Kaspersky Enterprise Cybersecurity

KASPERSKY lab

Kaspersky®
Embedded Systems
Security

KESS 2.0 Features

Kaspersky Embedded Systems Security components and features

Real-Time Protection

Kaspersky Embedded Systems Security scans the following objects as they are accessed:

- Files
- Alternative file system threads (NTFS threads)
- The master boot record and boot sectors on local hard and removable drives

On-Demand Scans

Kaspersky Embedded Systems Security runs a single scan of the specified area for viruses and other computer security threats. The application scans files, RAM, and startup objects on a protected computer.

Trusted Zone

You can generate the list of exclusions from scanning activity and from other on-demand and real-time protection tasks applied by Kaspersky Embedded Systems Security.

Process Memory Protection

You can protect the process memory from exploits, using an Agent injected into the process.

Application Launch Control

This component tracks users' attempts to launch applications, and controls application launches.

Device Control

This component controls the registration and usage of mass storage devices and CD/DVD drives, protecting against security threats that may arise while exchanging files with USB-connected flash drives or other types of external device.

USB Connections Monitor

You can configure settings for notifications about different types of device connecting to a protected system via a USB port.

Firewall Management

This component provides the ability to manage the Windows Firewall: configuring settings and operating system firewall rules, and blocking all other attempts to reconfigure firewall settings.

File Integrity Monitor

Kaspersky Embedded Systems Security detects changes in files within the scope specified in the task settings. These changes may indicate a security breach on the protected computer.

Log Inspection

This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.

Databases and Software Modules Update

Kaspersky Embedded Systems Security downloads updates of application databases and modules from a number of FTP or HTTP update server sources including the Kaspersky Security Center Administration Server.

Quarantine

Kaspersky Embedded Systems Security moves potentially infected objects from their original location into Quarantine. For security purposes, objects are stored in Quarantine in encrypted form.

Backup

Kaspersky Embedded Systems Security stores encrypted copies of objects classified as 'Infected' or 'Probably infected' in Backup before disinfecting or deleting them.

Administrator and User Notifications

You can configure the application to notify the administrator and users who access the protected computer about events in Kaspersky Embedded Systems Security operation and the status of anti-virus protection on the computer.

Importing and Exporting Settings

You can export Kaspersky Embedded Systems Security settings to an XML configuration file, and import settings into Kaspersky Embedded Systems Security from the configuration file. You can save all application settings. Or just settings for individual components, to a configuration file.

Applying templates

You can manually configure a node’s security settings in the tree or in a list of the computer’s file resources, and save the configured setting values as a template. This template can then be used to configure the security settings of other nodes in Kaspersky Embedded Systems Security protection and scan tasks.

Managing Access Permissions for Kaspersky Embedded Systems Security functions

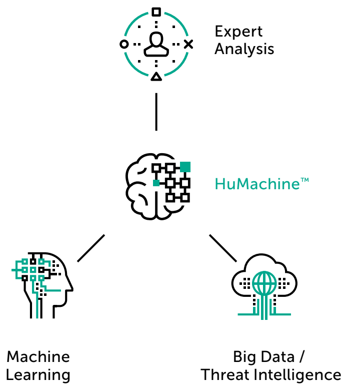
You can configure the rights to manage Kaspersky Embedded Systems Security and the Windows services registered by the application, for individual users or groups of users.

Writing Events to the Application Event Log

Kaspersky Embedded Systems Security logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Embedded Systems Security management, and information required to diagnose errors in Kaspersky Embedded Systems Security.

Integration with External SIEM Systems

You can configure export settings so that applications logs are exported to external event aggregation systems using the syslog protocol.



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com