Métodos de autenticación PortalGuard

Índice

Descargo de responsabilidad 1
BIO-key MobileAuth 2
FIDO2/WebAuthn Tokens 2
FIDO U2F Clave de seguridad 3
Claves de seguridad FIDO soportadas 3
HMAC-Basado en Token OTP 3
Push 3
Autenticador móvil 4
SMS 4
Email 4
Help Desk 5
Autenticación de cuadrícula 5
Biometría de voz 5
OTP Impresas 5
Preguntas de seguridad 6
Obligatorio 6
Opcional 6

Descargo de responsabilidad

Esta lista está destinada a proporcionar una breve descripción general de los métodos de autenticación disponibles para el modo autoservicio y Autenticación Multifactor (MFA) en todo PortalGuard. Esta lista no es un documento técnico y solo sirve como introducción. Para preguntas técnicas detalladas o detalles de uso con respecto a cualquier función, comunícate directamente con el soporte técnico de PortalGuard:

Email: techsupport@portalguard.com

Teléfono: +1 (603) 547-1200

BIO-key MobileAuth

BIO-key MobileAuth es una app móvil fácil de usar que no requiere hardware nuevo y un rápido proceso de inscripción y registro de código QR que se puede completar en segundos. MobileAuth ofrece PalmPositive como un método de autenticación y una forma de biometría vinculada a la identidad que utiliza un simple escaneo de la palma de la mano para autenticar al individuo.

Como parte de la plataforma PortalGuard IDaaS de BIO-key, BIO-key MobileAuth admite sus soluciones de Autenticación Multifactor (MFA) e inicio de sesión único (SSO) para optimizar los inicios de sesión y hacerlos más seguros.

BIO-key MobileAuth con PalmPositive está disponible para iOS y Android y requiere una cuenta activa de BIO-key PortalGuard IDaaS.

WEB-key™

WEB-key es una plataforma biométrica vinculada a la identidad (IBB) de nivel empresarial de BIO-key. Para la autenticación biométrica de huellas dactilares, tiene los puntos de referencia NIST más probados y verificados de forma independiente para la identificación, velocidad y precisión de huellas dactilares.

La autenticación de WEB-key está integrada con PortalGuard para acciones de restablecimiento de contraseña autoservicio y Autenticación Multifactor (MFA). Esta integración requiere la inscripción manual del usuario, así como la configuración y el uso de un servidor de WEB-key independiente para la validación segura de los datos biométricos.

Para capturar escaneos de huellas dactilares, BIO-key ofrece una variedad de escáneres USB Windows Hello calificados por Microsoft que se pueden usar de forma inmediata con Windows Hello y Windows Hello for Business, o para usar con BIO-key Identity y Access Management (IAM) soluciones como PortalGuard, como una de las muchas marcas compatibles de escáneres. Los modelos de escáner de huellas dactilares disponibles incluyen:

- SidePass
- PIV-Pro
- EcoID II
- SideSwipe
- SideTouch
- Pocket10

FIDO2/WebAuthn Tokens

FIDO2 (AKA WebAuthn) se diferencia de FIDO U2F en que está diseñado para un enfoque "sin contraseña" para la autenticación segura. Funcionalmente, los tokens FIDO2 admiten el mismo uso que FIDO U2F, aunque utilizan un estándar de la industria diferente y una API basada en navegador. Los tokens FIDO2 admiten uno de dos tipos de uso: hacer clic para autenticar o autenticación en el dispositivo.

Hacer clic para autenticar requiere un toque/clic en el token mientras que la autenticación en el dispositivo detecta la solicitud FIDO2 y responde automáticamente, lo que permite que continúe la acción de autenticación.

FIDO U2F Clave de seguridad

FIDO U2F es un protocolo estándar desarrollado conjuntamente por Yubico y Google como una forma alternativa de autenticación de dos factores basada en "token". El uso de FIDO U2F requiere una clave de seguridad compatible, así como un navegador compatible.

Las llaves de seguridad FIDO U2F no requieren ningún software adicional, controladores o instalación del lado del cliente para su uso, y actúan como un segundo factor sólido y seguro para la autenticación. La adopción y el uso son sencillos: simplemente conecta la llave a un puerto USB y presiona el botón para usar.

Claves de seguridad FIDO soportadas

Como se mencionó anteriormente, las llaves de seguridad FIDO son dispositivos de hardware compatibles con los estándares FIDO2 y FIDO U2F. PortalGuard es compatible con varias marcas, incluidas:

- **BIO-key FIDO-keys:** Las claves de seguridad FIDO-key de BIO-key son compatibles con los estándares FIDO U2F, FIDO2 y WebAuthN para una autenticación en línea fácil y segura. Estas claves cuentan con tecnología plug-and-play y son compatibles con las principales plataformas, incluidas Microsoft Windows, macOS y Linux. Todos los tokens almacenan una cantidad infinita de claves criptográficas y son de alta calidad, duraderos e incluso impermeables. Con FIDO-key, los clientes y las empresas tienen una selección de opciones rentables para la autenticación en línea.

- YubikeyTM: los tokens YubiKey son dispositivos de hardware únicos que generan un código de acceso de un solo uso, generalmente con solo tocar un botón. Estos dispositivos emulan un teclado y ofrecen un método simple y seguro para proporcionar un segundo factor durante la autenticación. Las fichas Yubikey no tienen fuente de alimentación, pantalla ni piezas móviles. Estos tokens son extremadamente resistentes a los daños y tienen una larga vida útil.

- RSA SecurIDTM: los tokens de RSA SecurID vienen en muchas formas y formas. La mayoría muestra un código de acceso de un solo uso directamente en el dispositivo, que luego ingresa el usuario cuando se lo solicita a través de una aplicación compatible. La compatibilidad con los tokens de RSA SecurID depende de que el servidor PortalGuard pueda comunicarse directamente con los servidores RSA Authentication Manager. También debe ser un cliente de RSA activo.

HMAC-Basado en Token OTP

Los tokens OTP basados en HMAC (HOTP) utilizan una clave compartida estática y un contador para generar un código de acceso único válido. Este tipo de Token OTP requiere una sincronización entre el dispositivo y el servidor PortalGuard para garantizar la validación bidireccional.
Los administradores tienen acceso total para inscribir o resincronizar estos tokens a través de la Consola de la mesa de ayuda de PortalGuard.

Push

Push es un segundo factor "fuera de banda" vinculado a un dispositivo móvil. Este segundo factor permite a los usuarios finales confirmar o denegar una solicitud de autenticación interactuando con el dispositivo móvil en tiempo real. No es necesario recordar ningún código, simplemente toque sí o no en la pantalla.

Autenticador móvil

PortalGuard admite el uso de múltiples aplicaciones de autenticación móvil. Estas aplicaciones generan un código de acceso único basado en el tiempo (TOTP), que posteriormente se puede utilizar durante varias acciones de restablecimiento de contraseña de autoservicio y Autenticación Multofactor (MFA) en todo PortalGuard.

La aplicación de autenticación móvil requiere una inscripción única para sincronizar la aplicación de autenticación y el sitio web de PortalGuard. A partir de ahí, el dispositivo puede generar un TOTP válido aunque no esté conectado a la red.

Las aplicaciones de autenticación móvil compatibles incluyen, entre otras:

- Google Authenticator
- Microsoft Authenticator
- Authy
- Duo

SMS

El método de entrega de SMS (a menudo denominado simplemente "teléfono") consiste en enviar un mensaje de texto SMS a un número de teléfono móvil registrado. Este mensaje de texto SMS contiene un código de acceso único (OTP) para validar al usuario en el sistema PortalGuard para una acción específica. Los administradores tienen control total sobre la longitud, el juego de caracteres y la validez de las OTP utilizadas por esta opción. Estas configuraciones también son compartidas por el tipo de OTP 'Correo electrónico'.

La funcionalidad de SMS requiere integración con un sistema proveedor de SMS de terceros.

Los siguientes proveedores son compatibles con PortalGuard para enviar mensajes SMS para MFA:

- Clickatell
- Esendex
- MessageMedia
- Regroup
- SMSMatrix
- Twilio
- Plivo

Email

El método de envío de email consiste en enviar un correo electrónico a una dirección registrada. Este email contiene una OTP para validar al usuario en el sistema PortalGuard para una acción específica. Los administradores tienen control total sobre la longitud, el juego de caracteres y la validez de las OTP utilizadas por esta opción. Estas configuraciones también son compartidas por el tipo de OTP 'SMS'.

Help Desk

Esta opción permite a los usuarios finales recibir una OTP generada por la Consola de la mesa de ayuda de PortalGuard. Se debe instruir a los usuarios finales (a través de la capacitación para usuarios finales y/o la interfaz de usuario de PortalGuard) sobre cómo comunicarse con el equipo de soporte técnico. Una vez contactado, el equipo de la mesa de ayuda puede utilizar la consola del help desk de PortalGuard para generar un código para proporcionar al usuario.

Las OTP de la mesa de ayuda siempre utilizan caracteres numéricos, pero la longitud se puede configurar en el lado administrativo.

Autenticación de cuadrícula

Grid Authentication utiliza una implementación de JavaScript de terceros para permitir el seguimiento de un patrón como segundo factor. Este patrón se traza en una cuadrícula de puntos y puede ser visible u oculto según lo defina el usuario.
Este segundo factor le resultará familiar a cualquier usuario que haya utilizado un patrón para desbloquear su dispositivo móvil, ya que se ve y se siente igual. Este tipo es especialmente útil para entornos con muchos dispositivos móviles, aunque también se puede utilizar en un entorno de escritorio completo.

Biometría de voz

Voice Biometrics admite la entrega de un código de acceso único (OTP). Se realiza una llamada tradicional al número de teléfono inscrito del usuario a través de un proveedor de mensajería de terceros. El proveedor de mensajería de terceros toma el texto completo del mensaje establecido por el administrador de PortalGuard y lo convierte a un formato de audio de texto a voz, que luego se lee al usuario final cuando responde la llamada para su verificación.

Esta funcionalidad es muy útil ya que es compatible tanto con teléfonos fijos como con teléfonos móviles.

Los siguientes proveedores son compatibles con PortalGuard para enviar mensajes biométricos de voz para MFA:

- Esendex
- MessageMedia
- Regroup
- SMSMatrix
- Twilio

OTP Impresas

Las OTP impresas se generan aleatoriamente a pedido del usuario a través de la página de Administración de cuentas. Estos códigos se pueden usar cada vez que el usuario no recibe una OTP en tiempo real (por ejemplo, a través de SMS, email o a través de un autenticador móvil) o no puede autenticarse para una acción de autoservicio o MFA específica.
Cada una de estas OTP impresas se puede usar solo una vez y está vinculada específicamente a la cuenta de usuario utilizada para generar el lote.
La longitud y la cantidad de OTP impresas se pueden configurar en el lado administrativo, pero solo se utilizan caracteres numéricos para esta opción de OTP.

Preguntas de seguridad

Las preguntas de desafío son el enfoque estándar para la verificación del usuario. Los usuarios proporcionan respuestas a las preguntas previamente registradas. Esta inscripción la completa un administrador o el usuario durante la primera vez que inicia sesión en el sistema.

Las respuestas de desafío toman dos formas:

Obligatorio

Las respuestas de desafío obligatorias son más estrictas. El administrador determina cuántas preguntas obligatorias se requieren y el usuario debe responder todas las preguntas.
Durante una acción restablecimiento de contraseña autoservicio o autenticación basada en conocimientos (KBA), el usuario debe responder todas las preguntas de seguridad obligatorias para completar la acción.

Opcional

Las respuestas de desafío opcionales permiten al usuario elegir entre una serie de preguntas y solo proporcionar respuestas a un subconjunto.

Por ejemplo, cuando un usuario inscribe respuestas de desafío opcionales, el usuario debe configurar cinco respuestas a las preguntas elegidas por dicho usuario. Durante un autoservicio de restablecimiento de contraseña o una acción de KBA, el usuario debe elegir tres de esas cinco preguntas inscritas y proporcionar respuestas válidas.

Esta opción brinda flexibilidad si ciertas respuestas cambian o simplemente se olvidan.