Engineer

Autenticación multifactor

inicio de sesión con pruebas de dos o más tipos distintos

Qué es

La autenticación multifactor, normalmente abreviada MFA, es un inicio de sesión que solo acepta una identidad declarada cuando la respalda más de un tipo de prueba. NIST SP 800-63B-4, la guía federal estadounidense de autenticación que también siguen muchas organizaciones ajenas al Gobierno, enumera tres tipos: algo que sabe, como una contraseña; algo que tiene, como un teléfono o una llave de seguridad; y algo que es, como una huella dactilar. Una palabra es decisiva en la definición: el sistema debe exigir más de un tipo distinto de factor. Una contraseña y la respuesta a una pregunta de seguridad suman un único factor, porque ambas son cosas que sabe. La autenticación de dos factores, o 2FA, es el caso habitual de exactamente dos.

La guía admite dos maneras de conseguirlo. La primera combina autenticadores independientes de un solo factor: una contraseña junto con una aplicación del teléfono que muestra códigos de un solo uso, o bien con una lista de códigos de respaldo impresos. La segunda emplea un autenticador multifactor, como una llave de seguridad o un teléfono que guarda una clave privada y solo la utiliza después de introducir un PIN o presentar una huella. En ese caso, el PIN o la huella se denomina factor de activación. Se comprueba en el propio dispositivo; el servidor solo recibe el resultado, una firma verificable, de modo que un solo toque presenta dos factores.

La biometría tiene un papel limitado. NIST solo permite una huella o un rostro si en la autenticación también interviene un autenticador físico, nunca como factor aislado, y exige ofrecer siempre una alternativa no biométrica. La guía deja claro que los rasgos biométricos no son secretos: puede fotografiarse un rostro y obtenerse una huella de algo que su dueño haya tocado.

Utilice el concepto en una decisión

Aplique «¿Qué es la autenticación multifactor?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

Una contraseña puede copiarse sin que su dueño lo advierta: si la introduce en una copia convincente de la página de acceso, si alguien la adivina o si la reutiliza en un sitio cuya base de datos se roba después. MFA hace que una contraseña copiada sea insuficiente por sí sola, porque el atacante sigue necesitando algo de otro tipo.

NIST fija esta base para su segundo nivel de garantía. En AAL2, el usuario debe autenticarse con dos factores, combinados en un autenticador o proporcionados por separado; la combinación debe incluir un autenticador físico junto con una contraseña o una comparación biométrica. Los verificadores de ese nivel deben ofrecer al menos una opción resistente al phishing, y las agencias federales deben exigir autenticación resistente al phishing a su personal, contratistas y socios.

Los métodos vendidos bajo las mismas tres letras difieren entre sí más de lo que MFA difiere de una contraseña sola; la guía los distingue con claridad:

- Los **códigos enviados por SMS o llamada de voz** son el único tipo de autenticador que NIST califica de restringido. Todavía pueden usarse, pero el verificador debe ofrecer una alternativa sin esa calificación, informar al usuario del riesgo y tener un plan para abandonar el método. Cambiar el número registrado equivale a vincular un autenticador nuevo, con todas las comprobaciones correspondientes.
- Los **códigos de una aplicación y las solicitudes de aprobación en el teléfono** son aceptables en AAL2, pero no resisten el phishing: lo que la persona introduce o aprueba no está vinculado al sitio que lo solicitó.

- Los **autenticadores criptográficos que vinculan la respuesta al sitio**, como las claves de acceso o passkeys y las tarjetas inteligentes, resisten el phishing. AAL3 exige uno cuya clave privada no pueda exportarse del hardware.

El correo electrónico falta deliberadamente en la lista: la guía lo descarta como canal de autenticación fuera de banda.

Cómo se aplica en la práctica

El código de una aplicación de autenticación es el segundo factor más habitual; RFC 6238, de mayo de 2011, lo define en pocas páginas. Durante el alta, el servidor genera una clave secreta y la entrega a la aplicación, normalmente mediante un código QR; ambas partes pasan a tener la misma clave. Para producir un código, cada parte divide la hora Unix actual por un intervalo temporal, de 30 segundos de forma predeterminada, y utiliza la parte entera como contador. Calcula un HMAC del contador con la clave y reduce el resultado a un número decimal corto mediante el método HOTP, definido por RFC 4226 en 2005, que exige al menos seis dígitos. En Python, el cálculo completo cabe en unas pocas líneas:

```
import hashlib, hmac, struct

def totp(key: bytes, unix_time: int, digits: int = 6, step: int = 30) -> str:
    counter = struct.pack(">Q", unix_time // step)
    mac = hmac.new(key, counter, hashlib.sha1).digest()
    offset = mac[-1] & 0x0F
    code = struct.unpack(">I", mac[offset:offset + 4])[0] & 0x7FFFFFFF
    return str(code % 10**digits).zfill(digits)

print(totp(b"12345678901234567890", 59, digits=8))  # 94287082
```

Los vectores de prueba del RFC utilizan esa clave ASCII de 20 bytes y ocho dígitos. A los 59 segundos desde el inicio de la época, el contador vale 1 y la variante SHA-1 produce 94287082, que es lo que imprime la función. El código de seis dígitos que mostraría una aplicación corresponde a sus seis últimos dígitos: 287082. El cálculo no utiliza la red; por eso la aplicación funciona en un teléfono en modo avión y el servidor debe conservar su propia copia de la clave de cada usuario.

Comprobar un código consiste en repetir el cálculo en el servidor y comparar el resultado. RFC 6238 recomienda aceptar, como máximo, un intervalo temporal anterior para cubrir el retraso de la red y prohíbe aceptar un código por segunda vez después de haberlo utilizado correctamente.

Una clave de acceso sustituye el secreto compartido por un par de claves. En Web Authentication Level 3, recomendación del W3C desde el 25 de agosto de 2026, el autenticador crea un par para un solo sitio, identificado por su dominio, y entrega al servidor únicamente la clave pública. Al iniciar sesión, el navegador transmite el origen al que está conectado realmente y el autenticador firma el desafío del servidor junto con ese origen: una firma producida en un dominio parecido resulta inútil en el verdadero. Si utilizar la clave exige un PIN o una huella, una clave de acceso es un autenticador multifactor en un solo paso. WebAuthn llama credenciales multidispositivo a las claves de acceso copiadas entre los dispositivos de una persona; NIST acepta estas claves sincronizadas en AAL2, pero no en AAL3, porque una clave sincronizable es, por definición, exportable.

Activar MFA es la parte fácil. Decidir quién debe usarla, qué métodos se admiten en cada caso y qué ocurre si alguien pierde el teléfono es administración de cuentas, parte de una organización más amplia del acceso. El servicio de seguridad y gestión de accesos de este sitio describe ese conjunto: cuentas, contraseñas y permisos configurados para que cada persona tenga exactamente el acceso necesario para su trabajo y quienes se marchen lo pierdan el mismo día de su salida.

Dónde surgen los problemas

Una página de phishing retransmite el código. Un código de un solo uso es un número que el usuario lee e introduce; nada en él registra qué sitio estaba viendo. Una página parecida que reenvía la contraseña y el código al sitio verdadero dentro del intervalo temporal inicia sesión como el usuario. Por eso NIST declara que ningún autenticador cuya salida se introduzca a mano se considera resistente al phishing; añade que no importa cómo llegó el usuario a la página falsa. La solución es un autenticador que vincule su respuesta al verificador: por su dominio, como WebAuthn, o al propio canal TLS, como los certificados de cliente y las tarjetas inteligentes. Exija uno de ellos a los administradores y ofrézcalo a los demás.

El número de teléfono es el factor. Un código por SMS llega a quien reciba en ese momento el tráfico de ese número según el encaminamiento del operador móvil. La lista de amenazas de NIST incluye al atacante que convence al operador para redirigir el número de la víctima y recibe después el código. Antes de enviar un código por SMS o voz, los verificadores deberían buscar indicios como un cambio reciente de SIM, una portabilidad del número o un cambio de dispositivo. Conserve los SMS como alternativa de respaldo, en lugar de método principal, y exija un inicio de sesión completo antes de cambiar el número registrado.

Aprobar, aprobar, aprobar. Una notificación con un único botón Aprobar pide una decisión, no una prueba. Un atacante que ya tiene la contraseña puede provocar avisos hasta que el usuario, cansado del ruido, acepte uno. NIST lo llama fatiga de autenticación y ya no considera aceptables los procesos de mera aprobación: debe trasladarse un secreto de un canal al otro, como un número mostrado en la pantalla de acceso que el usuario introduzca en el teléfono. Elegirlo de una lista breve no basta: podría simplemente adivinarlo. Limite también cuántas notificaciones pueden enviarse desde el último inicio de sesión correcto, como recomienda la guía.

La recuperación omite el segundo factor. Un enlace «he perdido el teléfono» que solo pide la contraseña o envía un enlace de restablecimiento por correo convierte MFA en una opción que el atacante puede rechazar. Para cuentas AAL2, NIST exige recuperar el acceso mediante dos códigos de recuperación obtenidos por métodos distintos, un código de recuperación junto con un autenticador de un solo factor aún vinculado a la cuenta o una nueva comprobación de identidad. Toda recuperación debe notificar al usuario. En general, un factor nunca debe permitir obtener un autenticador de otro tipo: una contraseña sola no debe bastar para imprimir un conjunto nuevo de códigos de respaldo.

Se acepta el código dos veces o durante demasiado tiempo. Un código de seis dígitos tiene un millón de valores posibles; su fortaleza depende de las reglas que lo rodean. Un verificador que acepta varios intervalos anteriores o posteriores al actual o un código ya utilizado da a quien haya visto un código una ventana para reutilizarlo. Registre el último intervalo aceptado por usuario y rechace cualquiera igual o anterior, limite la ventana al único intervalo que RFC 6238 permite por retrasos y limite los fallos consecutivos: NIST admite como máximo 100 antes de desactivar el autenticador.

Las semillas están junto a las contraseñas. Los códigos de una aplicación son simétricos: el servidor guarda la clave de cada usuario y quien las copie puede generar códigos válidos para todas las cuentas. NIST exige protegerlas con medidas robustas y limitar el acceso a los componentes de software que las necesiten. No las guarde como columnas sin cifrar junto a los hashes de contraseñas. Cífrelas con una clave conservada en un almacén de secretos separado y permita leerlas únicamente al servicio que verifica los códigos.

Lecturas adicionales

- NIST SP 800-63B-4: definiciones y siglas — las definiciones de autenticación multifactor, autenticador multifactor y resistencia al phishing en la guía actual.
- NIST SP 800-63B-4 en el Computer Security Resource Center — el registro de publicación: julio de 2025, sustituyendo a SP 800-63B.
- RFC 6238: TOTP — el algoritmo de contraseña de un solo uso basado en el tiempo, sus vectores de prueba y las reglas sobre el desfase de los relojes.
- RFC 4226: HOTP — el algoritmo subyacente basado en contador, incluido el truncamiento a seis dígitos o más.
- Web Authentication, Level 3 — la especificación W3C de las claves de acceso, con credenciales vinculadas al origen y claves sincronizadas.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es la autenticación multifactor?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/multi-factor-authentication/