ESET Secure Authentication 1 Jahr Download Win, Multilingual (5-10 Lizenzen)

Artikelnummer	900212306
Gewicht	1kg
Länge	1mm
Breite	1mm
Höhe	1mm

Produktbeschreibung

ESET Secure Authentication 1 Jahr Download Win, Multilingual (5-10 Lizenzen)

Produktbeschreibung:

Optimaler Schutz Ihrer Daten dank mobilbasierter Multi-Faktor-Authentifizierung.

Multi Faktor Authentifizierung- was ist das?

???????Bei der Multi-Faktor-Authentifizierung (MFA), oft auch als Zwei-Faktor-Authentifizierung (2FA) bekannt, handelt es sich um eine leistungsstarke Authentifizierungsmethode, bei der sich Benutzer mit mehr als einem Element ausweisen müssen. Durch Kombination eines statischen Passworts mit einem zweiten, dynamischen Faktor wird die Gefahr von Datenverlusten bedeutend verringert. ESET Secure Authentication (ESA) dient Organisationen als Grundlage zur Erfüllung von Compliance-Anforderung und wirkt präventiv zur Vermeidung von Datenschutzvorfällen. Mit ESA implementieren Unternehmen jeder Größe einfach und unkompliziert eine MFA für gemeinsam genutzte Systeme (Windows- & Server Logins, Microsoft Cloud-Dienste wie Microsoft 365 oder OWA, SAML, FIDO, ADFS 3.0, VPNs und RADIUS-basierte Dienste).

Eine leistungsstarke und einfach zu implementierende Multi-Faktor-Authentifizierung für Unternehmen jeder Größe. Unternehmen profitieren von:

- Vermeidung von Datenschutzvorfällen
- Erfüllung von Compliance-Anforderungen
- Zentral gesteuert über Browser
- Über Handy oder bestehende HW Token ausführbar

Zwei-Faktor-Authentifizierung einfach gemacht

Authentifizierung ist simpel- der Code muss lediglich über Handy bestätigt werden. Funktioniert auf iOS und Android Smartphones sowie für alle Plattformen und Dienste.

Cloud Support

Neben der Absicherung von Anwendungen vor Ort kann ESET Secure Authentication zum Schutz von Web- und Cloud-Diensten wie Microsoft Office 365, Google Apps, Dropbox und viele weitere mehr durch ADFS 3.0 oder SAML Protokoll Integration eingesetzt werden.

Verschiedene Authentifizierungsmethoden

ESET Secure Authentication unterstützt Push-Benachrichtigungen, die Bereitstellung von Einmal-Passwörtern über die mobile Client-App, SMS oder bestehende Hardware-Token sowie FIDO-basierte Sticks und individuelle Methoden.

ESET bietet einfach mehr

Remote Management

ESET Secure Authentication verwendet eine eigens gebaute Managementkonsole, die über einen Webbrowser zugänglich ist. Sie können sich für die Integration mit Active Directory entscheiden, die Lösung aber auch in Nicht-AD-Umgebungen einsetzen. Nach der Installation sind für die Einrichtung und Bereitstellung von ESET Secure Authentication keine zusätzlichen Schulungen oder professionellen Dienstleistungen erforderlich.

Setup in nur 10 Minuten

Wir haben die Lösung so konzipiert, dass sie auch in kleinen Unternehmen ohne eigene IT-Abteilung problemlos auf- und eingesetzt werden kann. Unabhängig von Ihrer Firmengröße beansprucht die Installation von ESET Secure Authentication dank der Möglichkeit, mehrere Nutzer gleichzeitig einzurichten, nur wenig Zeit.

Keine zusätzliche Hardware nötig

ESET Secure Authentication erfordert keine zusätzliche Hardware. Nach der Installation der 10MB-großen Anwendung auf Ihrem Server können Sie umgehend mit der Bereitstellung starten.

Unterstützung aller gängigen Smartphones

Ihre Mitarbeiter können bereits eingesetzte Smartphones weiter nutzen. ESET Secure Authentication erfordert keine zusätzliche Hardware. Wir unterstützen auch Hardwareschlüssel, aber dies ist optional.

Einschließlich SDK und API

Zur individuellen Anpassung der Funktionalitäten stellen wir sowohl ein SDK als auch eine API bereit. So können Unternehmen ESET Secure Authentication nach ihrem Bedarf erweitern und die Nutzung auf eigene Anwendungen oder Webservices ausweiten.

Push-Authentifizierung

Bequeme Authentifizierung ohne Eingabe eines Einmal-Passworts über die Bestätigung einer Push-Benachrichtigung. Funktioniert auf iOS und Android Smartphones.

Mit ESET Secure Authentication schützen Sie:

- VPN-Zugänge zu Ihrem Unternehmen
- Remote Desktop Protocol (RDP)
- Zusätzliche Authentifizierung für Desktop-Logins (Anmeldung beim Betriebssystem)
- Web-/Cloud-Dienste via Microsoft ADFS 3.0, z.B. Office 365
- Online Web App (OWA)
- Microsoft Web Apps
- VMware Horizon View
- RADIUS-based services
- Exchange Control Panel & Exchange Administrator Center

Unterstützte VPNs

- Barracuda
- Cisco ASA
- Citrix Access Gateway
- Citrix NetScaler
- Check Point Software
- Cyberoam, F5 FirePass
- Fortinet FortiGate
- Juniper
- Palo Alto
- SonicWall

Systemvoraussetzungen:

Server:

32&64-Bit Versionen von Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, 2016

Client:

iOS (iPhone), Android, Windows 10 Mobile

Unterstützung von Token:

Auch wenn die Nutzung von Hardware-Token nicht erforderlich ist, unterstützt die Lösung alle ereignisbasierten, OATH-konformen HOTP-Token ebenso wie FIDO2 und FIDO U2F Hardware-Schlüssel.