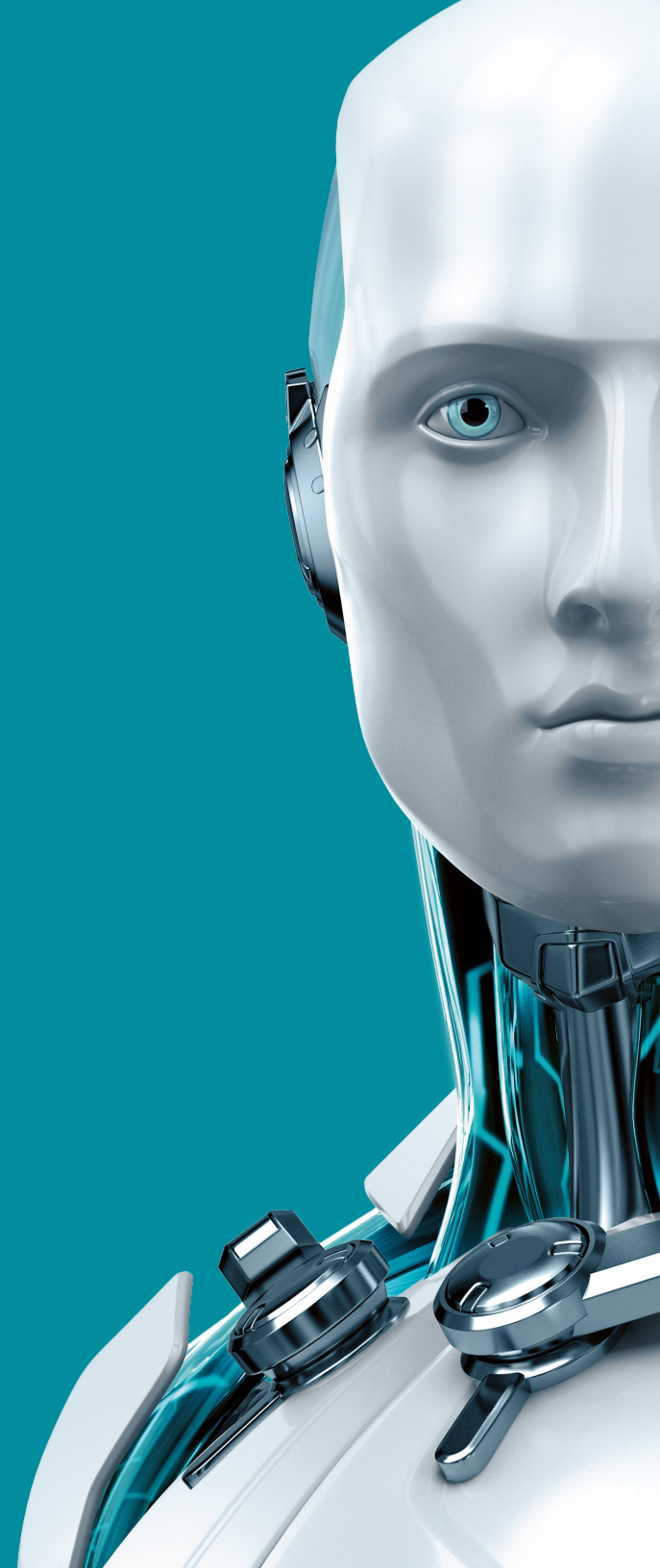




# ENDPOINT ENCRYPTION



ENJOY SAFER TECHNOLOGY®





# ENDPOINT ENCRYPTION

**ESET Endpoint Encryption** is a simple-to-use encryption application for companies large and small. Take advantage of the optimized setup that speeds up the time to adoption for admins. The client side requires no user interaction, increasing user compliance and the security of your company data.

## Client side

Data is a critical part of every organization, but this most valuable asset often poses a huge risk when it travels or is transmitted beyond the corporate network. Full disk- and removable media-encryption protect laptop computers against the unexpected. File, folder and email encryption allow fully secure collaboration across complex workgroups and team boundaries, with security policy enforced at all endpoints via remote central management. Meet your data security compliance obligations with a single MSI package.

---

<b>Zero User Interaction</b>	The implementation of encryption is completely transparent for the users and requires no action on their part
<b>Full disk encryption</b>	Encrypt only disks and partitions you want On-screen keyboard that allows encrypting of Windows tablets and convertible devices Transparent preboot security using FIPS 140-2 validated, 256-bit AES encryption Encryption may be started and managed remotely Remote user password recovery Enhanced workstation screening prior to encryption, including Safe Start mode Fully compatible with Microsoft Windows 10, 8 and 8.1, with support for UEFI and GPT Support of Trusted Platform Module (TPM)
<b>Removable media encryption</b>	No extra space is reserved for encrypted content, and the whole device capacity can be used by the user Policy-driven encryption includes “Go” portable encryption, on-device software for use on unlicensed systems Works with any USB drive, CD and DVD media
<b>File &amp; folder encryption</b>	Encrypt only files and folders you want All files moved to an encrypted folder are encrypted immediately
<b>Email encryption</b>	Transparent email encryption for Outlook through a dedicated plugin The email can be decrypted only by recipients who share the same key as the sender Text and clipboard encryption works with any email client, including webmail

---

# System requirements

## Client & server side:

Microsoft® Windows® 10

Microsoft Windows 8, 8.1\*

Microsoft Windows 7

Microsoft Windows Vista

Microsoft Windows XP SP 3

Microsoft Windows Server 2003 – 2012

\* Microsoft Windows RT is not supported;  
full disk encryption requires keyboard

## Mobile platforms:

iOS

## Certifications:

FIPS 140-2 level 1

## Algorithms & standards:

AES 256 bit

AES 128 bit

SHA 256 bit

SHA1 160 bit

RSA 1024 bit

Triple DES 112 bit

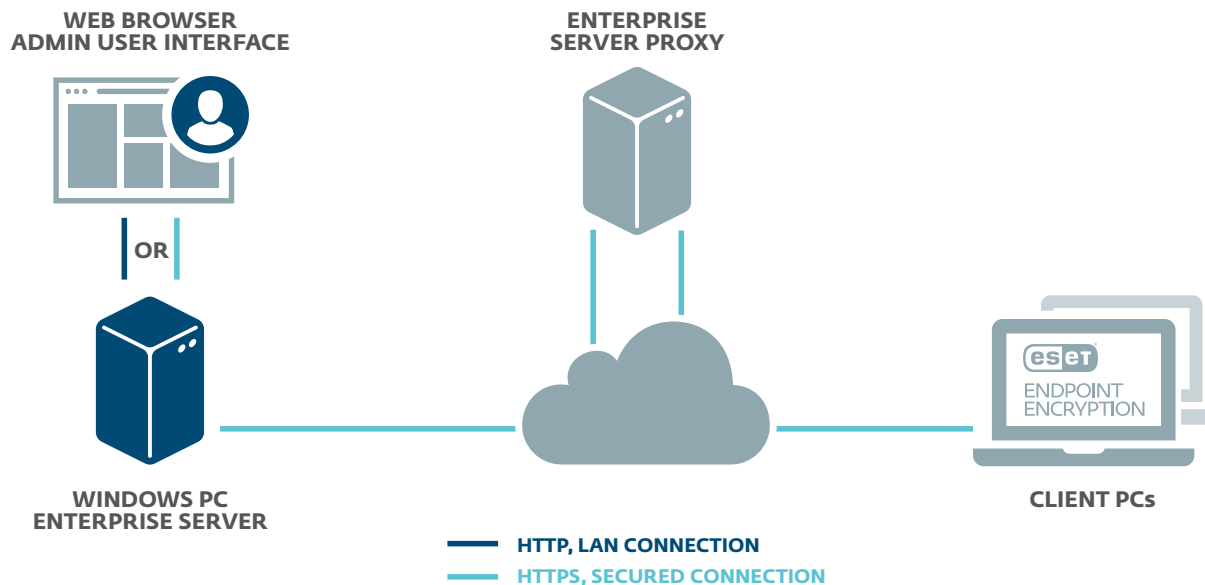
Blowfish 128 bit

Desktop	Essential	Standard	Pro
Full disk encryption	—	—	✓
Removable media encryption	—	✓	✓
Go portable encryption	—	✓	✓
File & folder encryption	✓	✓	✓
Email encryption	✓	✓	✓
Text & clipboard encryption	✓	✓	✓
Virtual disks & encrypted archives	✓	✓	✓
Centralized management compatible	✓	✓	✓

A single install serves all license types. Upgrading is silent and automatic for managed users; unmanaged users simply enter an activation code.

Mobile	Unmanaged mode	Managed mode
File encryption	✓	✓
Email encryption	✓	✓
Text & clipboard encryption	✓	✓
Encryption using passwords	✓	✓
Encryption using encryption keys	—	✓

<b>Remote central management</b>	<p>Manage any user or workstation with a standard internet connection</p> <p>All commands, updates, status requests and responses are posted via the enterprise proxy</p> <p>No dependency on Active Directory or any existing server architecture installation</p> <p>Secure connectivity allows control of endpoint encryption keys, security policy and software features beyond the corporate security boundary</p> <p>Full remote management, creation and removal of user accounts</p>
<b>Encryption key management</b>	<p>Patent-pending technology</p> <p>Add or remove any or all encryption keys</p> <p>Change the encryption policy remotely and silently, without user interaction</p>
<b>Enterprise server proxy</b>	<p>By using the enterprise proxy as an intermediary, all connections from client and server are outgoing</p> <p>All information is encrypted with either RSA or AES, and the connection itself is SSL encrypted</p> <p>No need for your own SSL certificate and additional hardware, network or firewall changes</p>



## Server side

The Enterprise Server can manage users and workstations together or independently. Activation and changes to security policy, software feature set, encryption keys and endpoint status are all handled securely through the cloud, keeping your most high-risk endpoints under close control at all times. Only ESET Endpoint Encryption offers full control wherever your users are.



**FREE U.S.-BASED  
TECHNICAL  
SUPPORT**

As an ESET customer, Do More with the help of our technical support team.

© 1999-2017 ESET, LLC, d/b/a ESET North America. All rights reserved.

ESET, the ESET Logo, ESET android figure, ESET SMART SECURITY, ESET CYBER SECURITY, ESET.COM, ESET.EU, NOD32, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid and LiveGrid logo are trademarks, service marks and/or registered trademarks of ESET, LLC, d/b/a ESET North America and/or ESET, spol. s r. o., in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.