **Seleccionado**. Seleccione el grupo **SSPRTesters** y después **Guardar**.



4. En **Administrar**, seleccione las páginas **Métodos de autenticación**, **Registro** y **Notificaciones** para revisar los valores predeterminados.
5. Seleccione **Personalización**.
6. Seleccione **Sí** y después, en el cuadro de texto **Dirección URL o correo electrónico del departamento de soporte técnico personalizados**, escriba admin@organization-domain-name.onmicrosoft.com. Reemplace "organization-domain-name" por el nombre de dominio de la organización de Azure AD creada. Si ha olvidado el nombre de dominio, mueva el puntero sobre el perfil en la esquina superior derecha de Azure Portal.
7. Seleccione **Guardar**.

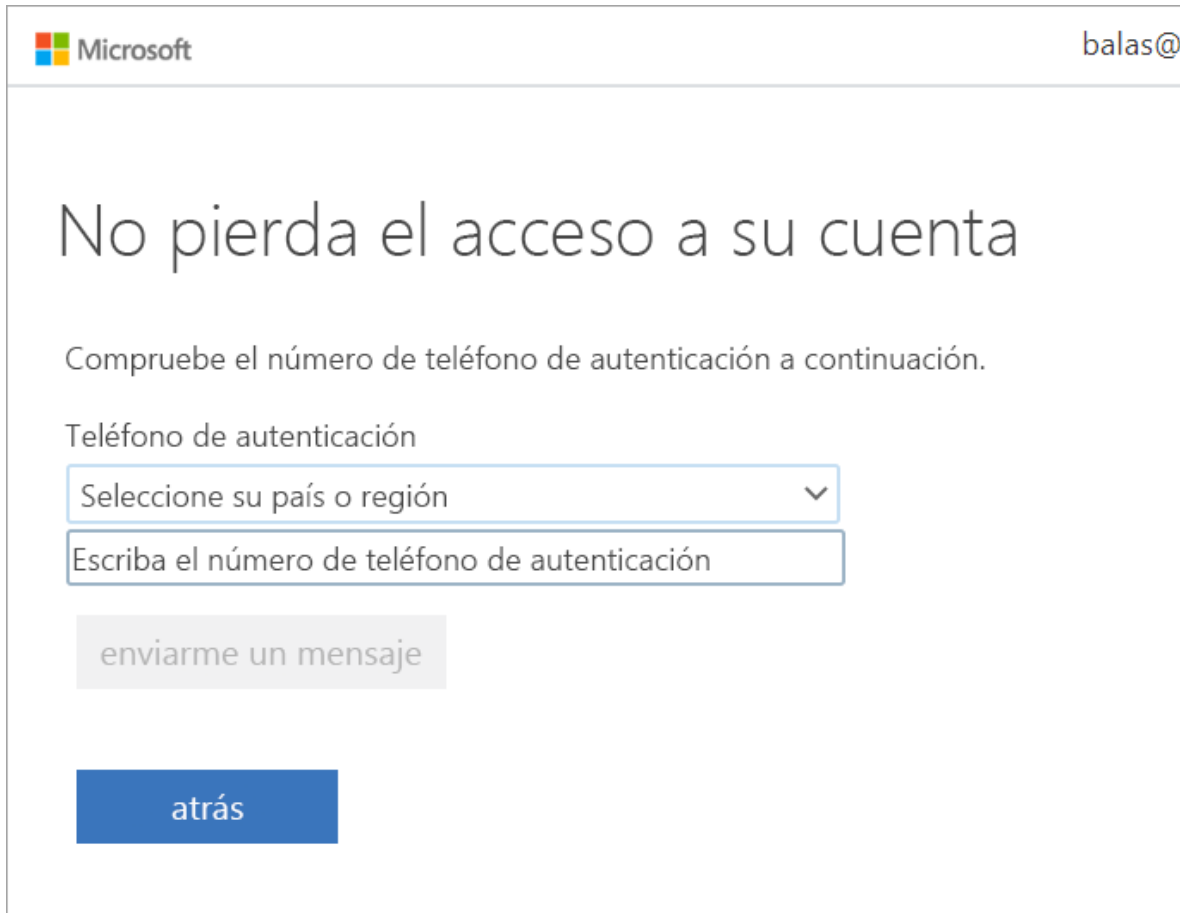
Registro en SSPR

Ahora que ya tenemos completada la configuración de SSPR, podemos registrar un número de teléfono móvil para el usuario que hemos creado.

Nota

Si recibe el mensaje "The administrator has not enabled this feature" (El administrador no ha habilitado esta característica), use el modo privado o de incógnito en el explorador web.

1. En una nueva ventana del explorador, vaya a <https://aka.ms/ssprsetup>.
2. Inicie sesión con el nombre de usuario balas@organization-domain-name.onmicrosoft.com y la contraseña que anotó anteriormente.
3. Si se le pide que actualice la contraseña, escriba otra nueva que prefiera. No olvide anotar la nueva contraseña.
4. Junto a **El teléfono de autenticación no está configurado**, seleccione **Configurarlo ahora**.
5. Escriba los detalles del teléfono móvil.



The screenshot shows a Microsoft account recovery interface. At the top left is the Microsoft logo, and at the top right is the email address 'balas@'. The main heading is 'No pierda el acceso a su cuenta'. Below this, it says 'Compruebe el número de teléfono de autenticación a continuación.' The section is titled 'Teléfono de autenticación'. There are two input fields: the first is a dropdown menu labeled 'Seleccione su país o región' with a downward arrow, and the second is a text box labeled 'Escriba el número de teléfono de autenticación'. Below these fields is a button labeled 'enviarme un mensaje'. At the bottom left of the form area is a blue button labeled 'atrás'.

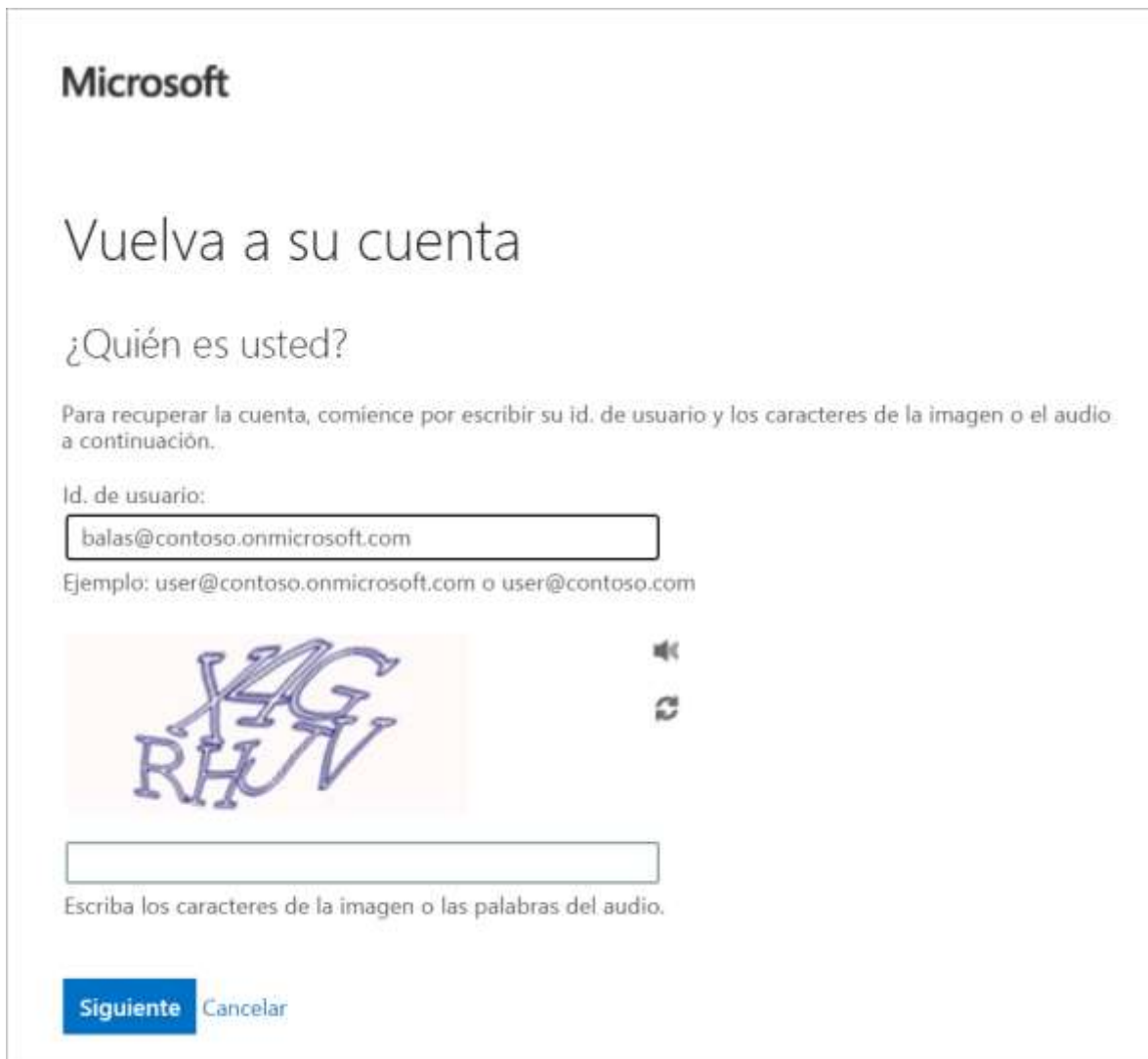
6. Seleccione **enviarme mensaje de texto**.
7. Cuando reciba el código en el teléfono móvil, escríbalo en el cuadro de texto.
8. Seleccione **comprobar** y después seleccione **finalizar**.

Comprobación de SSPR

Ahora vamos a comprobar si el usuario puede restablecer su contraseña.

1. En una nueva ventana del explorador, vaya a <https://aka.ms/sspr>.

2. En **Id. de usuario**, escriba `balas@organization-domain-name.onmicrosoft.com`. Reemplace "organization-domain-name" por el nombre de dominio que se ha usado para la organización de Azure AD.



Microsoft




Vuelva a su cuenta

¿Quién es usted?

Para recuperar la cuenta, comience por escribir su id. de usuario y los caracteres de la imagen o el audio a continuación.

Id. de usuario:

Ejemplo: user@contoso.onmicrosoft.com o user@contoso.com



Escriba los caracteres de la imagen o las palabras del audio.

Siguiete Cancelar

3. Escriba los caracteres del captcha y seleccione **Siguiete**.
4. Escriba el número de teléfono móvil y seleccione **Texto**.
5. Cuando le llegue el mensaje de texto, escriba el código que se le ha enviado en el cuadro de texto **Escriba el código de verificación**. Haga clic en **Siguiete**.
6. Escriba la nueva contraseña y seleccione **Finalizar**. No olvide anotar la nueva contraseña.
7. Cierre la sesión en la cuenta.

Ejercicio: personalizar la información de marca de directorio

Supongamos que nos han pedido que la página de inicio de sesión de Azure muestre la información de marca de la organización minorista para que los usuarios puedan tener la tranquilidad de que están introduciendo credenciales en un sistema legítimo.

Aquí aprenderemos a configurar esta información de marca personalizada.

Para completar este ejercicio, debemos tener dos archivos de imagen:

- Una imagen de fondo de la página. Debe ser un archivo PNG o JPG de 1920 × 1080 píxeles y menos de 300 KB.
- Una imagen de logotipo de la compañía. Debe ser un archivo PNG o JPG de 280 × 60 píxeles y menos de 10 KB.

Personalización de la información de marca de una organización de Azure AD

Vamos a usar Azure Active Directory (Azure AD) para configurar la información de marca personalizada.

1. Inicie sesión en [Azure Portal](#) con la misma cuenta que ha usado para activar el espacio aislado.
2. Seleccione **Azure Active Directory** para ir a la organización de Azure AD. Si no está en la organización de Azure AD correcta, acceda al perfil de Azure en la esquina superior derecha y seleccione **Cambiar el directorio** para encontrar la organización.
3. En **Administrar**, seleccione **Personalización de marca de empresa>Configurar**.
4. Junto a **Imagen de fondo de la página de inicio de sesión**, seleccione **Examinar**. Seleccione la imagen de fondo de la página.
5. Junto a **Logotipo del banner**, seleccione **Examinar**. Seleccione la imagen del logotipo.

Configurar personalización de marca de empresa

Azure Active Directory

 Guardar  Descartar

Lenguaje ⓘ

Imagen de fondo de la página de inicio...

Tamaño de la imagen: 1920 x 1080 px

Tamaño de archivo: < 300 KB

Tipo de archivo: PNG, JPG o JPEG ⓘ

Predeterminado



Quitar

*fondo.png

Logotipo del banner

Tamaño de la imagen: 280 x 60 px

Tamaño de archivo: 10 KB

Tipo de archivo: PNG transparente, JPG o JPEG ⓘ



Quitar

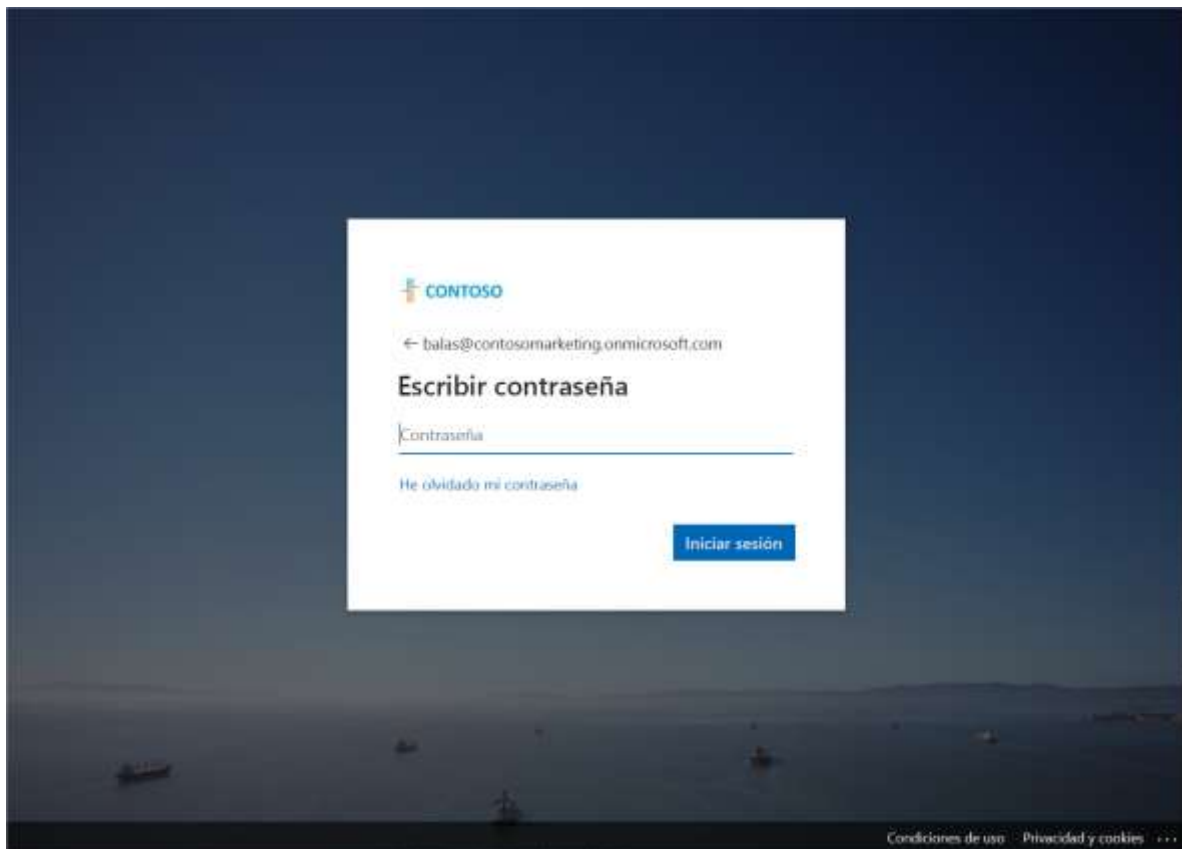
*logotipo-contoso-280x60.png

6. Seleccione **Guardar**.

Prueba de personalización de marca de la organización

Ahora, vamos a usar la cuenta que creamos en el último ejercicio para comprobar la personalización de marca.

1. En una nueva ventana del explorador, vaya a <https://login.microsoft.com>.
2. Seleccione la cuenta de **Bala Sandhu**. Se muestra la personalización de marca.



3. Seleccione **He olvidado mi contraseña**.



Vuelva a su cuenta

¿Quién es usted?

Para recuperar la cuenta, comience por escribir su id. de usuario y los caracteres de la imagen o el audio a continuación.

Id. de usuario:

Example: user@contoso.onmicrosoft.com or user@contoso.com



Escriba los caracteres de la imagen o las palabras del audio.

Siguiente

Cancelar