

eScan Enterprise 360 (with MDM and Hybrid Network Support)

eScan Enterprise 360 (with MDM and Hybrid Network Support) is a specially designed Anti-Virus and Information Security Solution that provides protection to Windows as well as Macintosh, Linux and Android based devices and endpoints in the corporate network. eScan Enterprise 360 includes Mobile Device Management module which is specifically designed with an aim to facilitate administrator to remotely monitor, secure, and manage all Android-based devices in the network.

eScan Enterprise 360 also includes MailScan, an advanced real-time anti-virus and anti-spam solution for Mail Servers. MailScan safeguards organizations against Virus, Worm, Trojan and many other malware breeds with futuristic and proactive technologies.

Key Features (eScan Server, Windows)



New Secure Web Interface with Summarized Dashboard

The new Secure Web Interface uses SSL technology to encrypt all communications. eScan's summarized dashboard provides administrators the status of the managed endpoints in graphical format such as deployment status, protection status, as well as protection statistics.



Asset Management

eScan's Asset Management module provides the entire hardware configuration and list of software installed on endpoints. This helps administrators to keep track of all the hardware as well as software resources installed on all the endpoints connected to the network.



Role Based Administration

Role based Administration through eScan Management Console enables the administrator to share the configuration and monitoring responsibilities of the organization among several administrators. Using this feature, pre-defined roles can be assigned to the administrators, each with own set of rights, permissions and groups.



Mobile Device Management

eScan facilitates effective Mobile Device Management that allows administrator to create different groups for different location, add devices, move devices from one group to another group, define rules/policies for Anti-Virus, setting Call and SMS Filter, Web Protection, Anti-Theft, Password, and Device Oriented policy. It also allows administrator to create New Task, Start an existing Task, create Group Task, define Task Settings, and Schedule Task at a desired period of time.



Client Live Updater

With the help of eScan's Client Live Updater, events related to eScan and security status of all endpoints are captured and recorded/logged and can be monitored in real-time. Also, the events can be filtered to retrieve exact required information to closely watch security level on all managed endpoint on a real-time basis, thus ensuring total security on all managed endpoints. It also facilitates export of the reports in Excel format that can further be used for audit compliance.



Outbreak Prevention

This allows the administrators to deploy outbreak prevention policies during an outbreak that restricts access to network resources from selected computer groups for a defined period of time. These policies will be enforced on all the selected computers or groups correctly.



Session Activity Report

eScan Management Console monitors and logs the session activity of the managed computers. It will display a report of the endpoint startup/ shutdown/ logon/ log off/ remote session connects/ disconnects. With this report the administrators can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

Other Highlights

- ☑ Unified Console for Windows, Mac, Linux
- ☑ Set Advanced Security Policies
- ☑ License Management
- ☑ Import and Export of Settings
- ☑ Proxy Setting Protection
- ☑ Auto Grouping (New)
- ☑ Message Broadcast (New)
- ☑ File Reputation Services
- ☑ Sophisticated File Blocking and Folder Protection
- ☑ Auto Back-up and Restore of Critical System Files
- ☑ Wizard to create a Windows®-based Rescue Disk to clean Rootkits and File infectors
- ☑ Inbuilt eScan Remote Support
- ☑ Greylisting
- ☑ LDAP and POP3 Authentication
- ☑ Autogenerated Spam Whitelist
- ☑ Comprehensive Attachment and Email Archiving



Active Directory synchronization

With this feature, the administrators can synchronize eScan Centralized Console groups with Active Directory containers. New computers and containers discovered in Active Directory are copied into eScan Centralized Console automatically and the notification of the same can be sent to the system administrators.



Policy Templates

Policy deployment can be made easy through policy templates; this will allow the administrators to create policy templates and deploy it to the desired managed groups.



Print activity

eScan comprises of Print Activity module that efficiently monitors and logs printing tasks done by all the managed endpoints. It also provides a detailed report in PDF, Excel or HTML formats of all printing jobs done by managed endpoints through any printer connected to any computer locally or to the network.



One-Time Password

Using One Time Password option, the administrator can enable

or disable any eScan module on any Windows endpoint for a desired period of time. This helps to assign privileges to certain users without violating a security policy deployed in a network.

Note – Print Activity and One Time Password features are valid for endpoints with Windows Operating system only.

Key Features - eScan Endpoints

Enhanced Endpoint Security

Device Control

eScan's advanced device control feature helps in monitoring USB devices that are connected to Windows or Mac endpoints in the network.

- On Windows endpoints, administrators can allow or block access to USB devices such as Webcams, CD-ROMs, Composite devices, Bluetooth devices, SD Cards or Imaging device.
- On Mac endpoints, administrators can block USB access.

Data Theft Notification

Many times access to the USB port is misused and data pilferage becomes a common occurrence causing potential damage to the organization as intellectual property falls into wrong hands. A sub-feature in eScan's Device Control enables to send notifications to the administrator of the web-console when any data (which is not read-only) on the client system's hard disk is copied to the USB. Device Control, thus ensures that data theft is completely eradicated leaving no scope for misuse of confidential data.

Application Control

eScan's effective Application Control module allows you to block/whitelist and define time restrictions for allowing or blocking execution of applications on Windows endpoints. It helps in accessing only the whitelisted applications, while all other third-party applications are blocked.

Enhanced Two-way Firewall

The two-way Firewall with predefined rule sets will help you in putting up a restriction to incoming and outgoing traffic and hacking. It provides the facility to define the firewall settings as well as define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

Privacy Advisor

eScan comprises of Privacy Advisor that provides you the complete list of application using device permissions in a classified format. This helps you to keep a check on the security level of all applications installed.



Anti-Theft

eScan helps you in blocking, data wiping, SIM watching, and locating your Android-based device through GPS finder. With its Anti-Theft feature, eScan ensures complete protection to your Android from any unauthorized access on the event, if your device is lost or stolen.



Call Filter

eScan Mobile Security for Android facilitates call filtering based on parameters. A user can block calls from specified numbers. Under the Whitelist feature, only whitelisted calls are allowed to the device, while all other calls are blocked. If the numbers are added to the Blacklist, then those numbers are blocked from calling.

Key Features - MailScan for Mail Servers



Web Based Administration Console

MailScan Administration Console can be accessed using a browser. MailScan's operations can be managed from a central location using the web administration tool.



Advanced Anti-Spam and Anti-Phishing

MailScan for Mail Servers uses a combination of technologies like Real-time Black List, SURBL Checking, MX/A DNS Record Verification, Non-Intrusive Learning Patterns and many more to accurately block Spam and phishing emails from entering the corporate network.



Real-Time Virus Scanning at the Mail Gateway

MailScan scans all the email in real-time for Viruses, Worms, and hidden malicious content using powerful, heuristic driven Dual Anti-Virus engines.



Real-Time Content Scanning

All incoming and outgoing messages are scanned in real-time for offensive words and adult content, with the help of Security Policies.



Blocking Image Spam

Spam images that you receive through mails can infect your computer system. MailScan uses powerful in-built technologies to filter out image spam.



Non-Intrusive Learning Pattern (NILP)

With an advanced revolutionary NILP technology, MailScan offers accurate security. It works on the principles of Artificial Intelligence to create an adaptive mechanism in Spam and Phishing Control.

Minimum System Requirements

Windows

(Windows Server and Workstations)

Platforms Supported

Microsoft® Windows® 2019 / 2016 / 2012 R2 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-Bit and 64-Bit Editions)

Hardware for Clients and Server

- CPU - 2GHz Intel™ Core™ Duo processor or equivalent.
- Memory - 4 GB and above
- Disk Space – 8 GB and above

(Windows Endpoints)

- CPU: 1.4 Ghz minimum(2.0 Ghz recommended) Intel Pentium or equivalent
- Memory: 1 GB minimum(1.5GB recommended)
- Disk Space: 800 MB and more

eScan Console can be accessed by using below browsers:

- Internet Explorer 7 / 8 / 9 / 10
- Firefox 14 and above
- Google Chrome latest version

Linux

(Linux Endpoints)

Platforms Supported

RHEL 4 and above (32 and 64 bit)
CentOS 5.10 and above (32 and 64 bit)
SLES 10 SP3 and above (32 and 64 bit)
Debian 4.0 and above (32 and 64 bit)
openSuSe 10.1 and above (32 and 64 bit)
Fedora 5.0 and above (32 and 64 bit)
Ubuntu 6.06 and above (32 and 64 bit)

Hardware Requirements (Endpoints)

- CPU - Intel® Pentium or compatible or equivalent.
- Memory – 1 GB and above
- Disk Space – 1 GB free hard drive space for installation of the application and storage of temporary files

Mac

(Mac Endpoints) Platforms Supported

OS X Snow Leopard (10.6 or later)
OS X Lion (10.7 or later)
OS X Mountain Lion (10.8 or later)
OS X Mavericks (10.9 or later)
OS X Yosemite (10.10 or later)
OS X El Capitan (10.11 or later)
macOS Sierra (10.12 or later)
macOS High Sierra (10.13 or later)
macOS Mojave (10.14 or later)

Hardware Requirements (Endpoints)

- CPU - Intel based Macintosh
- Memory –1 GB and More recommended
- Disk Space – 1 GB and above

Android

(Android Endpoints) Platforms Supported

- Operating System: Android 4.0 and above
- Others: Internet connection

MailScan

CPU Hardware Requirements

- 2GHz Intel™ Core™ Duo processor or equivalent
- 1GHz Intel™ Pentium™ processor

Disk Space: 8 GB & above

Memory: 4 GB & above

*Specific MailScan versions are available for following Mail Servers:

SMTP servers, Microsoft Exchange 2003 / 2007 / 2010 / 2013, Lotus Domino, Mail Servers, CommuniGate Pro, MDAemon, VPOP3, Mailtraq, Mailtraq Lite, DMail/SurgeMail, Postmaster Pro, Postmaster Enterprise, Merak, Avirt, Sharemail, Netnow, SpearMail, VOPMail, CMail, GiftMail, MailMax, IAMS, LAN-Projekt, Winroute, WinProxy, 1st Up Mail Server and Mail Servers.

* Some modules will only be available with specific MailScan Versions. e.g. SMTP is available with MailScan for SMTP and Exchange. Other versions does not have SMTP module.

MailScan is available in English Language only.