SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™

Starke Authentifizierung zum Schutz Ihrer Daten und Netzwerke

Eines der größten Sicherheitsrisiken sind schwache und verlorene Passwörter. ESET Secure Authentication stellt Einmal-Passwörter (OTPs) auf den Mobiltelefonen Ihrer Mitarbeiter bereit und bietet somit optimalen Schutz vor unerlaubten Zugriffen auf Netzwerke, Dienste und Daten. Diese Passwörter ergänzen die normale Anmeldung um einen zuverlässigen Sicherheitsfaktor.

ESET Secure Authentication ist eine leistungsfähige Lösung zur Zwei-Faktor-Authentifizierung mit Einmal-Passwörtern (2FA-OTP). Die Integration in Ihre bestehenden IT-Systeme ist schnell und problemlos möglich.

Nativ werden sowohl Outlook Web Access/App für Microsoft Exchange 2007, 2010 und 2013 als auch kritische Endpoints wie das Exchange Control Panel oder das Exchange Administration Center unterstützt. Darüber hinaus kann es mit einer Reihe von Business-Tools wie Microsoft Sharepoint und Microsoft Dynamics CRM genutzt werden.

Die Logins bei Remote Desktop WebAccess oder VMware Horizon sind ebenso leicht abzusichern wie Ihre VPN-Zugänge.

Fügen Sie ESET Secure Authentication einfach zu Ihren RADIUS-basierten Diensten hinzu oder nutzen Sie die API für die Integration in Ihr bestehendes Active Directory Authentifizierungssystem.

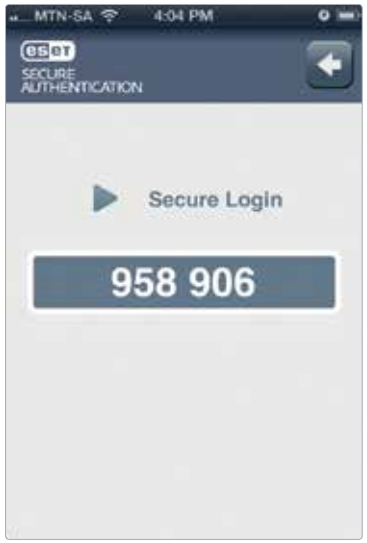
Für Eigenentwicklungen oder Systeme ohne Active Directory Anbindungen kann die vollständige Funktionalität problemlos über das SDK eingebunden werden.

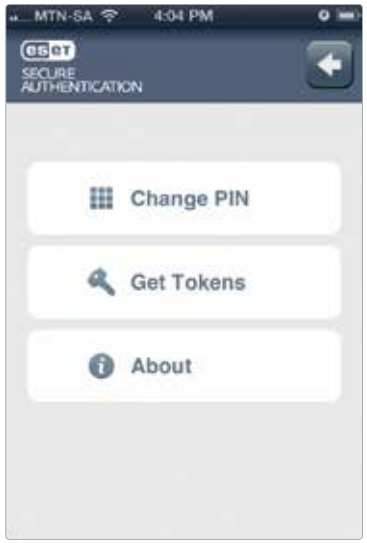
Wie funktioniert ESET Secure Authentication?

Für die sichere Anmeldung an Netzwerken und Diensten wie VPN oder OWA wird auf den Mobiltelefonen Ihrer Mitarbeiter ein zusätzliches Einmal-Passwort bereitgestellt. Somit sind Ihre Daten und Informationen vor Eindringlingen und verschiedenen Arten von Cybercrime geschützt. Das Erraten von Passwörtern oder der Angriff über Wörterbuchattacken werden verhindert.

Was heißt 2-Faktor-Authentifizierung (2FA)?

Im Gegensatz zur herkömmlichen Passwort-Authentifizierung verwendet 2FA zwei Elemente. Einer der Faktoren ist: "Was der Nutzer weiß". Das kann ein Passwort oder ein PIN Code sein. Der zweite Faktor besteht typischerweise aus einem Mobiltelefon oder einem Hardware Token - also aus etwas "Was der Nutzer hat". Die Kombination dieser beiden Elemente gewährleistet eine wesentlich höhere Sicherheit beim Datenzugriff.





Löst die Probleme "klassischer" Passwörter:

- Statische Passwörter können abgefangen werden
- Passwörter, die nicht aus zufälligen Zeichenkombination bestehen, können einfach erraten werden
- Firmenpasswörter auch für in privatem Gebrauch
- Passwörter enthalten oftmals persönliche Daten - z.B. Namen, Geburtstage usw.
- Einfachste Muster für neue Passwörter, wie "peter1", "peter2" usw.
- Sichere Passwörter werden häufig auf Zetteln notiert

Vorteile für Ihr Unternehmen

- Einmal-Passwörter bieten Sicherheit für Ihre wertvollen Daten
- Schutz vor Risiken durch schwache Passwörter
- Kostengünstig - keine zusätzliche Hardware nötig
- Einfache Installation und Benutzung
- Kostenloser technischer Support in Ihrer Landessprache

Vorteile für Ihre IT

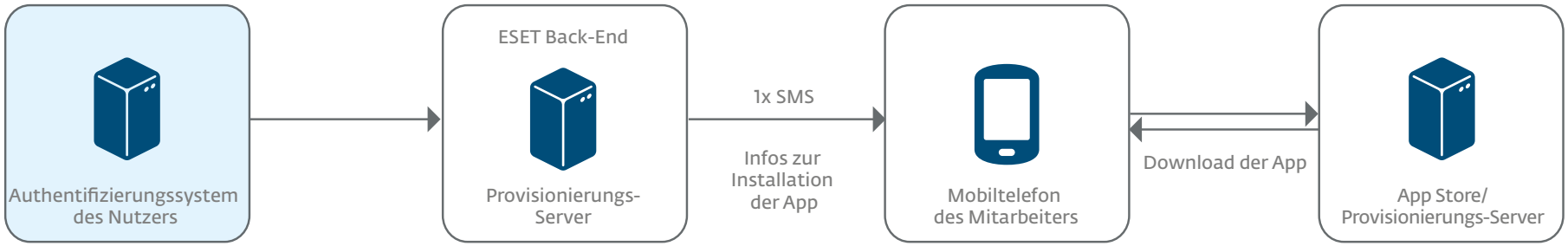
- Innerhalb weniger Minuten einsatzbereit
- Nach der Installation funktioniert die App auch ohne Internetverbindung
- Unterstützt die meisten VPN Appliances
- Unterstützt alle marktüblichen mobilen Betriebssysteme
- Weltweiter technischer Support in Ihrer Landessprache
- API und SKD für volle Flexibiltät verfügbar

Genauere Betrachtung

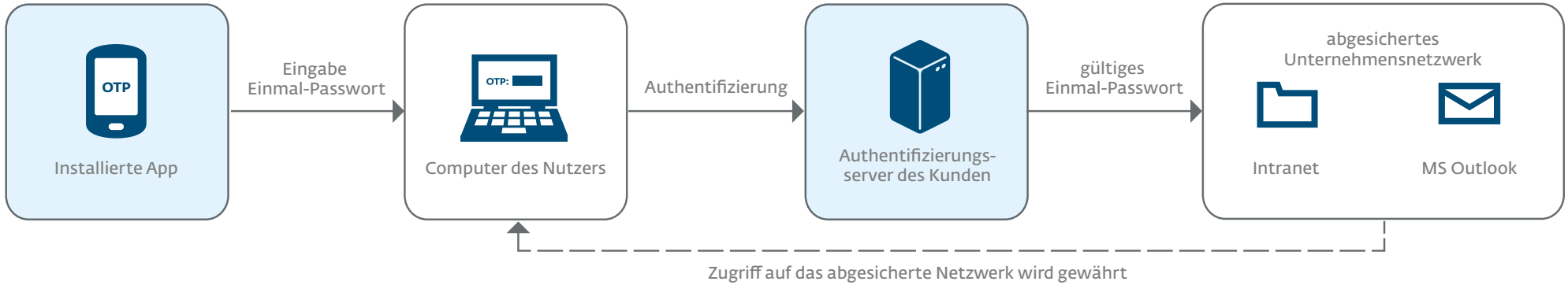
ESET Secure Authentication wurde für die problemlose Integration in die bestehende Unternehmens-Infrastruktur konzipiert. Den Nutzern der ESET Secure Authentication werden Apps für deren Mobilgeräte bereitgestellt. Innerhalb des Unternehmen läuft eine Server Anwendung, die sich nahtlos in die vertraute Umgebung der Netzwerk-Administratoren einfügt. Dies wird durch die Einbindung in die MMC (Microsoft Management Console) und ADUC (Active Directory Benutzer & Computer) gewährleistet. Mit der Authentifizierung über die API lässt sich ESET Secure Authentication in ein bestehendes Anmeldesystem problemlos integrieren. Das SDK ermöglicht die flexible Umsetzung eigener Lösungen ohne die Verwendung von Active Directory. Der native Support von Microsoft Exchange Server 2013, VMware Horizon View und nahezu allen verbreiteten VPN-Lösungen ist besonders hilfreich.

Alles, was Sie zum Versand der App auf das Mobiltelefon benötigen, ist die Mobilfunknummer des Mitarbeiters. ESET Secure Authentication schickt dem Nutzer eine SMS mit einem Aktivierungslink. Sobald er diesen anklickt, wird automatisch die passende Installationsdatei für die jeweilige Plattform herunter geladen.

Installation und Einrichtung



Was passiert beim Nutzer?



Datasheet

Zwei-Faktor-Authentifizierung	Die auf Mobiltelefonen basierende Zwei-Faktor-Authentifizierung (2FA) mit Einmal-Passwörtern (OTP) bietet ein höheres Maß an Sicherheit	
	Nativer Schutz von Outlook Web App (OWA), VPN und auf RADIUS basierenden Diensten	
	Nativer Support von Microsoft Exchange Server 2013	
	Reine Software-Lösung - keine zusätzlichen Geräte oder Tokens nötig	
	Praktisch für mobile Mitarbeiter	
Mobile App	Installation mit einem Klick, einfache und effektive Benutzeroberfläche	
	Bereitstellung des OTP per Client App oder SMS	
	Generierung der OTP ist ohne Internetanbindung möglich	
	Kompatibel mit jedem Mobiltelefon-Betriebssystem, das SMS unterstützt	
	Apps für marktübliche mobile Betriebssysteme	
	Zugriffsschutz per PIN, um unbefugte Benutzung zu verhindern	
	Unterstützt mehrere OTP-Zonen, wie OWA-Zugriff, VPN-Zugriff und weitere	
	Die App ist in folgenden Sprachen erhältlich: Deutsch, Englisch, Französisch, Spanisch, Russisch und Slowakisch	
Server im Unternehmen	Innerhalb weniger Minuten einsatzbereit	
	Der Installer erkennt automatisch das Betriebssystem, überprüft die System-konfiguration und passt die Grundeinrichtung entsprechend an.	
	Eine nahtlose Integration in firmeneigene Systeme wird durch das SDK ermöglicht	
Remote Management	Unterstützt die Microsoft Management Console (MMC)	
	Active Directory Integration	
	ESET Secure Authentication erweitert ADUC mit einem Plugin, das zusätzliche Features zur Verwaltung der Einstellungen der Zwei-Faktor- Authentifizierung bereitstellt	
Unterstützte VPN-Appliances	Alle VPNs mit RADIUS-Support	Check Point Software SSL VPN
	Barracuda SSL VPN	F5 FirePass SSL VPN
	Cisco ASA (IPSec) VPN	Fortinet FortiGate SSL VPN
	Cisco ASA SSL VPN	Juniper SSL VPN
	Citrix Access Gateway SSL VPN	Palo Alto SSL VPN
	Citrix NetScaler SSL VPN	SonicWall SSL VPN

Systemanforderungen:

Server

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

Mobilgeräte

iOS 4.3 oder neuer (iPhone)
Android 2.1 oder neuer
Windows Phone 7 oder neuer
Windows Mobile 6
BlackBerry 4.3 bis 7.1 und 10 und neuer
Symbian - alle mit J2ME
Alle auf J2ME basierende Telefone

www.eset.de

Kontakt Information: