

Sophos Enterprise Console

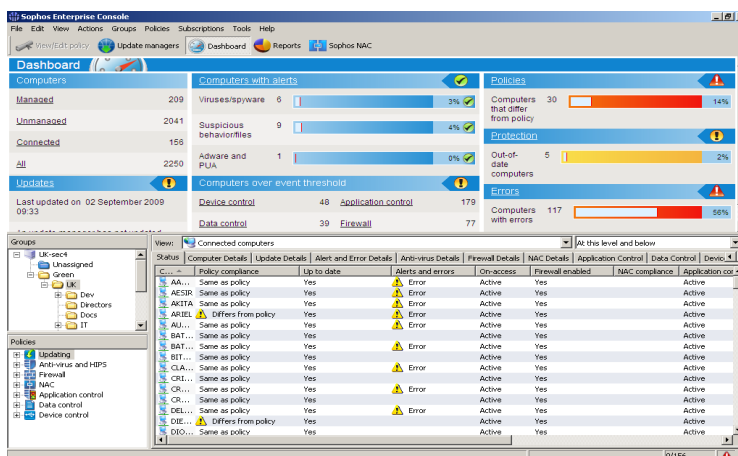
Sophos Enterprise Console™ is part of Sophos Endpoint Security and Data Protection. It automates the policy-based management and enforcement of Sophos Anti-Virus, and Sophos Client Firewall and Sophos NAC. The single console with its security dashboard and automatic email alerts simplifies the deployment and updating of anti-malware, firewalls, host intrusion prevention, device and data control, application control, and endpoint assessment and control as well as allowing centralized cleanup of malware.

One simplified, automated console reduces complexity

- Sophos Anti-Virus and Sophos Client Firewall can be installed and updated across Windows, Mac OS X, Linux and UNIX computers — including remote computers.
- Sophos NAC can be installed and managed on Windows computers, providing fundamental endpoint assessment and control.
- The Sophos Security Dashboard provides an at-a-glance view of security status across all the computers on the network. Outbreak risks are constantly monitored and automatic email alerts are sent when your chosen security thresholds are threatened.
- The flexibility of different computer discovery methods— including network find, IP/Subnet and Microsoft Active Directory— ensures that protection can be rapidly deployed.
- Synchronization with Active Directory ensures that when new computers join your network, they are automatically protected and your chosen security policy is automatically enforced.
- Administrators can create management roles and sub-estates to share the workload without handing over full administration capabilities. Three default roles (administrator, help desk and report only) enable responsibility for specific actions like cleanup or management areas of the network, such as remote offices, to be delegated to trusted users.
- Security policies can be quickly created and enforced using Sophos ActivePolicies™ in Enterprise Console. A single policy can be created once and applied across multiple groups, and across Windows, Mac, Linux and UNIX computers.

Key benefits

- » Provides scalable management across tens of thousands of Windows, Mac OS X, Linux and UNIX computers.
- » Reduces administrator workload with its ability to share specific tasks with other teams through role-based administration
- » Enables a wide range of customizable, graphical computer and user-based reports to be created, scheduled to run and automatically emailed
- » Monitors security status providing an at-a-glance view of all alerts and policy compliance across all the computers on the network
- » Enables the easy discovery of all computers on the network and centrally deploys across the network from a single console
- » Synchronizes with Microsoft Active Directory to automatically protect new computers as they join the network
- » Monitors and controls suspicious files and behavior, providing a complete host intrusion prevention system (HIPS)
- » Controls the movement of sensitive and confidential data off the network to prevent data loss
- » Controls removable storage devices and the installation and use of legitimate software applications such as VoIP, P2P, IM and games
- » Quickly creates and enforces security policies across multiple groups, using Sophos ActivePolicies
- » Enables centralized cleanup of malware and potentially unwanted applications
- » Provides role-based administration privileges assigned with help desk and read-only consoles
- » Allows management of networked computers without end-user knowledge or involvement
- » Generates graphical reports on virus alerts, infections and protection status



Scalable, centralized control of more than just anti-virus

- Enterprise Console simplifies the management of anti-virus, anti-spyware, anti- adware, client firewall, host intrusion prevention, data and device control, application control, and endpoint assessment and control.
- Data control functionality provides integrated DLP that monitors all the common ways users can move data off the network: removable storage devices, CD/DVD/floppy drives and internet-enabled applications such as web browsers, email clients and instant messaging. Supported by an extensive library of global data definitions right out of the box, data control policies can be easily configured, deployed and monitored across your network.
- Legitimate software applications such as VoIP, P2P, IM, media players and games can be blocked or authorized for different groups of computers using ActivePolicies in Sophos Enterprise Console. For example, VoIP could be switched off for office-based desktop computers, yet authorized for remote computers.
- Device Control blocks or allows removable storage including USB sticks, music players, external hard disks, CD/DVD drives and wireless connection technologies: Wi-Fi, Bluetooth and Infrared (IrDA). Policies based upon groups can be created centrally and device block events are reported instantly via the Enterprise Console dashboard.
- Runtime analysis, buffer overflow and unique pre-execution protection provide a complete host intrusion prevention system without the need for complex installation and configuration. This proactive detection of malware, suspicious files and suspicious behavior is monitored and controlled from Enterprise Console.
- Sophos Enterprise Console allows the assessment and control agent and policies to be deployed and managed across all Windows computers.
- MSDE or SQL Server database integration provides a choice of simplicity and scalability to suit all sizes of enterprise networks.

Automated, powerful management

- Centralized disinfection and cleanup of malware across the network is performed in a single, simple operation from the console.
- Security, management and policy compliance information is delivered through the Enterprise Console security dashboard and customizable, integrated graphical reports. The computer and user-based reports can be scheduled to run at specific times and be automatically emailed.
- Rapid threat analysis from SophosLabs™ and the fastest updates in the industry are downloaded as frequently as every 10 minutes.

Industry-leading expertise 24x7

- Our 24x7 customer support operation is highly acclaimed, while SophosLabs, our global network of threat analysis centers, provides a rapid response to emerging and evolving threats.

Languages available

- English, French, German, Japanese, Italian, Spanish, Simplified Chinese and Traditional Chinese

System requirements

Platforms managed

- » **Windows**
7/2008/Vista/2003/XP/2000/98/95/NT4
- » **Mac OS X**
Versions 10.4/10.5/10.6
- » **Linux***
- » **UNIX***

Management server

- » **Windows**
Server 2008/Server 2003/2000 Server
- » **VMware**
ESX 3.0, 3.5/Workstation 5.0/Server 1.0

Remote console

- » **Windows**
2003/2000 Pro or Server/XP Pro
- » **VMware**
ESX 3.0, 3.5/Workstation 5.0/Server 1.0

Hardware

- » Minimum: Pentium III 450 MHz or equivalent

Disk space

- » Minimum: 2.0 GHz Pentium or equivalent

Memory

- » Minimum: 512 MB

* For full details, visit www.sophos.com.

