eScan Endpoint Security

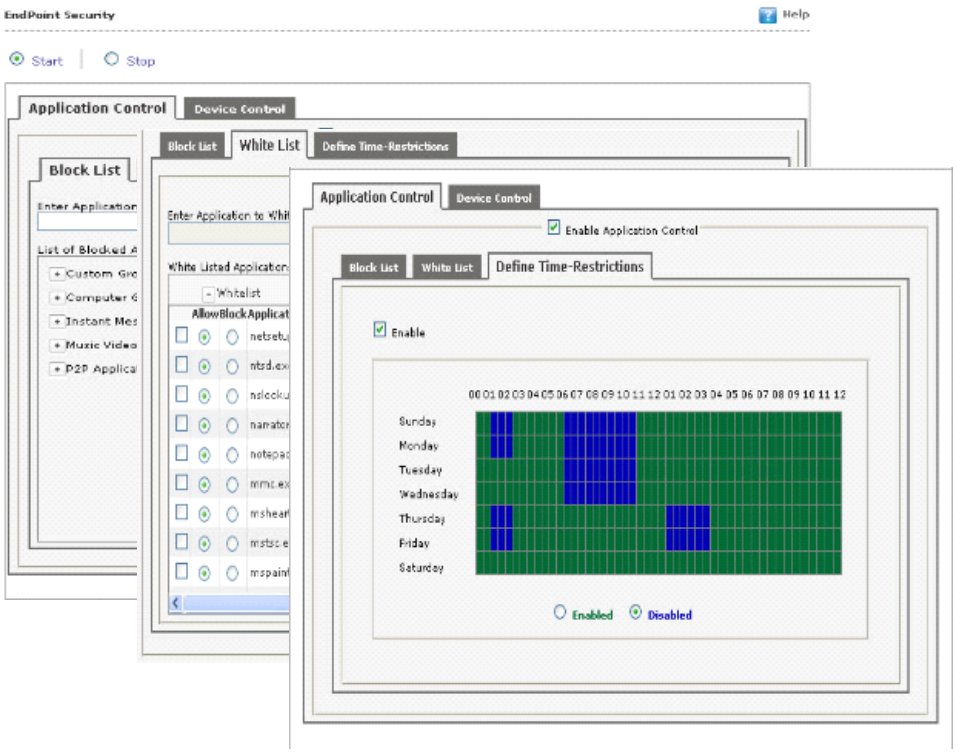
eScan™
Anti-Virus & Content Security

Tired of looking out for the cogent method to block external devices and restrict unauthorized applications? eScan Corporate's Endpoint Security has the apt solution to address your needs.

This robust module features two salient functionalities – Device Control and Application Control, which uses the latest security attributes to block advanced persistent threats from a central management console.

Application Control

Application control is a versatile functionality which allows you to block, whitelist (allow) and define time restrictions for applications. The module contains the list of blocked executables of applications that are pre-defined by MicroWorld. By default, all the applications listed in pre-defined category are blocked. Application(s) can be added that need to be blocked or application(s) can be unblocked as per requirement. The predefined categories include computer game, instant messengers, music video players, and P2P applications. In addition, the pre-defined categories of a group or an application in a group can be allowed or blocked. The whitelisting feature helps in accessing only the whitelisted applications and all other third-party applications are blocked. The Define Time-Restriction feature helps in accessing or blocking applications on the parameters which includes specific days and pre-defined time during specific days. Clubbed together these features enhance the application control functionality which leverages maximum control over the system applications.



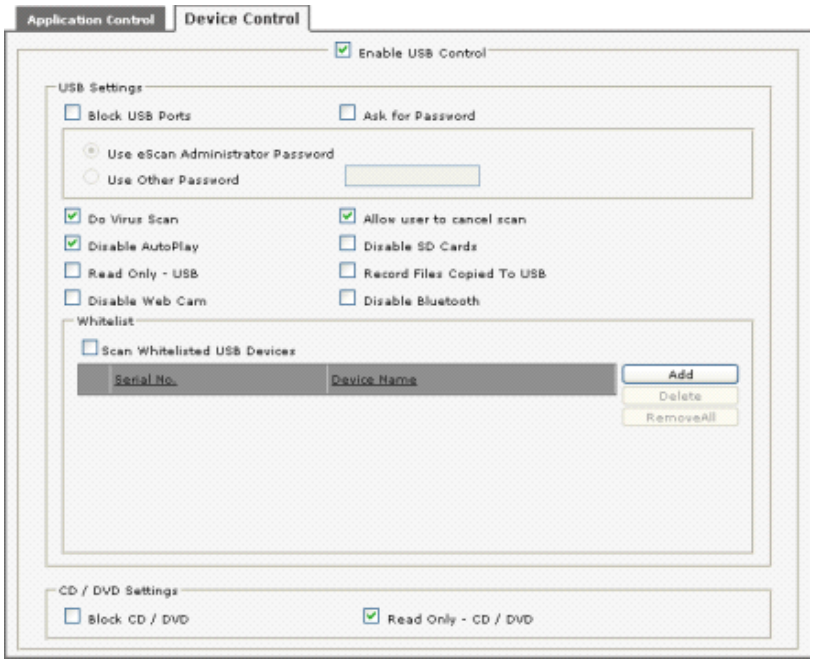
Device Control

Device control is another potent feature that aids in safeguarding the system in a network form unauthorized portable storage devices like USBs, SD cards, Webcams, CDs, and DVDs. It is very vital and crucial that adequate and strong protection methods must be employed to prevent data-theft besides containing and eliminating viruses that surface through external devices.

The device control feature assists you in monitoring devices that are connected to the system in the network. Using the password protect feature USB devices can be blocked and unauthorized USB devices cannot access the system unless a valid password is entered.

Other plus points include blocking, disabling and keeping devices in read-only mode as per requirement apart from disabling auto-play for USBs. A virus scan can be performed on connected devices and as per requirement and USB devices can be whitelisted in order for them to have complete access to the system.

Thus as the name suggests the device control feature is aimed to protect the system from unauthorized external devices.



Scan password protection restricts user access from violating a security policy deployed in a network. For example, the administrator has deployed a security policy to block all USB devices, but someone wants to access it for a genuine reason, for example – making a sales presentation residing on a USB pen drive. How would an administrator give the user an access without violating the current security policy? OTP is the answer for the same by generating one time password for a specified period of time for that specified client system to disable the module without violating existing policy.

Thus the need for Device and Application Control enables to minimize insider risks such as data theft/loss and malware introduction via removable devices apart from regulating applications within the organization.