Instructivo

Autenticación Multi-Factor Microsoft (MFA)

Usuarios finales

Para configurar MFA en tus clientes, sigue estos pasos:

Descargar e instalar la aplicación

- Instala la última versión de la aplicación Authenticator, en función de tu sistema operativo:
- Google Android. En tu dispositivo Android, ve a Google Play para descargar e instalar la aplicación Authenticator.
- Apple iOS. En el dispositivo apple iOS, vaya a la App Store para descargar e instalar la aplicación Authenticator.

Importante: Si no está actualmente en su dispositivo móvil, aún puede obtener la aplicación de Authenticator si <u>se envía a sí mismo un vínculo de descarga</u> desde la página de la aplicación Authenticator.

Configurar la verificación en dos pasos en Authenticator

Para proteger tu cuenta, la aplicación Authenticator puede proporcionarte un código que proporciones verificación adicional para iniciar sesión. No es necesario esperar mensajes de texto o llamadas. Las siguientes instrucciones garantizan que solo usted pueda acceder a su información.

Instalar la aplicación Authenticator

Para instalar la aplicación Authenticator en un dispositivo Android, descarga desde tu dispositivo móvil.

Para instalar la aplicación Authenticator en Para iOS, <u>descarga desde su dispositivo móvil.</u>

Después de instalar la aplicación Authenticator, sigue los pasos que se indican a continuación para agregar tu cuenta:

- Abre la aplicación Authenticator.
- Seleccione (+) en la esquina superior derecha.
- Apunta la cámara hacia el código QR o sigue las instrucciones proporcionadas en la configuración de tu cuenta.

Cuando tu cuenta aparezca en la aplicación de Authenticator, puedes usar los códigos de un solo uso para iniciar sesión. Para obtener más información y soporte técnico sobre la aplicación Authenticator, abre la página <u>Microsoft Authenticator.</u>

Siguientes pasos

<u>Configura la información de seguridad para usar mensajes de texto (SMS)</u>. Escribe el número de tu dispositivo móvil y recibe un código de texto que usarás para la verificación en dos pasos o el restablecimiento de contraseña.

<u>Configura la información de seguridad para usar las llamadas telefónicas.</u> Escribe tu número de dispositivo móvil y recibe una llamada telefónica para realizar la verificación en dos pasos o restablecer la contraseña.

Instructivo

Autenticación Multi-Factor Microsoft (MFA)

Administradores

Puedes desplegar MFA en los tenants de tus clientes siguiendo estos pasos:

- Ingresa al portal de Azure con alguno de estos roles: Administrador de Seguridad, Administrador de acceso condicional o Administrador global
- Navega a "Active Directory > Properties"
- Selecciona "Manage security defaults"
- Activa "Enable security defaults"
- Guarda el ajuste

Microsoft Azure		.P Search resources, services, and docs (G+)/	E 🛱 C 🐵 ? 😅 balas@contoso.com 🍕	
Home > Contoso - Properties		Enable Security defaults		
Contoso - Pr Azure Active Directory	operties			
,C Search (Ctrl+)	« 🔒 Sa	ve X Discard	Security defaults is a set of basic identity security mechanisms	
Overview	Direc	tory properties	recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks. Learn more	
Manage	Cont	050		
Users Groups Gr	Count United Locati inistrators Notifi lications Engli Direct response	ry or region States on State datacenters cation language bh ory ID 716 Anth 454 is holts: 100716/c66/1	Drawe any operated	
App registration	ans to the second			
A Identity Gove	nance Techn tech	ical@contoso.com		
Application p	Globa priva	l privacy contact cy@contoso.com		
Azure AD Cor	nect Privac	v statement URL		
Custom doma	in names			
Mobility (MDI	f and MAM)			
Password rese	Acce	ss management for Azure resources		
Company bra	ding balasi	@contoso.com Bala Sandhu (balas@contoso.com) can manage access to		
User settings	mana	gement groups in this directory.Learn more		
III Properties				
Notifications	ettings	ge security detaults		
	10070		29646	



Después de habilitar los defaults de seguridad en el tenant de tu cliente, todos los usuarios serán requeridos para registrarse mediante MFA utilizando la app móvil "Microsoft Authenticator" y tendrán 14 días de gracia para descargar e instalarla en un dispositivo.

Los usuarios con el rol de Global Administrator deberán, además, proporcionar un número telefónico.

Una vez activada MFA, puedes dar seguimiento al proceso de registro desde el tenant de tus clientes mediante el reporte de actividad de métodos de autenticación, como se muestra en la figura abajo:

Home > Authentication methods	Activity		
Search (Ctrl+/) « Registrati	on Usage		
Manage			
Policies	apable of Azure multifactor	Users capable of passwordless	Users capable of self-service password
Password protection authen	tication	authentication	reset
Registration campaign 2 of 4	total	1 of 4 total	2 of 4 total
Monitoring	▲ 50% of your organization isn't capable.	75% of your organization isn't capable.	50% of your organization isn't enabled.
fin Activity cap			
User registration details			
Registration and reset events			
Bulk operation results			