



Secure Your Network Endpoints From Intrusion and Theft

With the influx of portable storage devices and removable media, data theft is becoming an increasing threat to organizations. Devices such as USBs, Wi-Fi, FireWire, Bluetooth, iPods, MP3s connect seamlessly to company networks, without IT administrators having any knowledge that their corporate data is being exposed. Portable devices also provide an easy entryway for infecting systems with viruses or malicious software.

SHADOW Device Patrol acts as your corporate watchdog securing company devices to minimize unauthorized access to proprietary information. New devices connected to your computers are automatically recognized and tracked by the software and can be easily managed based on administrators policies.

Discover the benefits of SHADOW^{DP} Device Patrol

- ✓ **Centralize security** with our unique policy manager that can create rules for individuals, groups or corporate wide
- ✓ **Schedule** specific protection policies based on time of day allowing administrators the flexibility of full access after hours
- ✓ **Protect** your intellectual property by establishing rules for access to external devices such as iPods, Bluetooth, CD/DVD, memory sticks and external hard drives
- ✓ **Offsite security** features control devices such as notebooks not currently connected to the corporate network.
- ✓ **Power management** feature allows for scheduled and remote shutdown and restart of devices



RSI

www.telecost.com

40 King St. W, Suite 300. Oshawa, Ontario. L1H 1A4
Phone: 905 576-4575 Fax: 905 576-4705 Email: rsi@telecost.com

Prevent data theft

Unauthorized access or transfer of data through USB, CDs, iPods, MP3s, FireWire, WiFi, Bluetooth on all company systems, can be managed centrally through the SHADOW Device Patrol web console.

Centralized Security Management

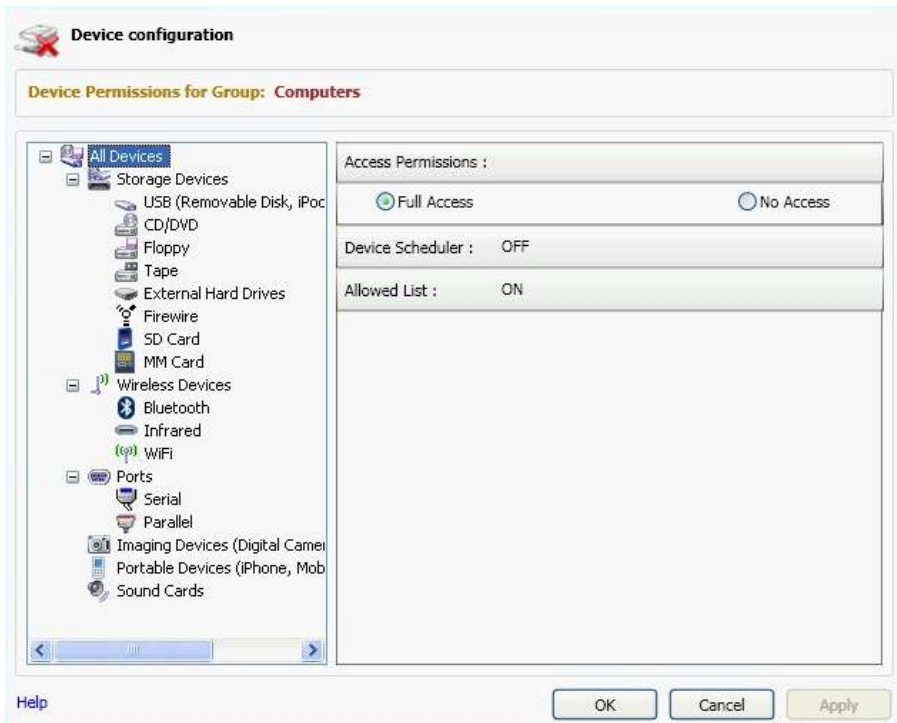
The web based SHADOW^{DP} console provides remote flexibility in accessing the console from any location to authorized administrators.

Device Access Permissions

Security levels can be established for all devices including full access, read only or no access.

Off Site Device Management

When a laptop or computer is offsite, SHADOW^{DP} can still manage the security of endpoint devices.



Guard Your Network Endpoints

Storage Devices

USB, Firewire
CD/DVD, Floppy, Tape
External Hard Drive

Communication Ports

Serial, Parallel

Wireless Devices

Bluetooth, Infrared, Wi-Fi

Other

Digital camera, webcam
iPhone, Mobiles
Sound Cards

Allowed List

SHADOW^{DP} can restrict access to all endpoint devices or specific allowed devices. This feature can minimize potential intrusions by allowing access to approved employee devices on their authorized computers such as USBs, FireWire, External Hard Drives.

Scheduler

Device access privileges can be configured for specific times. For examples, the IT team can be scheduled to have access to CD/DVDs for software installation during after hours, when daytime users are away.

Power Management

Remotely shutdown, restart and boot computers on a network. These features can also be scheduled to run automatically at designated times through the Scheduler.

Remote Install

SHADOW^{DP} clients can be deployed from the server to all the computers on the network. The setup file for the client can be integrated into Active Directory's software deployment. There is no need to visit each remote computer to install the software.



SHADOW Device Patrol Console

RSI

www.telecost.com

40 King St. W, Suite 300. Oshawa, Ontario. L1H 1A4
Phone: 905 576-4575 Fax: 905 576-4705 Email: rsi@telecost.com