

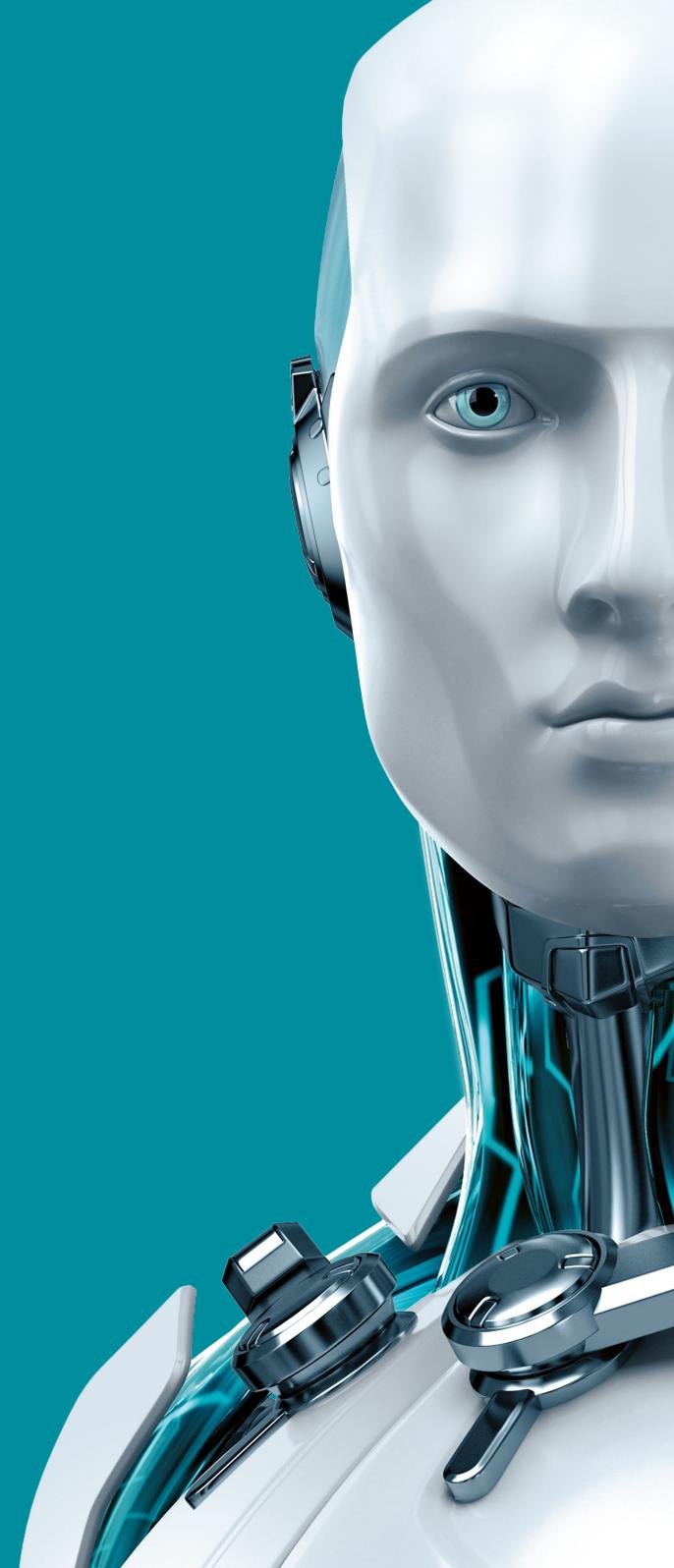


# ENDPOINT ANTIVIRUS

FOR WINDOWS



ENJOY SAFER TECHNOLOGY™





# ENDPOINT ANTIVIRUS

FOR WINDOWS

ESET Endpoint Antivirus with award-winning ESET NOD32® technology delivers superior detection power for your business.

Its low system demands and virtualization capability keep your system humming.

Keep the security of offline devices under control, and customize scanning and update options as you see fit. Control it all effortlessly with our all-new, user-friendly remote administrator tool.

## Endpoint Protection

---

<b>Antivirus and Antispyware</b>	Eliminates all types of threats, including viruses, rootkits, worms and spyware.  <b>Optional cloud-powered scanning:</b> 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 are not personally attributable.
<b>Virtualization Support</b>	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so same files are not scanned again resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, thus these don't have to be downloaded every time after the virtual machine is reverted to default snapshot.
<b>Host-Based Intrusion Prevention System (HIPS)</b>	Enables you to define rules for system registry, processes, applications and files. Provides tampering protection and detects threats based on system behavior.
<b>Exploit Blocker</b>	Strengthens security of applications on users' systems, such as web browsers, PDF readers, email client 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.
<b>Advanced Memory Scanner</b>	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.
<b>Cross-Platform Protection</b>	ESET security solutions for Windows are capable of detecting Mac OS threats and vice-versa, delivering better protection in multi-platform environments.

---

## Data Access Protection

---

<b>Anti-Phishing</b>	Protects end users from attempts by fake websites masquerading as trustworthy ones to acquire sensitive information such as usernames, passwords or banking and credit card details.
<b>Device Control</b>	Blocks unauthorized devices (CDs/DVDs and USBs) from your system. Enables you to create rules for user groups to comply with your company policies. Soft blocking notifies the end user his device is blocked and gives him the option to access the device, with activity logged.

---

## Scanning and Update Options

---

<b>Idle-State Scanner</b>	Aids system performance by performing full scan proactively when the computer is not in use. Helps speed up subsequent scans by populating the local cache.
<b>First Scan after Installation</b>	Provides the option to automatically run low priority on-demand scan 20 minutes after installation, assuring protection from the outset.
<b>Update Rollback</b>	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.
<b>Postponed Updates</b>	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).
<b>Local Update Server</b>	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

<b>RIP &amp; Replace</b>	Other security software is detected and uninstalled during installation of ESET Endpoint solutions. Supports both 32 and 64-bit systems.
<b>Customizable GUI Visibility</b>	Visibility of Graphical User Interface (GUI) to end user can be set to: Full, Minimal, Manual or Silent. Presence of ESET solution can be made completely invisible to end user, including no tray icon or notification windows. 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.
<b>ESET License Administrator</b>	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.
<b>Touchscreen Support</b>	Supports touch screens and high-resolution displays. More padding for and complete rearrangement of GUI elements. Basic frequently used actions accessible from tray menu.
<b>Low System Demands</b>	Delivers proven protection while leaving more system resources for programs that end users regularly run. Can be deployed on older machines without the need for an upgrade, thereby extending hardware lifetime. Conserves battery life for laptops that are away from the office, using battery mode.
<b>Right-to-Left Language Support</b>	Native right-to-left language support (e.g. for Arabic) for optimum usability.
<b>Remote Management</b>	ESET Endpoint 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.

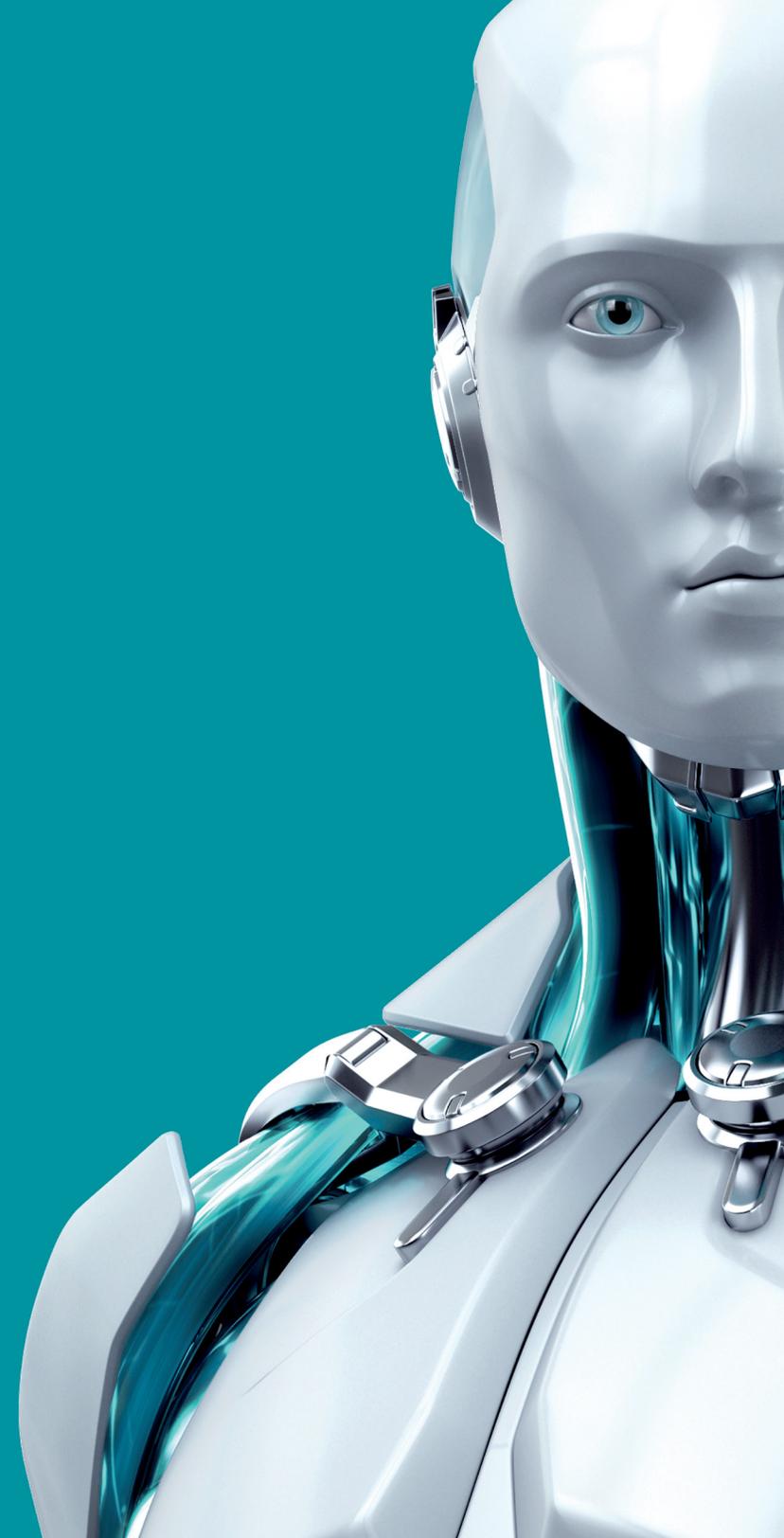
Copyright © 1992 – 2017 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark 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.



# FILE SECURITY

FOR MICROSOFT™  
WINDOWS SERVER

ENJOY SAFER TECHNOLOGY®





# FILE SECURITY

## FOR MICROSOFT WINDOWS SERVER

ESET File Security for Microsoft Windows® Server provides superior protection for your company's data passing through the file server.

The solution utilizes the proven ESET NOD32® scanning engine at its core and combines high detection speed, smooth performance and stability to ensure a continuously high level of security.

Maintain more memory and CPU power for critical system tasks thanks to the solution's minimal resource usage. Stay on top of server security with detailed and comprehensive security logs, vital protection status information and system notifications.

## File 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.

---

### 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.

---

### Hyper-V storage scan

Agentless scanning for malware on Hyper-V based virtual servers; scans offline virtual server disks to save system resources.

---

### 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 File Security 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.

---

### Specialized cleaners

Provides most relevant critical malware standalone cleaners within the product interface for malware that cannot be removed by the regular cleaner.

---

### 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.

---



FREE LOCAL  
TECHNICAL  
SUPPORT

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

## Data access protection

---

<b>Anti-phishing</b>	Protects you from attempts by fake websites to acquire sensitive information.
<b>Device control</b>	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 that the device is blocked and gives user the option of accessing the device, with activity logged.

---

## Scanning and update options

---

<b>Idle-state scanner</b>	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.
<b>Update rollback</b>	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.
<b>Postponed updates</b>	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).
<b>Local update server</b>	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.

---

## 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

Allows you to monitor key functionalities of ESET File Security via Windows Management Instrumentation framework. This allows integration of ESET File Server 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, Minimal, Manual or Silent.

Presence of ESET solution can be made completely invisible to end user, including no tray icon or notification windows.

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:

- Real-Time File System Protection
  - Web Protocol Filtering
  - Device Control
  - Graphical User Interface (GUI)
  - E-mail Client Protection
  - ESET Log Collector
  - ESET SysInspector
  - ESET SysRescue
  - Offline Help
- 

### Remote management

ESET endpoint 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 that collects all logs relevant for troubleshooting, assisted by ESET’s technical support, and bundles them into a single archive that can be sent via email or uploaded to a shared network drive to speed up the troubleshooting process.

---



# REMOTE ADMINISTRATOR



ENJOY SAFER TECHNOLOGY®





# REMOTE ADMINISTRATOR

ESET Remote Administrator empowers your IT staff, allowing them to oversee the entire network—including workstations, servers and smartphones—from a single point.

Developed based on in-depth consultation with IT professionals, it allows you to manage IT security via a web console from anywhere that has an internet connection. It can be installed on Windows as well as Linux servers, and also comes as a virtual appliance. The built-in task management system helps minimize downtime by responding quickly to incidents.

ESET Remote Administrator uses dynamic threat protection and integrated tools, and comes with new agent-based architecture to streamline network security and minimize administrative overhead.

## Components

---

<b>ESET Remote Administrator Server</b>	ESET Remote Administrator's server component can be installed on Windows as well as Linux servers and also comes as a virtual appliance. It handles communication with agents, and collects and stores application data in the database.
<b>Independent Agent</b>	The agent is a small application that handles the remote management communication and runs independently of the security solution itself. It connects to ESET Remote Administrator and executes tasks, collects logs from ESET applications, interprets and enforces policies, and performs other tasks, e.g. software deployment and general computer monitoring. As the agent executes tasks and interprets server logic locally, it reacts to and eliminates security issues even when the client is not connected to the server.
<b>Web Console</b>	The front-end component of ESET Remote Administrator, the web-console, manages everyday network security. It has a role in interpreting the data stored in the database, visualizing it in the form of clear dashboards and lists with drill-down capabilities, and commands the agents and other ESET applications. In addition, it offers a huge array of customization options to suit the needs of any administrator by providing an easy "look & see" overview of the entire network's security.
<b>ESET Remote Administrator Proxy</b>	The proxy handles collection and aggregation of data from machines in distant locations and forwards it to the centralized ESET Remote Administrator server. Remote locations no longer require ESET Remote Administrator server installation; the proxy alone will suffice. It's possible to install several proxies in large and complex environments and connect them to a central server. The hierarchy and access rights are enforced by the central server, and through its access rights structure.
<b>Rogue Detection Sensor</b>	This component of ESET Remote Administrator is used to discover unprotected and unmanaged machines in the network by listening to their traces. It provides the administrator with improved visibility of all devices located within the corporate network. Discovered machines are immediately located and reported, allowing the admin to move them to a specific static group and proceed with management tasks.
<b>Multi-Platform Support</b>	ESET Remote Administrator runs on both Windows and Linux machines. The general installer deploys ESET Remote Administrator, including server, database and other components, in one step. The admin can also install component-by-component, or deploy as a virtual appliance.

---



FREE U.S.-BASED  
TECHNICAL  
SUPPORT

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

## Usability

---

**ESET License Administrator**

Protects you from attempts by fake websites to acquire sensitive information.

---

**Endpoint Deployment**

ESET Remote Administrator offers several methods of endpoint deployment, making the process smooth and quick. All installers' metadata is stored on the server, so it's easy to utilize different installers for different customers (useful for MSPs) or create groups with specific settings, policies or license credentials.

---

**Multi-tenancy**

A single instance of ESET Remote Administrator can serve multiple independent users with specific access and privileges—while the user cannot see the data of other users. It is also possible to grant three levels of access to each object—read/use/write—as well as granular access settings for different types of tasks. Multi-tenancy is ideal for large enterprises with one centralized server and different admins managing only endpoints in their respective locations, or for MSPs managing multiple customers from a single server but who need to ensure that customers are not able to see the data of other users.

---

**Secure Peer Communication**

ESET Remote Administrator now utilizes the Transport Layer Security (TLS) 1.0 standard and employs its own created and distributed certificates to digitally sign and encrypt communication between the solution's individual components for peer identification. The admin can build a public key infrastructure (PKI) with certificates and certification authority during the installation process, or at a later date. Alternatively, admins can choose to use their own certificates. Certificates are then assigned during the deployment of each ESET Remote Administrator component, resulting in secure communication and a secure network environment.

---

**2FA-protected Login**

To validate the identities of users logging in to ESET Remote Administrator, it's possible to enable two-factor authentication (2FA) directly from the web console. Up to 10 accounts can be 2FA-protected for free. After a simple self-enrollment directly from the web console, the user will receive a link via SMS to download the ESET Secure Authentication mobile app—which is then used to generate random one-time passwords. Once 2FA is set up, one-time passwords are used to complement and strengthen the authentication process.

---

**Integrated ESET SysInspector®**

ESET SysInspector is a diagnostic tool that helps troubleshoot a wide range of system issues and is integrated into the ESET Remote Administrator web console. The admin is able to view all generated SysInspector snapshots directly for a particular client. This allows the admin to track-back security incidents or system changes chronologically.

---

# In-Depth Customization

---

## Dynamic and Static Groups

ESET Remote Administrator uses a client-centric approach, similar to the Active Directory with which ESET Remote Administrator syncs automatically, and adopts its group structure. Clients can be assigned to either static or dynamic groups. The admin sets inclusion criteria for a dynamic group; thereafter, any client that meets these criteria is moved automatically to the respective dynamic group. It is also possible to assign a policy to a dynamic group, with this policy applied to clients upon entry to the respective dynamic group and withdrawn upon exit. This happens without any admin/user interaction.

---

## Policies

The admin can define policies per security product and clearly specify their mutual relationship. Policies are executed on the agent, so even without a connection to the ESET Remote Administrator server the agent is able to apply policies assigned to a specific dynamic group in the event that a client enters that dynamic group. For even easier management, the admin can choose from predefined policy templates for each ESET security product, according to the needs of various clients, e.g. applying specific policy templates for laptops or servers, and restrictive or soft policies.

---

## Triggers

By configuring triggers, the admin is able to define if and when a specific task is executed. Triggers can be paired with dynamic groups and execute the tasks on a client once it enters the group. Scheduled triggers provide the ability to specify task execution according to date, time, day and repeat frequency.

---

## Tasks

Tasks are created in wizard-style steps and clearly sorted for various ESET security products; this also includes pre-configured tasks.

---

## Reports

Admins can choose from pre-defined report templates or create custom ones by using a selected set of data and values. ESET Remote Administrator collects only data which is necessary for generating reports, with the remaining logs stored on the client, resulting in better database performance. Each report template can be viewed in the web console as a dashboard element to provide the administrator with an excellent real-time overview of network security, including drill-down possibilities. Reports can be displayed via web console, exported to a PDF/PS/CSV and saved to a predefined location, or sent as an email notification.

---

## Notifications

It's critical for administrators to get notification of any security issues happening in the network, in order to react immediately. The admin can configure notification options via a wizard-style series of steps, or use any of the predefined notification templates. Templates can be mapped to the specific dynamic group memberships of clients or triggered by specific indications or events as they are recorded in event logs.

---

## IBM QRadar Integration

All major ESET events are exported in LEEF format, which is natively recognized by IBM QRadar. ESET Remote Administrator is shown as a "Log Source" for these events in the IBM QRadar console.

---



[www.eset.com](http://www.eset.com)

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

ESET, the ESET Logo, 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.