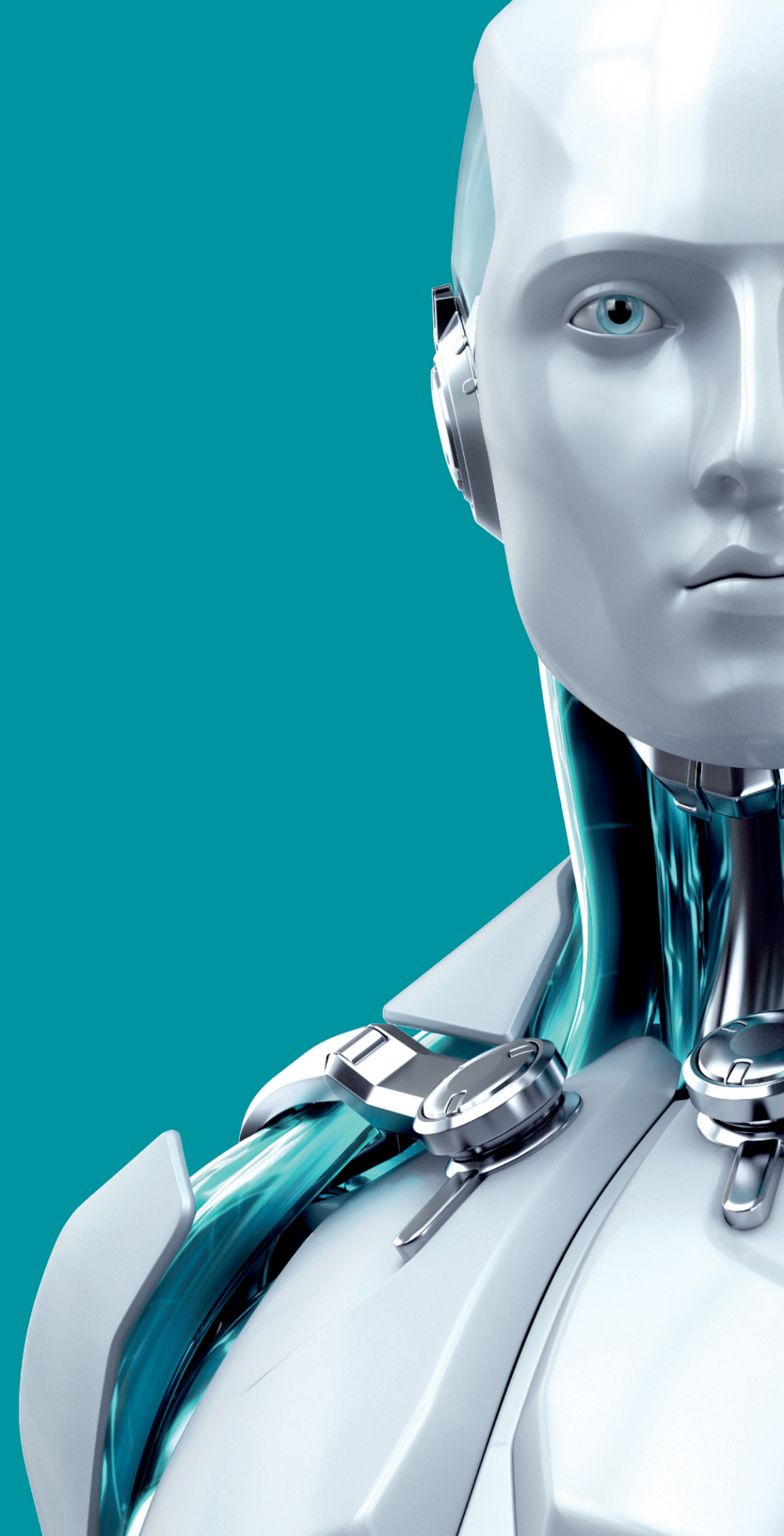




MAIL
SECURITY
FOR IBM DOMINO

ENJOY SAFER TECHNOLOGY®





MAIL SECURITY

FOR IBM DOMINO

ESET Mail Security for IBM Domino integrates powerful antivirus and antispam detection capabilities that ensure all harmful email-borne content is filtered away at the server level, while ESET's light footprint means your system can continue to run at full speed.

With our solution, you get complete server protection – including the server's own file system. You can apply policies for specific content based on real file type, and monitor security status or fine-tune configuration easily via our user-friendly ESET Remote Administrator tool.

Antimalware protection and Antispam

Antivirus and Antispyware

Eliminates all types of threats, including viruses, rootkits, worms and spyware with optional cloud-powered scanning for even better performance and detection.

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.

Antispam and Anti-Phishing

Stops spam and phishing attempts, and delivers high interception rates without the need to manually set a Spam Confidence Level (SCL) Threshold. After installation, the antispam module is ready to run without the need to manually tune settings or thresholds.

Database On-Demand Scan

Administrators can choose which databases will be scanned, thereby reducing to a minimum the server resources devoted to the task.

Message Processing Rules

Message processing rules offer a wide range of combinations by which every single message can be handled. The evaluated parameters include standard fields like subject, sender, body and specific message header, but also allow further conditional processing depending on previous anti-spam filtering or antivirus scanner results. Corrupted or password-protected archives are detected and attachments are screened internally to determine real file type, not only purported extension. Rules can be changed according to the desired actions.

Exploit Blocker

Strengthens the security of applications such as web browsers, PDF readers, email clients and 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.

Host-Based Intrusion Prevention System (HIPS)

Enables you to define rules for system registry, processes, applications and files. Provides anti-tamper protection and detects threats based on system behavior.

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. Allows soft blocking, which notifies the end user that his device is blocked and gives him the option to access it, with activity logged.



FREE LOCAL
TECHNICAL
SUPPORT

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

Complex infrastructure covered

Snapshot Independence	ESET updates and program modules can be stored outside of the default location—so are not affected by reverting to an earlier snapshot of the virtual machine. As a result, the updates and modules don't have to be downloaded every time a virtual machine is reverted to an earlier snapshot and the reverted machine can utilize untouched updates and avoid large downloads, resulting in faster snapshot recovery times.
Native Clustering Support	Allows you to configure the solution to automatically replicate settings when installed in a cluster environment. Our intuitive wizard makes it easy to interconnect several installed nodes of ESET Mail Security within a cluster and manage them as one, eliminating the need to replicate changes in configuration manually to other nodes in the cluster.
ESET Shared Local Cache	<p>ESET Shared Local Cache compares the metadata of files with the metadata of those that have already been stored, and automatically skips previously whitelisted clean files. Whenever a new, previously unscanned file is found, it's automatically added to the cache.</p> <p>This means that files already scanned on one virtual machine are not repeatedly scanned on other virtual machines within the same virtual environment, resulting in a significant scanning boost. As communication happens over the same physical hardware, there is practically no delay in scanning, resulting in considerable resource savings.</p>
Windows Management Instrumentation (WMI) Provider	Allows you to monitor key functionalities of ESET Mail Security via Windows Management Instrumentation framework. This allows integration of ESET Mail Server into 3rd party management and SIEM software, such as Microsoft System Center Operations Manager, Nagios, and others.

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.

Incremental Micro-Definitions

Regular updates and actualizations are downloaded and applied incrementally in small packages. This concept conserves system resources and internet bandwidth without any noticeable impact on the speed of the whole network infrastructure and servers, or on endpoints system demands on memory or the CPU.

Component-Based Installation

Apart from the required components, ESET allows you to choose to install only those components you need:

- Real-Time File System Protection
- Web and Email Protection
- Device Control
- Graphical User Interface (GUI)
- ESET Log Collector
- and others

Remote Management

ESET Mail Security is 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.

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.
