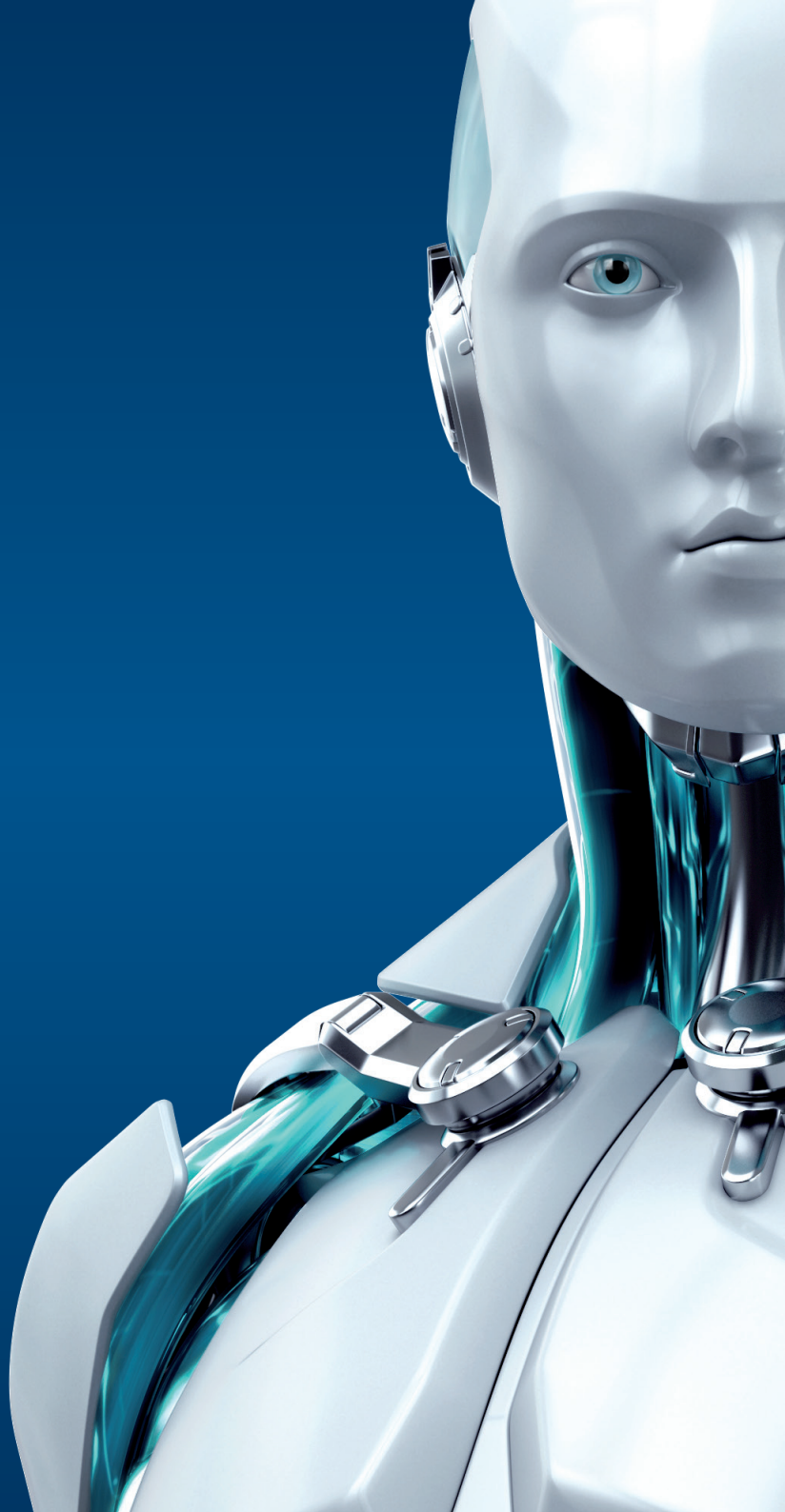
SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™



Ultra-strong authentication to protect network access and assets

ESET Secure Authentication provides powerful authentication to make remote access to the company network and sensitive data safe, but hassle-free.

It is a mobile-based solution that uses two-factor, one time password (2FA OTP) authentication for accessing the company's VPN and OWA (Outlook Web App). The advantage of one-time passwords (OTPs) is that they are randomly generated and can't be predicted or reused. ESET Secure Authentication natively supports Outlook Web Access/App for Microsoft Exchange 2007, 2010 and 2013. Native support is also provided for critical endpoints such as the Exchange Control Panel in 2010 and the Exchange Administration Centre in 2013.

Use it with a broad range of business tools, including Microsoft SharePoint, and Microsoft Dynamics CRM.

Strengthen the protection of your sensitive data accessed from outside the company - via a Remote Desktop Web Access login or VMware Horizon View.

Easily implement ESET Secure Authentication to your RADIUS-based services or use the API to integrate it with your existing authentication system based on Active Directory.

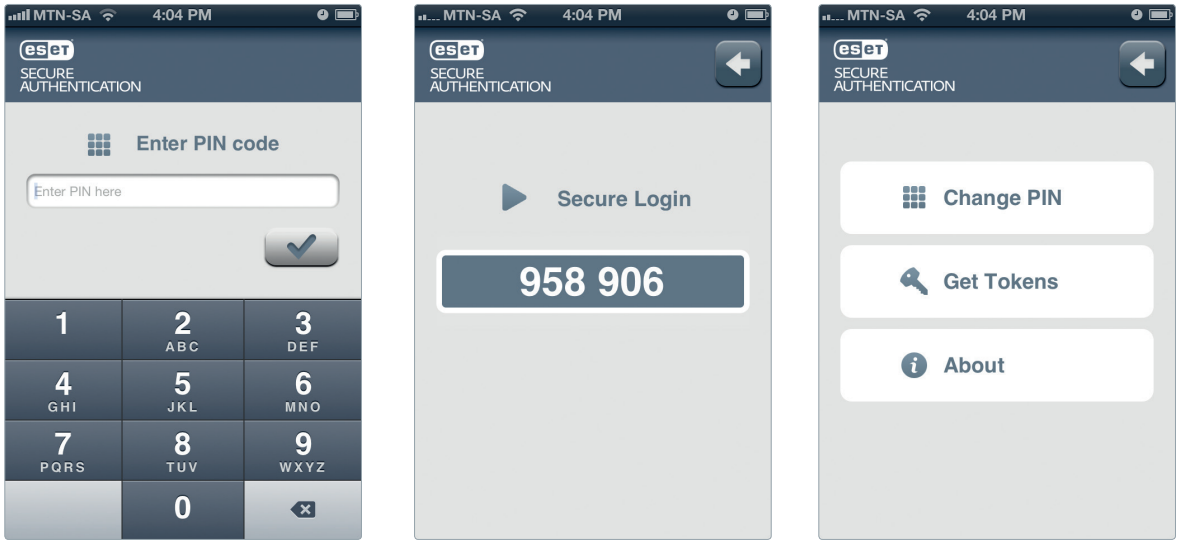
Moreover, the app comes with an SDK that enables you to implement the solution into any proprietary system, without the need to use Active Directory.

How does ESET Secure Authentication work?

Employees, upon remotely accessing the company network using VPN or OWA, receive a one-time password on their mobile phones. This password is then used to complement and strengthen the usual authentication process. As a result, the company data and assets are protected against intruders, dictionary attacks, password guessing and other forms of cybercrime. The technology used is two-factor, one time password authentication.

Two-factor Authentication (2FA) explained

As opposed to the standard password authentication, 2FA OTP uses two elements. These are "something that the user knows", such as a password or a PIN code, and "something that the user has", typically a mobile phone or hardware token. Used in combination, they provide greatly enhanced security for data access.



Solves the problem of:

- Static passwords that can be intercepted
- User-created passwords that are not a random combination of characters and can be easily guessed
- Re-use of passwords intended for access to company assets for private accounts
- Passwords containing user-specific data – e.g. a name, a date of birth
- Simple patterns to derive new passwords, such as "peter1", "peter2", etc.

Business benefits

- Helps prevent the risk of breaches with unique passwords for each access
- Protects from poor password practices
- Saves costs - no additional hardware needed
- Easy to migrate to and use
- Global technical support in local languages

IT benefits

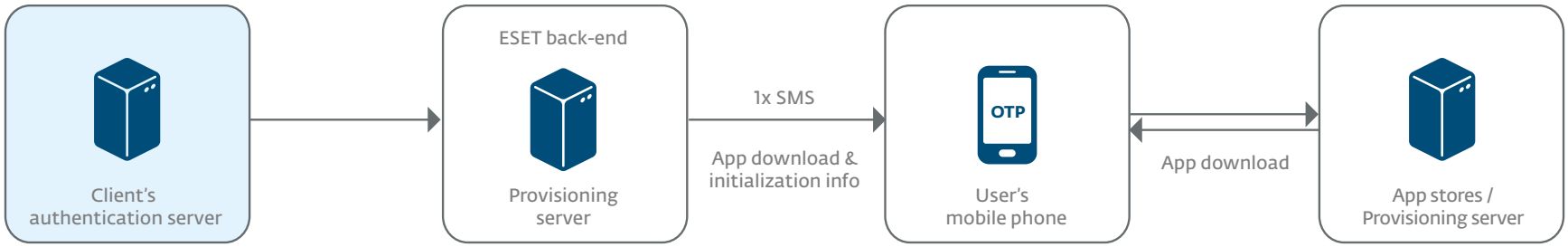
- Out-of-the-box solution
- App works without internet connection (once downloaded)
- Works with most VPN appliances
- Supports most types of mobile operating systems
- Global technical support in local languages
- API and SDK available for seamless integration

A closer look

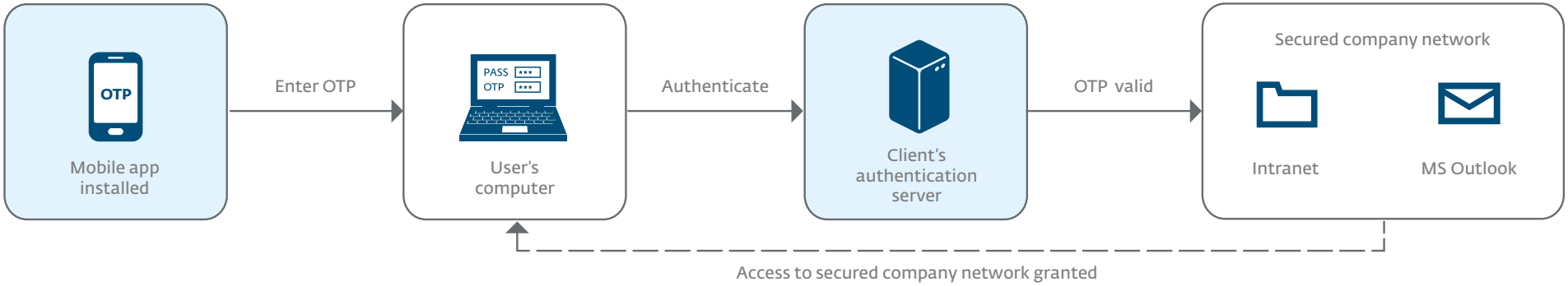
The architecture of ESET Secure Authentication is designed to only use your existing company infrastructure. In addition to the ESET Secure Authentication app on employee mobiles – the client side – it contains a server application that seamlessly integrates with the familiar network administrator environment of the MMC (Microsoft Management Console) and ADUC (Active Directory Users & Computers). With the authentication API, you can integrate ESET Secure Authentication with an existing authentication system. Moreover, the app's SDK allows to implement the solution into any proprietary system, without the need to use Active Directory. Take advantage of native support of Microsoft Exchange Server 2013, VMware Horizon View, and many other VPNs.

To distribute the ESET Secure Authentication app on mobile phones, all you need to know is the employee phone number. ESET Secure Authentication will send the user an SMS with an activation link. Clicking on the link automatically downloads an installer for that mobile platform.

Installation and first initialization



Client side communication



Datasheet

Two-factor Authentication	Mobile-based, two-factor (2FA) one-time password (OTP) authentication for a higher level of security	
	Native protection of Outlook Web App (OWA), VPNs and all RADIUS-based services	
	Native support of Microsoft Exchange Server 2013	
	Software only solution – no need to carry additional device or token	
	Convenient for the mobile workforce	
Client Side (mobile app)	One-tap installation, simple and effective user interface	
	Delivery of OTP via client application or SMS	
	OTP generating works independent of the availability of internet connection Compatible with any mobile phone supporting SMS messaging	
	Supports a broad range of mobile operating systems	
	PIN-protected access to prevent fraud in case of device theft or loss	
	Serves multiple OTP zones, e.g. OWA access, VPN access, and others	
	Apps available in these languages: English, German, Russian, French, Spanish, Slovak	
Server Side	Out-of-the-box solution	
	Easy double-click installation and setup	
	The installer automatically recognizes OS and selects all suitable components	
	SDK allows implementation into any proprietary company system	
Remote Management	Supports Microsoft Management Console (MMC)	
	Active Directory integration	
	ESET Secure Authentication extends Active Directory Users & Computers (ADUC plugin) with additional features to enable managing the users' two-factor authentication settings	
Supported VPN Appliances	VMware View installation	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

System Requirements:

Server Side
32&64-bit versions of Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
Microsoft Windows Small Business Server 2008

Client Side
iOS 4.3 or higher (iPhone)
Android 2.1 or higher
Windows Phone 7 or newer
Windows Mobile 6
BlackBerry 4.3 to 7.1 and 10 and higher
Symbian - all supporting J2ME
All J2ME enabled phones

www.eset.com

Contact information: