



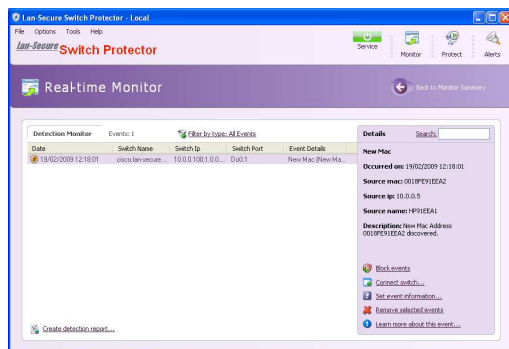
If you want your network protected and secured You need Switch Protector to help you keep it that way

Switch Protector software is a built-in engine of Switch Center management software that implements Network Access Control (NAC) using IEEE-802.1X features on managed network switch ports and helps to protect networks from potential intruders, unauthorized network connections and malicious network activities from within your organization.

Switch Protector combines a variety of access protection rules for intrusion detection and prevention. The powerful protection engine can monitor the standard Switch Center database and external SNMP linkup traps from managed network switches and alerts or block network entities that doesn't comply with the selected protection rules.

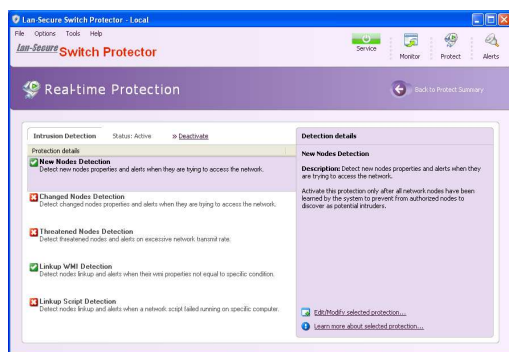
Real-time detection

Switch Protector provides variety of detection rules that can protect against any network nodes that connected to the organization network including MAC addresses, IP addresses, Port location changes and any policy organization enforcement rules.



Real-time prevention

Switch Protector provides real-time prevention using standard or user-define SNMP protocol as well as user-define scripts like Telnet or SSH. The prevention options can be combined with blocked nodes notification messages and specific schedule inactivity operation times.



Real-time policy enforcement

Switch Protector can enforce organization policy rules using any windows WMI query or external script. The policy enforcement capability is checked upon end users network card linkup and interacts with their operating system for specific services, programs, processes or any anti-virus check that can be included with the policy rules. The end users reply is checked upon the enforcement rules and their workstation can be prevented from accessing the network if not comply with the organization policy.

Real-time management control

Switch Protector can be controlled using the software built-in administration interface, intranet organization web or remote email activation requests for managing network access control of specific authorized switch ports or end-users workstation detection and prevention control.

Key features

- Real-time monitoring scanner supporting built-in Switch Center database discovery and external SNMP traps.
- Real-time prevention supporting standard SNMP commands and external remote scripts like Telnet and SSH.
- Real-time detection rules supporting MAC address discovery with built-in spoofing control mechanism.
- Real-time policy enforcement detection rules supporting WMI and external remote scripts.
- Real-time management administration using software built-in interface, intranet web or email activation requests.
- Real-time daily and weekly reports including HTTP and SQL export capabilities.
- Real-time state and threshold alerts.
 - Email alerts forwarding.
 - SNMP traps alerts forwarding.
 - SYSLOG alerts forwarding.

System requirements

- A 800 MHz or faster processor with at least 256 MB of RAM
- Microsoft Windows 2000, Windows XP, 2003 Server™ or Windows Vista™
- At least 10 MB of available free space on your hard disk