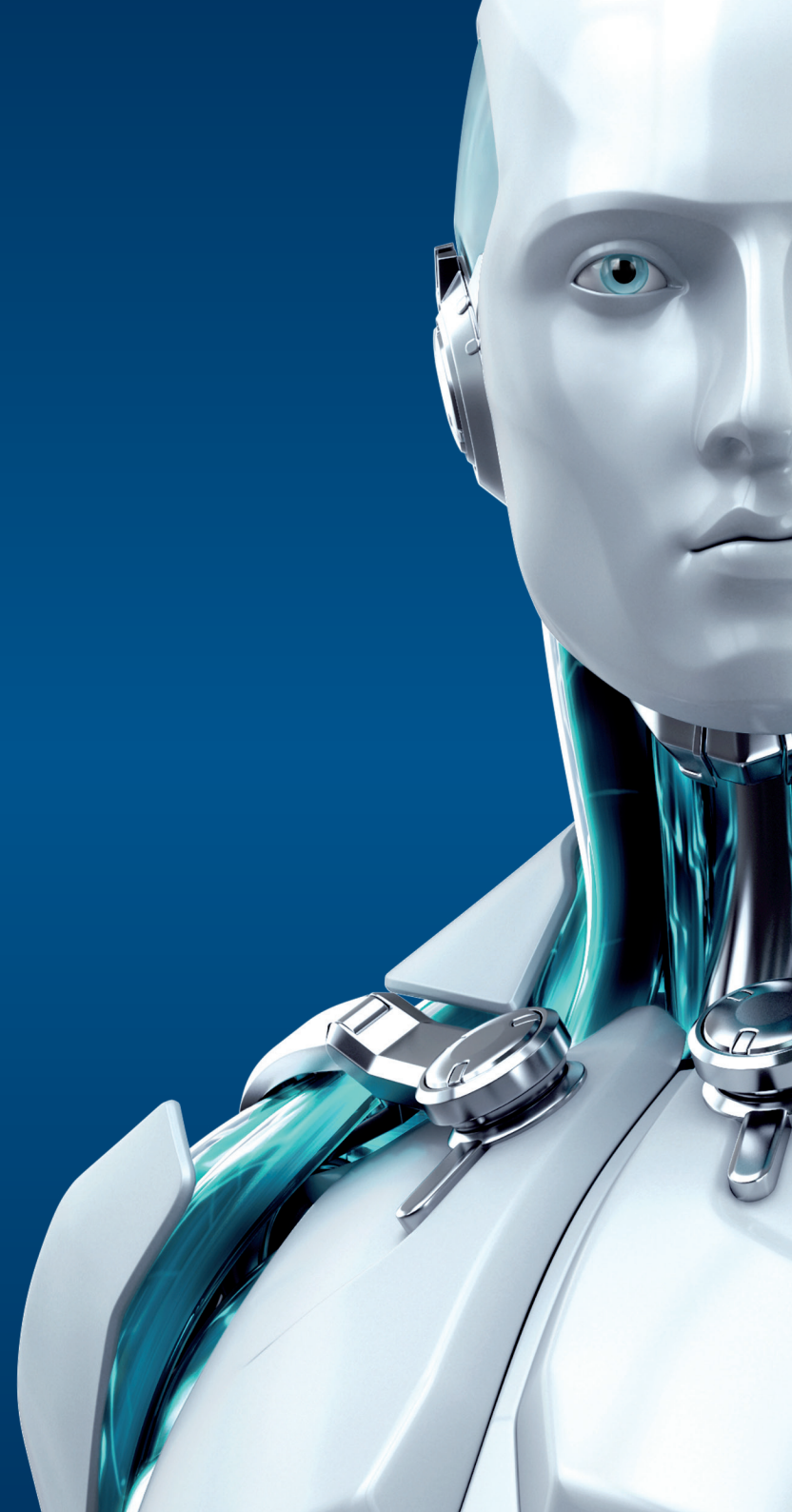




SECURE AUTHENTICATION

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.

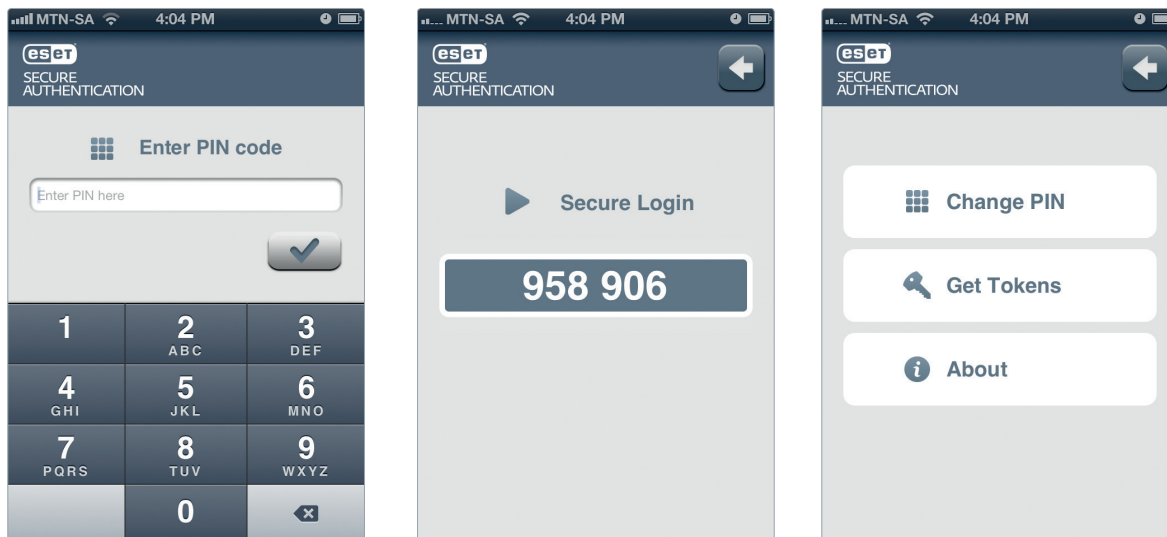
How does ESET Secure Authentication work?

Employees, upon remotely accessing the company network, 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

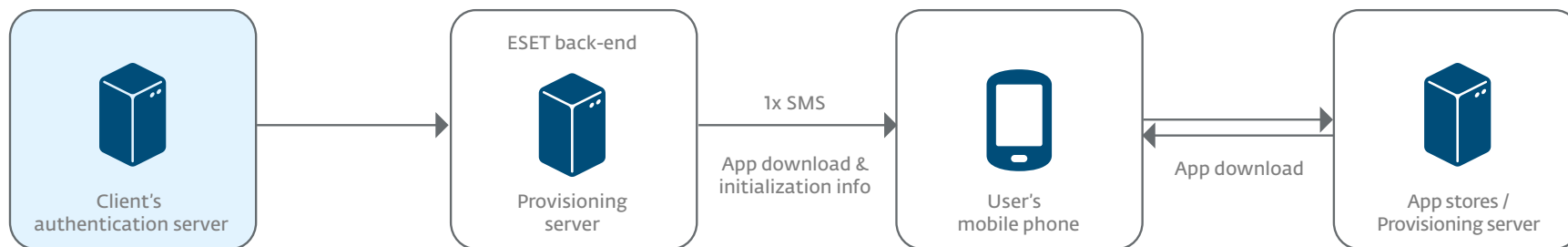
- API/SDK for easy integration into proprietary software and business tools
- App works without internet connection (once downloaded)
- Works with most VPN appliances
- Supports most types of mobile operating systems
- Global technical support in local languages
- Out-of-the-box solution

A closer look

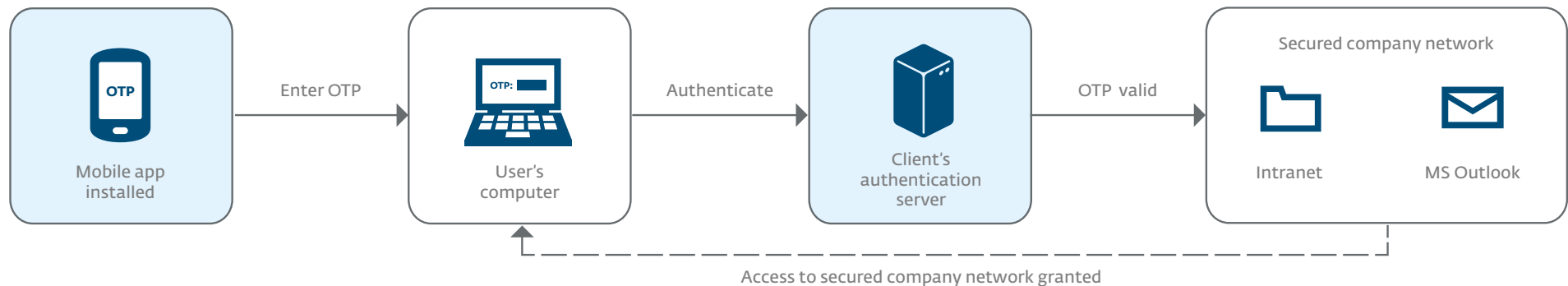
The architecture of ESET Secure Authentication is designed to only use your existing company infrastructure. In addition to the ESET Secure Authentication app on employee mobiles – the client side – it contains a server application that seamlessly integrates with the familiar network administrator environment 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 enables integration of 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, Citrix XenApp and many 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	<p>Mobile-based, two-factor (2FA) one-time password (OTP) authentication for a higher level of security</p> <p>Native protection of Outlook Web App (OWA), VPNs and all RADIUS-based services</p> <p>Native support of Microsoft Exchange and other business tools</p> <p>Software only solution – no need to carry additional device or token</p> <p>Convenient for the mobile workforce</p>										
Client Side (mobile app)	<p>One-tap installation, simple and effective user interface</p> <p>Delivery of OTP via client application or SMS</p> <p>OTP generation works independently of an available internet connection</p> <p>Compatible with any mobile phone supporting SMS messaging</p> <p>Supports a broad range of mobile operating systems</p> <p>PIN-protected access to prevent fraud in case of device theft or loss</p> <p>Serves multiple OTP zones, e.g. OWA access, VPN access, and others</p> <p>Apps available in these languages: English, German, Russian, French, Spanish, Slovak</p>										
Server Side	<p>Out-of-the-box solution</p> <p>Easy double-click installation and setup</p> <p>The installer automatically recognizes OS and selects all suitable components</p> <p>SDK allows implementation into any proprietary company system</p>										
Remote Management	<p>Supports Microsoft Management Console (MMC)</p> <p>Active Directory integration</p> <p>ESET Secure Authentication extends Active Directory Users & Computers (ADUC plugin) with additional features to enable managing the users' two-factor authentication settings</p>										
Supported VPN Appliances	<table border="0"> <tr> <td>Barracuda</td> <td>F5 FirePass</td> </tr> <tr> <td>Cisco ASA</td> <td>Fortinet FortiGate</td> </tr> <tr> <td>Citrix Access Gateway</td> <td>Juniper</td> </tr> <tr> <td>Citrix NetScaler</td> <td>Palo Alto</td> </tr> <tr> <td>Check Point Software</td> <td>SonicWall</td> </tr> </table>	Barracuda	F5 FirePass	Cisco ASA	Fortinet FortiGate	Citrix Access Gateway	Juniper	Citrix NetScaler	Palo Alto	Check Point Software	SonicWall
Barracuda	F5 FirePass										
Cisco ASA	Fortinet FortiGate										
Citrix Access Gateway	Juniper										
Citrix NetScaler	Palo Alto										
Check Point Software	SonicWall										
Supported VDI platforms	<table border="0"> <tr> <td>VMware Horizon View</td> <td>Citrix XenApp</td> </tr> </table>	VMware Horizon View	Citrix XenApp								
VMware Horizon View	Citrix XenApp										



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, 2011

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

Copyright © 1992 – 2014 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2000.

Contact information: