eScan Total Security Suite for Business

eScan Total Security Suite for Business is a comprehensive Anti-Virus and Information Security Solution that allows you to manage risk and protect your critical infrastructure efficiently. Moreover, the new eScan Management Console (EMC) module includes a Secure Web Interface that facilitates dynamic security management of the server and endpoints. It is an excellent combination of advanced and futuristic technologies that provides protection to your Windows based devices and endpoints in the corporate network.

Advanced Protection against Ransomware Threats

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.

Endpoint Security (Device Control & Application Control)

This module protects your computer or endpoints from data thefts and security threats through USB or FireWire® based portable devices. It comes with an Application control feature, which helps you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that helps you determine which applications and portable devices are allowed or blocked by eScan.

Firewall

This will help you in putting up a restriction to incoming and outgoing traffic and hacking. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

Client Live Updater

With the help of eScan's Client Live Updater, events related to eScan & 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, 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

Outbreak Prevention will allow the administrator to deploy outbreak prevention policies during an outbreak that restricts access to network resources from selected computer groups for a defined period of time. The outbreak prevention policies will be enforced on all the selected endpoints or groups. Incorrect configuration of these policy settings can cause major problems with the computers.

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 administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

Active Directory synchronization

With the help of Active Directory synchronization, the administrator 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 administrator. Administrator can also choose to Auto Install or Protect discovered Windows workstations automatically.

Other Highlights

- Secure eScan Management Console
- Set advanced security policies
- License Management
- Task deployment
- Outbreak Prevention (Improvised)
- Policy Templates (New)
- Policy Criteria (New)
- Update Agent (Improvised)
- Auto Grouping (New)
- Active Directory Synchronization (New)
- Message Broadcast (New)
- Session Activity (New)
- Customize Setup (New)
- Manage updates
- Real-Time Protection against Malware
- Sophisticated File Blocking & Folder Protection
- Powerful Heuristic Scanning for Proactive Protection
- Auto Back-up and Restore of Critical System files
- Wizard to create a Linux-based Rescue UBS to clean Rootkits & File infectors
- Inbuilt eScan Remote Support
- 24x7 FREE Online Technical Support through e-mail, Chat & Forums

#1 Choice of DIGITAL WORLD

eScan™ Enterprise Security

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

Policy Criteria
The administrator can specify policy criteria and deploy it to endpoints automatically if it complies with the pre – defined criteria in the management console. The Administrator will select Policy Criteria based on which the policies will be deployed.

eBackup
eScan allows you to take a backup of your files on a scheduled basis, and is stored in an encrypted and compressed file format. It takes backup of the following extensions - doc, docx, ods, wps, wpd, pdf, xls, xlsx, csv, odp, one, pptx, ppt, ppsx, pps, rels, and many more. The backup will be taken on the drive with the largest free storage available. The backup can also to be taken on network drive which has a pay and use feature.

Auto Grouping
The administrator can define the settings to automatically add clients under desired sub groups. The administrator will have to add groups and also add client criteria under these groups based on host/host name with wild card/IP address/ IP range.

Customized Client Setup
eScan allows you to create customized client setup with pre-defined Policy Template. This allows you to implement group policies to the endpoints automatically where eScan Client is installed on the endpoint manually. It allows you to define the customized settings for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Firewall, Endpoint Security, Privacy Control, Client Installation Settings, Update Intervals, exclude / remove download files. The major benefit of this feature is that even if the endpoint is not connected to the eScan server, the Policy template will be deployed on to the endpoint while customized eScan client is installed on the endpoint.

PBAE
Proactive Behavioral Analysis Engine provides real time protection for organizations and users against Ransomware attacks. It monitors the activity of all processes and blocks the one whose behaviour matches to a Ransomware.

TSPM
Terminal Services Protection Module by eScan not just detects the brute force attempts but also heuristically identifies suspicious IP Addresses / Hosts. It blocks any attempts to access the system.

Data Leak Prevention
eScan empowers enterprises to minimize the risk of data theft with its advanced features like Attachment Control and Device Control. Through Attachment control the admin can block/allow all attachments the user tries to send through specific processes as well as trusted websites that you define.

Update Agent
In a large organization the Administrator can create computer groups for better management and distribution of Policies and Updates. Using eScan they can install Update agent on any managed endpoint (where eScan Client is already installed). This update Agent will take the signature updates and policies from eScan Total Security Server and distribute the same to other managed computers in the group.

The Update agent will alternatively query eScan Update servers on internet for getting updates whenever there is a connectivity problem between the update agent and eScan Total Security Server.

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

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. With this report the administrator can trace the file activities on all the managed computers. Additionally misuse of any official files can be tracked down to the user through the details captured in this report.

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.

Key Features (eScan Endpoints)

File Anti-Virus
This would scan all the existing files and folders for any infection. It will allow you to report/ disinfect/ quarantine/delete objects.

Mail Anti-Virus
This will allow you to analyze all the incoming mails. This analyses the mails by breaking it into three sections the header, subject and the body.

Anti-Spam
This will prevent you from receiving spam mails by checking the content of outgoing and incoming mails, quarantines advertisement mails.

Web Protection
This will allow you to define the sites that you do not want to allow access to. You can define the site names you want to block, do a time based access restriction.

Privacy Control
This will allow you to schedule an auto erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where no traces of deletion could be found.

Minimum System Requirements

(Windows server & workstations) Platforms Supported

- Microsoft® Windows® 2019 / 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 & 64-Bit Editions)

eScan Console can be accessed by using below browsers:

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

Hardware Requirement (Server)

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

Hardware Requirement (Endpoints)

- 1.4 Ghz minimum(2.0 Ghz recommended) Intel Pentium or equivalent
- 1.0 GB minimum (1.5GB recommended)
- Disk Space – 800 MB and more