eScan Enterprise Edition (with Hybrid Network Support)

With the constantly increasing security threats in the information technology landscape, protection of valuable intellectual property and business data against theft/misuse without interrupting business continuity is a critical issue.

eScan Enterprise Edition (with Hybrid Network Support) also includes MailScan, which is the world's most 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.

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 endpoints on a real-time basis.

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.

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.

Note – Print Activity features are valid for endpoints with Windows Operating system only.

One-Time Password

Using One Time Password option, the administrator can enable or disable any eScan module on any endpoint for a desired period of time. It restricts user access from violating a group security policy deployed in a network.

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

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
- Automatic Uninstallation of other Antivirus Products
- Inbuilt eScan Remote Support
- Greylisting
- LDAP and POP3 Authentication
- Autogenerated Spam Whitelist
- Comprehensive Attachment and Email Archiving

#1 Choice of DIGITAL WORLD

eScan™ Enterprise Security

Key Features-eScan Endpoints

Enhanced Endpoint Security

Device Control

It 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. Unauthorized access to USB devices can be blocked using password protection thus preventing data leakage.

Data Theft Notification

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.

Application Control

It 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 Control

Privacy control allows scheduling the auto erase of your cache, ActiveX, cookies, plugins and history. It also helps you to permanently delete files and folders without the fear of having them retrieved through the use of third-party applications, thus preventing misuse of data.

Advanced Web Protection

eeScan comes with an advanced Web Protection feature that allows administrators to define the list of websites to be blocked or whitelisted on endpoints connected to the network where eScan is installed. For Windows endpoints eScan also provides the facility for time-based access restriction.

Schedule Scan

eScan offers you an option for scheduled scanning, which will run seamlessly in the background without interrupting your current working environment. It performs scheduled scans for selected files/folders or the entire system for the scheduled period, thus providing you the best protection against cyber threats.

Windows OS and App Patch/Update Management

eScan's Patch Management Module auto-updates Windows OS security patch from Cloud or from EMC Console, on PC's those are part of DMZ/Air-Gapped Networks. The module also reports patching availability for Critical Apps like Adobe, Java, etc.

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..

Clustering

Clustering facilitates load balancing by distributing mails to multiple computers for scanning.

Relay Control

This module prohibits spammers from using your organization's IP addresses to send spam.

Customized Disclaimers

This is an easy-to-use option to add customized disclaimers to all external and internal emails.

Extensive Reports

Provides advanced analytical reports in graphical and non-graphical formats.

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 / 11 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-Bit and 64-Bit Editions)

For Server

- CPU - 3.0 GHz Intel™ Core™ Duo processor or equivalent.
- Memory - 4 GB and above
- Disk Space (Free) – 8 GB and above

For Endpoint (Windows)

- CPU - 2.0 GHz recommended Intel Pentium or equivalent
- Memory - 1.0 GB and above
- Disk Space (Free) – 1 GB and above

eScan Console can be accessed by using below browsers:

- Google Chrome & all chromium-based browsers
- Firefox 14 and above
- Internet Explorer 9 and above

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)
Mint 12 and above (32 and 64 bit)

Hardware Requirements (Endpoints)

- CPU - Intel® Pentium or compatible or equivalent.
- Memory – 1 GB and above
- Disk Space – 1GB 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)
macOS Catalina (10.15 or later)

Hardware Requirements (Endpoints)

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

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.