

## eScan Endpoint Security (with MDM and Hybrid Network Support)

eScan Endpoint Security offers cogent method to block access to unauthorized USB devices on managed endpoints with Windows or Mac Operating systems and restrict the execution of unauthorized applications on endpoints with Windows Operating system. It also provides comprehensive Software and Hardware Asset Management for Windows, Mac, Linux or Android endpoints. This helps to tackle your system in an efficient manner by providing total control over Application and Device control on Windows, Mac as well as Android endpoints. It is equipped with advanced Mobile Device Management system that provides highly advanced features to manage Android endpoints accessing corporate network.

**Note:** eScan Endpoint Security client as well as server can be installed on any computer where any other third party anti-virus software is already installed.

## 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.



### Client Live Updater

With the help of eScan's Client Live Updater, events related to eScan and security status of all endpoints are captured logged and monitored on real time as it displays live events of USB and web access captured from managed endpoints. These events can be filtered to retrieve required information. It also allows to export reports in excel format that can further be used for audit compliance.



### 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 setting Call and SMS Filter, Web Protection, Anti-Theft, Password, and Device Oriented policy.



### 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/logoff activity along with remote sessions.



### File Activity Report

eScan Management Console monitors and logs the file activity of the managed computers. It will display a report of the files created, copied, modified, and deleted. Select and filter the report based on any of the details captured. It also allows you to export the generated report in desired file formats such as PDF, Excel, or HTML.



### Print Activity

eScan comprises of Print Activity module that efficiently monitors and logs printing tasks done by all the managed endpoints. It provides you a detailed report in PDF, Excel or HTML formats of all printing jobs done by managed endpoints

**Note – Print Activity and One Time Password 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.



### Software Licensing

This feature provides a list of licenses for Microsoft Operating system and Office License Keys installed on the endpoints.

## 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.

#### 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. On Android by default, all downloaded applications are blocked.



#### Advanced Web Protection

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



#### Anti-Theft

eScan helps you in blocking, data wiping, SIM watching, and locating your Android-based device. 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 and SMS Filter

eScan facilitates content filtering of calls and SMSs based on parameters set through its Whitelist and Blacklist feature. A user can block calls and SMSs from specified numbers based on specific phrases/words/keywords.

## Highlights for Endpoint Security (with MDM and Hybrid Network Support)

- ▣ Secure Unified Console for Windows, Mac, Linux and Android
- ▣ USB Vaccination
- ▣ Centralized Policy and Task deployment
- ▣ License Management
- ▣ Inbuilt eScan Remote Support (Windows) with 24x7 online Support through email, Chat and Forums

eScan Feature	eScan Corporate 360 (with MDM and Hybrid Network Support)	eScan Corporate Edition (with Hybrid Network Support)	eScan Endpoint Security (with MDM and Hybrid Network Support)
Unified Console for Windows/Mac/Linux/Android	✓	✓ (doesn't have console for Android)	✓
Cloud Security Network	✓	✓	X
Set Advanced Security Policies	✓	✓	✓
Personalized Dashboard	✓	✓	✓
Two Way Firewall	✓	✓	✓
Rescue Mode	✓	✓	X
Web Control	✓	✓	✓
Template based Policy	✓	✓	✓
Session Activity Report	✓	✓	✓
Outbreak Prevention and Restoration	✓	✓	✓
USB Blocking with Password Management	✓	✓	✓
Blocking of AutoPlay of USB Devices	✓	✓	✓
Reporting of File Activity	✓	✓	✓
Blocking of CD/DVD	✓	✓	✓
Disabling of Web Cam	✓	✓	✓
Mobile Device Management	✓	X	✓
Managed Backups for managed devices	✓	X	✓
Anti-Theft	✓	X	✓
Call and SMS Filter	✓	X	✓
App Store	✓	X	✓
Application Protection for Mobile Devices	✓	X	✓
Real-Time AV Scanning	✓	✓	X
Anti-Spam (NILP, RBL, SURBL)	✓	✓	X
User Defined File and Folder Protection	✓	✓	X
SNMP Trap Management	✓	✓	✓
Role Based Privilege	✓	✓	X
ADS Integration and Synchronization	✓	✓	✓
Print Management	✓	✓	✓

For more Comparison please visit@ <http://download1.mwti.net/download/wikifiles/comparison/eScan-Corp360-Corp-CS-Endpoint-Security.pdf>

### Minimum System Requirements

#### Windows

(Windows Server and Workstations)  
Platforms Supported

Microsoft® Windows® 2016 / 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)

#### For Server

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

#### For Endpoints (Windows)

- CPU - 1.4 Ghz minimum (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:

- 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 – 512 MB and above
- Disk Space – 500 MB 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)

#### Hardware Requirements (Endpoints)

- CPU - Intel based Macintosh
- Memory – 1 GB and More recommended
- Disk Space – 500 MB and above

#### Android

(Android Endpoints)  
Platforms Supported

- Operating System: Android 3.2 and above
- Others: Internet connection