ESET Secure Authentication helps businesses access their data securely. Our solution utilizes the existing Active Directory domain, allowing you to set up ESET's two-factor authentication in just 10 minutes – and thus easily reduce the risk of data breaches, caused by stolen, weak or compromised passwords.

The solution consists of the server side and the client side – the latter comes in the form of a mobile app. The authentication options include Push Authentication, as well as generation and delivery one-time passwords (OTPs) via the mobile app, but also via SMS messages or your organization's existing hardware tokens.

You can use ESET Secure Authentication for:
- Accessing your company's VPN
- Remote Desktop Protocol
- Additional authentication for desktop login (signing into an operating system)
- Web/cloud services via Microsoft ADFS 3.0, such as Office 365 and Google Apps
- Various Microsoft Web Apps, such as Outlook Web Access (OWA)
- Exchange Control Panel 2010 & Exchange Administrator Centre 2013
- VMware Horizon View
- RADIUS-based services

### Business benefits
- Helps prevent breaches by employing unique passwords for each access
- Protects against poor password practices
- Improved productivity and user experience—thanks to one-tap push authentication
- Saves costs—no additional hardware needed
- Easy to migrate to and use
- Supports existing hardware tokens to meet compliance requirements
- Also adds 2FA to your cloud applications, such as Office 365 or Google Apps

### IT benefits
- API/SDK for easy integration into proprietary software and business tools
- App works without internet connection (once downloaded)
- Supports most types of mobile operating systems
- Global technical support in local languages
- Out-of-the-box solution
- Increases productivity and reduces unnecessary friction when accessing trusted sites, thanks to IP whitelisting
- Tools for deployment and configuration in large user environments
## Two-factor authentication
- Mobile-based, two-factor (2FA) authentication for a higher level of security
- Native support for a broad range of platforms (see supported platforms overview, below)
- Software-based solution—no need to carry an additional device or token
- Convenient for your mobile workforce
- Support for hardware tokens
- Compatible with any mobile phone that supports SMS messaging

### Client side (mobile app)
- One-tap installation, simple and effective user interface
- Supports a broad range of mobile operating systems
- PIN-protected access to prevent fraud in case of device theft or loss
- Apps available in 16 languages, including English, German, Russian, French and Spanish

### Authentication methods
- Mobile client app—generates one-time passwords (OTPs); no internet connection required
- Push Authentication—single-touch authentication via mobile phone (requires mobile client app; works with Android and iOS devices)
- SMS delivery of one-time passwords
- Hardware tokens (while the solution does not require hardware tokens to work, it supports all event-based HOTP tokens that are OATH-compliant)
- Custom methods (e.g. via email)

### Server side
- Out-of-the-box solution
- Easy double-click installation and setup
- The installer automatically recognizes the OS and selects all suitable components
- Interactive installer, drop-in installation into ADFS

### Custom integration options
- In Active Directory environment, use either ESET Secure Authentication API or User Management API for easy integration into proprietary systems
- SDK allows for implementation for non-Active Directory users

### Remote management
- Via Microsoft Management Console (MMC)
- Active Directory integration for easy user management
- ESET Secure Authentication extends Active Directory Users & Computers (ADUC plugin) with additional features to enable management of users’ two-factor authentication settings
# Supported platforms overview


<table>
<thead>
<tr>
<th>Remote login platforms</th>
<th>Remote Desktop Protocol</th>
<th>VPN Protection:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local login protection (Windows)</th>
<th>Windows 7, 8, 8.1, 10</th>
<th>Windows Server 2008 R2 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active directory federation services</td>
<td>Microsoft ADFS 3.0 (Windows Server 2012 R2)</td>
<td>Citrix XenApp</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported VDI platforms</th>
<th>VMware Horizon View</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Custom integration | ESET Secure Authentication easily integrates with your RADIUS-based services, as well as via the ESET Secure Authentication API or the User Management API to your existing Active Directory-based authentication. Non Active Directory customers with custom systems can use the easy-to-deploy SDK. |

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported mobile phone platforms (Client-side app)</th>
<th>iOS</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Android</td>
<td>Symbian—all supporting J2ME</td>
</tr>
<tr>
<td></td>
<td>Windows Phone</td>
<td>All J2ME enabled phones</td>
</tr>
<tr>
<td></td>
<td>Windows Mobile</td>
<td></td>
</tr>
</tbody>
</table>