Overview

# Comodo Endpoint Security Manager

## With Auto-Sandbox Containment Technology

*Comodo's threat containment technology ensures that all viruses and malware are prevented from infecting your computer*

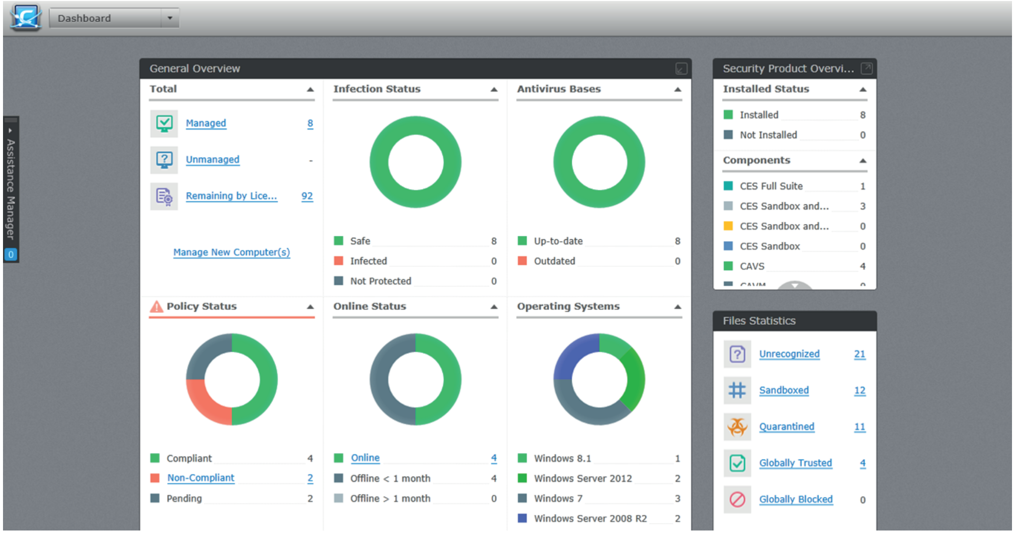
COMODO
Creating Trust Online®

Comodo Endpoint Security Manager (ESM) protects against viruses and malware by focusing on prevention and not solely on detection. Our threat prevention and containment technologies create an impenetrable shield that identifies safe, unsafe and questionable files (aka good, bad and unknown files).

Comodo Endpoint Security Manager provides centralized management of Comodo's 7-layered security suite that proactively protects endpoints and their applications against malware and advanced threats.

## Next-Generation 7-Layer Security for Endpoints

**Containment -** Traditional **endpoint security solutions** depend on blacklist and whitelist detection. Comodo's containment technology disrupts this traditional approach by adding a preventative layer that auto-sandboxes files that have yet to be reported. These unknown but potentially threatening files are contained in a virtual environment within the system, using very little system resource usage, until their behavior can be analyzed.



| Total | |
|---|---|
| Managed | 8 |
| Unmanaged | - |
| Remaining by Lice... | 92 |

| Infection Status | |
|---|---|
| 🟩 Safe | 8 |
| 🟥 Infected | 0 |
| ■ Not Protected | 0 |

| Antivirus Bases | |
|---|---|
| 🟩 Up-to-date | 8 |
| 🟥 Outdated | 0 |

| Policy Status | |
|---|---|
| 🟩 Compliant | 4 |
| 🟥 Non-Compliant | 2 |
| ■ Pending | 2 |

| Online Status | |
|---|---|
| 🟩 Online | 4 |
| ■ Offline < 1 month | 4 |
| ■ Offline > 1 month | 0 |

| Operating Systems | |
|---|---|
| 🟩 Windows 8.1 | 1 |
| 🟩 Windows Server 2012 | 2 |
| ■ Windows 7 | 3 |
| 🟦 Windows Server 2008 R2 | 2 |

| Installed Status | |
|---|---|
| 🟩 Installed | 8 |
| ■ Not Installed | 0 |

| Components | |
|---|---|
| ■ CES Full Suite | 1 |
| ■ CES Sandbox and... | 3 |
| 🟨 CES Sandbox and... | 0 |
| 🟦 CES Sandbox | 0 |
| 🟩 CAVS | 4 |
| ■ CAVM | 0 |

| Files Statistics | |
|---|---|
| Unrecognized | 21 |
| Sandboxed | 12 |
| Quarantined | 11 |
| Globally Trusted | 4 |
| Globally Blocked | 0 |

**Web URL Filtering** - With the powerful rule-configuration interface, you can create rules which are as sweeping or as granular as you require, even on a per-user basis.

**Comodo Firewall** - A highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.

**Comodo Antivirus** - A proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Users can automatically drag-and-drop items onto the home screen to run an instant virus scan.

**File Lookup Services** - A cloud-based file lookup service (FLS) that ascertains the reputation of files on your computer, checking them against Comodo's master whitelist and blacklists.

**Host Intrusion Protection System (HIPS)** - As part of Comodo's multi-layer Defense+ approach, HIPS is a rules-based intrusion prevention system that monitors the activities of all applications and processes on our computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system- memory, registry keys or personal data.

**Viruscope (Behavior Analysis)** - Viruscope monitors the behavior of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. It has the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely giving you more granular control over otherwise legitimate software.

## PRODUCT HIGHLIGHTS

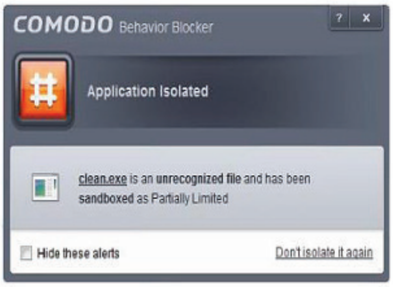
- Unique preventative security layer with Comodo Containment which auto sandboxes zero-day threats and Advanced Persistent Threats (APTs) in a virtual environment within the existing system requiring very little system resource usage.
- Containment technology can be deployed independently alongside existing AV solutions to increase endpoint protection against unknown files until they are behavioral tested.
- Enables centralized management of servers, workstations, laptops and netbook endpoints with built in reporting and detailed endpoint configuration information.
- 7-layer integrated endpoint security suite offering web URL filtering, Comodo firewall and antivirus, file lookup services, host intrusion protection (HIPS), containment with auto-sandboxing and viruscope (behavior analysis).
- Dashboard provides panoramic insight to control all aspects of endpoint protection and management.
- Manages endpoint processes, services, installed applications, resource usage, removable devices and power usage.
- Hierarchical deployment of CESM servers allows local or remote management of nonLAN endpoints.
- Administrative reports for more insight about antivirus database updates and scans.
- Immediate Microsoft Windows 10 support and functionality.
- Offers the industry's only $5,000 virus-free warranty against infection.

Comodo Endpoint Security (CES) offers real-time protection against all malware threats. Other antivirus products depend on signature updates alone but Comodo’s auto sandbox containment technology protects you from unknown threats. Thus enabling Comodo to be the only vendor to provide a $5,000* virus-free warranty against repair costs, should an endpoint in your enterprise become infected with a virus or malware and we are unable to restore you to working condition.

## The Future of Endpoint Administration

Comodo ESM not only provides unrivalled protection against zero-day threats, it also grants administrators total visibility and control over  the software, hardware and services of every machine. Comodo ESM is fully integrated with the Comodo Endpoint Security suite and provides centralized administration of antivirus and system health status.

Comodo's ESM dashboard enables administrators to see every important metric immediately. Utilizing a unique patent-pending panoramic display, the web-based administration console presents each endpoint as a tile containing 14 critical metrics facilitating rapid alerting and remediation of issues requiring a minimum of administrative effort.



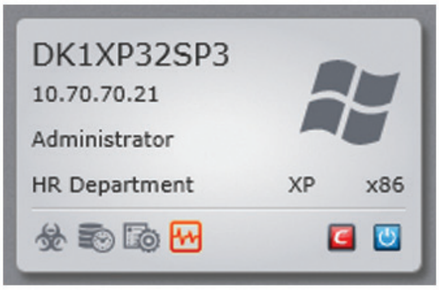
COMODO Behavior Blocker

Application Isolated

clean.exe is an unrecognized file and has been sandboxed as Partially Limited

□ Hide these alerts

Don't isolate it again

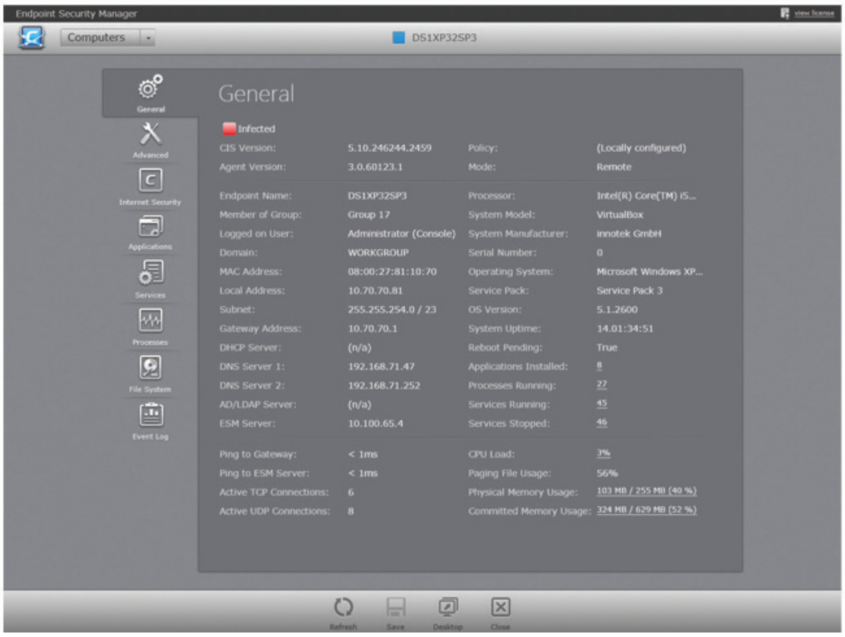


DK1XP32SP3

10.70.70.21

Administrator

HR Department XP x86



DS1XP32SP3

General

Infected

| | | | |
|---|---|---|---|
| CIS Version: | 5.10.246244.2459 | Policy: | (Locally configured) |
| Agent Version: | 3.0.60123.1 | Mode: | Remote |
| Endpoint Name: | DS1XP32SP3 | Processor: | Intel(R) Core(TM) i5... |
| Member of Group: | Group 17 | System Model: | VirtualBox |
| Logged on User: | Administrator (Console) | System Manufacturer: | innotek GmbH |
| Domain: | WORKGROUP | Serial Number: | 0 |
| MAC Address: | 08:00:27:81:10:70 | Operating System: | Microsoft Windows XP... |
| Local Address: | 10.70.70.81 | Service Pack: | Service Pack 3 |
| Subnet: | 255.255.254.0 / 23 | OS Version: | 5.1.2600 |
| Gateway Address: | 10.70.70.1 | System Uptime: | 14.01:34:51 |
| DHCP Server: | (n/a) | Reboot Pending: | True |
| DNS Server 1: | 192.168.71.47 | Applications Installed: | 8 |
| DNS Server 2: | 192.168.71.252 | Processes Running: | 27 |
| AD/LDAP Server: | (n/a) | Services Running: | 45 |
| ESM Server: | 10.100.65.4 | Services Stopped: | 46 |
| Ping to Gateway: | < 1ms | CPU Load: | 3% |
| Ping to ESM Server: | < 1ms | Paging File Usage: | 56% |
| Active TCP Connections: | 6 | Physical Memory Usage: | 103 MB / 255 MB (40 %) |
| Active UDP Connections: | 8 | Committed Memory Usage: | 324 MB / 629 MB (52 %) |

- Infection status
- Definition database status
- Security policy compliance
- System health status
- User assistance requests
- Security suite status
- Online status

The computer properties screen provides granular information about each endpoint, including OS version, service pack,  installed applications, whether a reboot is required, networking statistics and CPU, RAM and hard-drive usage metrics. With just one click, the administrator is able to view and stop services and processes as well as browse and uninstall MSI-based applications.

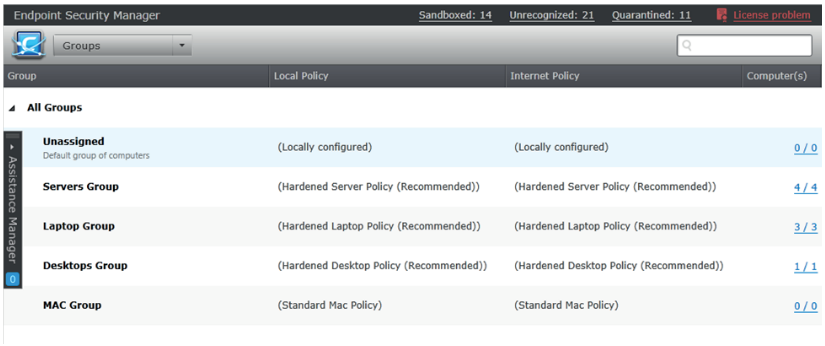
Armed with this information, the administrator can make swift and accurate decisions to protect the infrastructure and ensure the smooth and efficient continuation of users’ computing requirements.

Proactive administration is available through the configuration of policies or templates that dictate the endpoint’s behavior. Controlling everything from the definition database update schedule and source, granular manipulation of critical security configurations, and file and vendor whitelisting to removable device control and power management, the user-friendly policy creation wizard can generate and enforce the administrator’s configurations within minutes.

## More Efficient, Effective and Easier Management

The intuitive profiles and configurations save administrators thousands of man hours per year. For easy onboarding process, administrators can set up default profiles for all, or by groups, to roll out and centrally manage security policies.

Administrator time that would otherwise be lost to repetitive configuration and vendor interoperability problems can be re-directed towards more productive and profitable core business interests. Furthermore, because CESM policies can be deployed immediately across all protected nodes, administrators can respond more quickly to protect an entire network against the latest, zero-day threats and CESM's intuitive interface provides fingertip access to task wizards, important network and task related data, and support resources.



Endpoint Security Manager Sandboxed: 14 Unrecognized: 21 Quarantined: 11 License problem

| Group | Local Policy | Internet Policy | Computer(s) |
|---|---|---|---|
| All Groups | | | |
| Unassigned<br>Default group of computers | (Locally configured) | (Locally configured) | 0 / 0 |
| Servers Group | (Hardened Server Policy (Recommended)) | (Hardened Server Policy (Recommended)) | 4 / 4 |
| Laptop Group | (Hardened Laptop Policy (Recommended)) | (Hardened Laptop Policy (Recommended)) | 3 / 3 |
| Desktops Group | (Hardened Desktop Policy (Recommended)) | (Hardened Desktop Policy (Recommended)) | 1 / 1 |
| MAC Group | (Standard Mac Policy) | (Standard Mac Policy) | 0 / 0 |

## A Total Solution for both SMBs and the Enterprise

- **More Control, Less Worry:** Comodo's unique containment technology auto-sandboxes unknown malware onsite in a virtual environment with little resource usage required.
- **Manage with Ease:** Centrally manage your servers, workstations, laptops, netbooks and their applications.
- **Engage in Best Practices:** Our 7-layered security platform ensures each endpoint is protected with a combination of web URL filtering, firewall, antivirus, file lookup service, HIPs, containment with auto-sandboxing and viruscope (behavior analysis).
- **Gain Insights:** A robust dashboard presents a panoramic  view of 14 critical endpoint metrics.
- **Save Time:** View and modify endpoint processes, services and installed applications with powerful system management capabilities.
- **Simplify Administration:** Use 'push' deployment via Active Directory®, Workgroup and IP addresses; and "pull" deployment via group policy or login script.
- **Interact Remotely:** Interact directly with users and remote desktop endpoints with our remote assistance feature.
- **Lower Response Time:** Real-time notifications lower emergency response time to emerging threats.
- **Deepen Understanding:** Location-aware policies allow granular definition of security configurations for endpoints inside and outside of the VPN.
- **Go Green:** Wake-on-LAN enabled systems advance enables integrated power management functionality.
- **Keep System Requirements Low:** Minimal system requirements allow installation on non-dedicated Windows PCs and servers.

### About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online® . With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit  www.enterprise.comodo.com

* Comodo's Protection Plan is included with Comodo Endpoint Security and is available for one (1) year from the date of your software registration and installation. Please see Comodo Endpoint Security Manager End User Subscriber Agreement (http://www.comodo.com/repository/eula/EULA-CESM-v2013.pdf) for complete details. Comodo Endpoint Security trials exclude Comodo Protection Plan.

** System only