

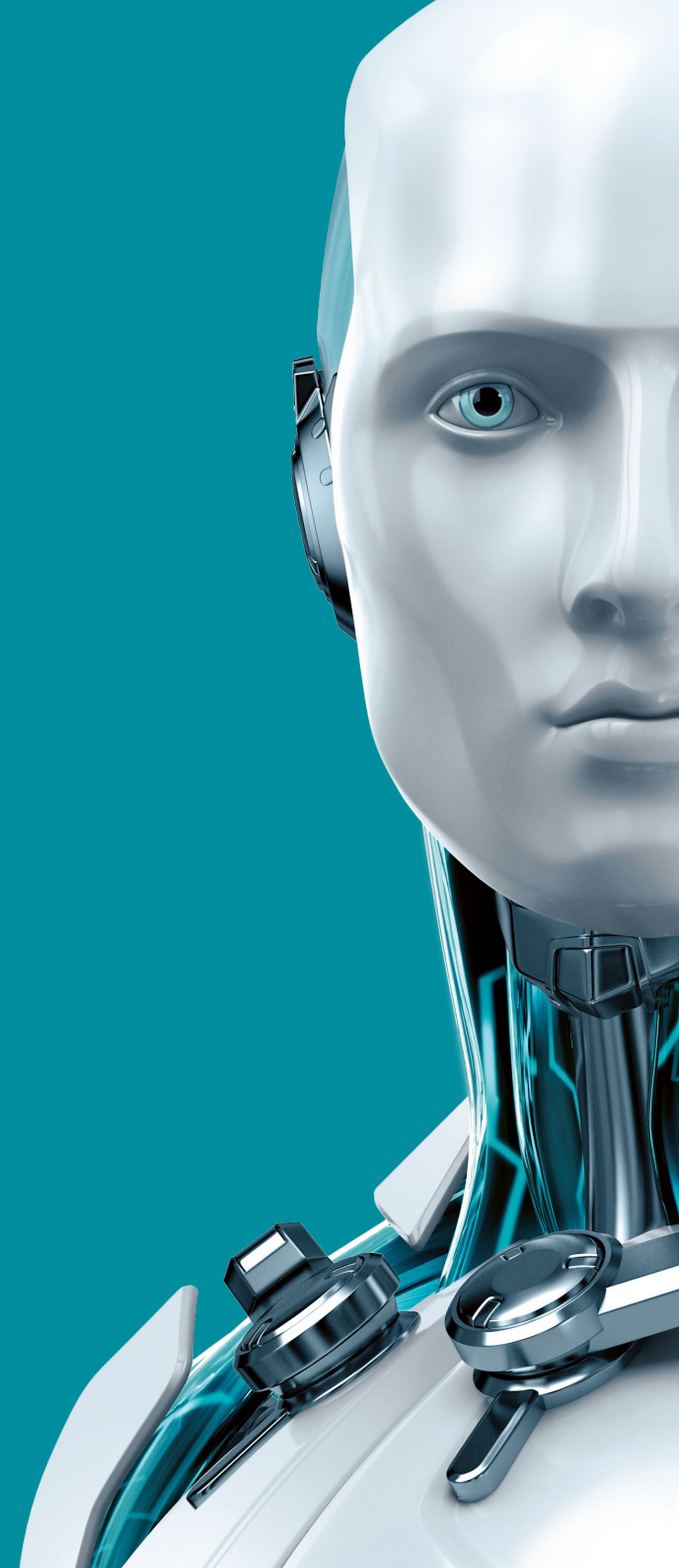


SECURITY

FOR MICROSOFT
SHAREPOINT SERVER



ENJOY SAFER TECHNOLOGY™





SECURITY FOR MICROSOFT SHAREPOINT SERVER

Keeps SharePoint clean by scanning files within the SharePoint database. Provides full-fledged server protection.

Prevents malicious threats and unauthorized users breaching system security and is fully manageable via ESET Remote Administrator 6.

Supported SharePoint versions:

Microsoft SharePoint Server 2016

Microsoft SharePoint Server 2013

Microsoft SharePoint Server 2010

Microsoft SharePoint Enterprise 2010

Microsoft Office SharePoint Server 2007

SharePoint Server protection

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware Optional cloud-powered scanning: Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data is not personally attributable.
Database Scan	Administrator can decide to run thorough database scans scheduled for off-peak hours and automate in-place cleaning or enforce inspection of various document or object versions in any available SharePoint site. Database queries can be parallelized into multiple scanning threads to significantly improve on-demand scanning time.
Database Object Rules	For both on-demand and on-access scanning a separate set of decision logic is available that can handle attributes ranging from file size or real content of scanned object to archive inspection and allows unlimited customizations by any desired chaining of rules and subsequent actions to execute.
Virtualization Support	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so identical files are not scanned again, resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, so these don't have to be downloaded every time a virtual machine is reverted to default snapshot.
Exploit Blocker	Strengthens security of applications such as web browsers, PDF readers, email clients or MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention, even from heavily obfuscated malware.
Native Clustering Support	Allows you to configure the solution to automatically replicate settings when installed in a cluster environment. An intuitive wizard makes it easy to interconnect several installed nodes of ESET Security for MS SharePoint within a cluster and manage them as one, eliminating the need to replicate changes in configuration manually to other nodes in the cluster.
Storage Scan	Allows you to easily set up on-demand scans of connected Network Attached Storage (NAS). Combined with ESET Shared Local Cache installed within the network, this can drastically reduce the amount of disk input/output operations on network drives.

Data Access Protection

Anti-Phishing	Protects you from attempts by fake websites to acquire sensitive information.
Device Control	Blocks unauthorized portable devices from connecting to the server. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that his device is blocked and gives him the option to access the device, with activity logged.

Scanning and Update Options

Idle-State Scanner	Aids system performance by performing a full scan proactively when the computer is not in use. Helps speed up subsequent scans by populating the local cache.
Update Rollback	Lets you revert to a previous version of protection modules and virus signature database. Allows you to freeze updates as desired - opt for temporary rollback or delay until manually changed.
Postponed Updates	Provides the option to download from three specialized update servers: pre-release (beta users), regular release (recommended for non-critical systems) and postponed release (recommended for company-critical systems – approximately 12 hours after regular release).
Local Update Server	Saves company bandwidth by downloading updates only once – to a local mirror server. Mobile workforce updates directly from ESET Update Server when the local mirror is not available. Secured (HTTPS) communication channel is supported.



FREE LOCAL
TECHNICAL
SUPPORT

Do More with the help of our specialists.
On call to provide technical support when
you need it, in your language.

Usability

Process Exclusions	The admin can define processes which are ignored by the real-time protection module – all file operations that can be attributed to these privileged processes are considered to be safe. This is especially useful for processes that often interfere with real-time protection, like backup or live virtual machine migration. Excluded process can access even unsafe files or objects without triggering an alert.
Windows Management Instrumentation (WMI) Provider	Provides the possibility to monitor key functionalities of ESET Server Security via Windows Management Instrumentation framework. This allows integration of ESET Server Security into 3rd party management and SIEM software, such as Microsoft System Center Operations Manager, Nagios, and others.
Customizable GUI Visibility	Visibility of Graphical User Interface (GUI) to end user can be set to Full or Terminal. By hiding the GUI completely, the "egui.exe" process does not run at all, resulting in even lower system resource consumption by the ESET solution.
ESET License Administrator	Makes it possible to handle all licenses transparently, from one place via web browser. You can merge, delegate and manage all licenses centrally in real-time, even if you are not using ESET Remote Administrator.
Component-Based Installation	Allows you to choose which components to install: <ul style="list-style-type: none">– Real-Time File System Protection– Web and Email– Device Control– Graphical User Interface (GUI)– ESET Log Collector– ESET SysInspector– Offline Help
Remote Management	ESET Server solutions are fully manageable via ESET Remote Administrator. Deploy, run tasks, set up policies, collect logs, and get notifications and an overall security overview of your network – all via a single web-based management console.
ESET Log Collector	A simple tool which collects all logs relevant for troubleshooting, assisted by ESET's technical support, and bundles them into a single archive which can be sent via email or uploaded to a shared network drive to speed up the troubleshooting process.

Copyright © 1992 – 2017 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 9001:2008.