

- ✓ Protect access to endpoint devices including USB's, Bluetooth and iPods
- ✓ Create allowed list of company approved USB's and external hard drives
- ✓ Conserve the power usage of workstations
- ✓ Schedule access privileges at specific times of the day

With an increasing popularity of portable storage devices, theft of proprietary data is becoming a growing security challenge in today's computing environments. Portable devices also provide an easy entryway for infecting systems with viruses, spyware, Trojans and other damaging malware, thus compromising an organization's network.

AccessPatrol, provides a proactive solution for securing company endpoints (USBs, CD/DVDs, Bluetooth, WiFi, FireWire, iPods, MP3s) to prevent illicit transfer of data to unauthorized devices.

✓ **Manage data leakage and system infection**

AccessPatrol manages endpoint device access both on and off the network. Unauthorized access or transfer of data through USB flash drives, CDs, iPods, MP3s, FireWire, WiFi, Bluetooth on all company systems, can be managed centrally through AccessPatrol's web console.

✓ **Centralized Security Management**

From a centralized web console, endpoint security can be applied to all device entry points across the company. The web based console, provides additional flexibility in accessing the AccessPatrol console from any location to authorized administrators only.

✓ **Security Levels**

Security levels to devices include full access, read only or no access. With a few simple clicks, endpoint security can be readily implemented through the centralized console. The web based console, provides the additional benefit of being able to access the console from any location.

✓ **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.

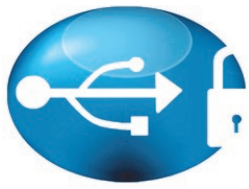
✓ **Offsite Device Management**

When a laptop or computer is offsite, AccessPatrol can still manage the security of endpoint devices. If access to blocked devices is legitimately required, then AccessPatrol can be easily configured to grant permissions.

✓ **Allowed List**

While AccessPatrol can restrict access to all endpoint devices, the Allowed List feature restricts access to only company authorized devices of USBs, FireWire and External Hard Drives.

This minimizes leakage of sensitive data or infection of systems through unapproved or personal employee devices.



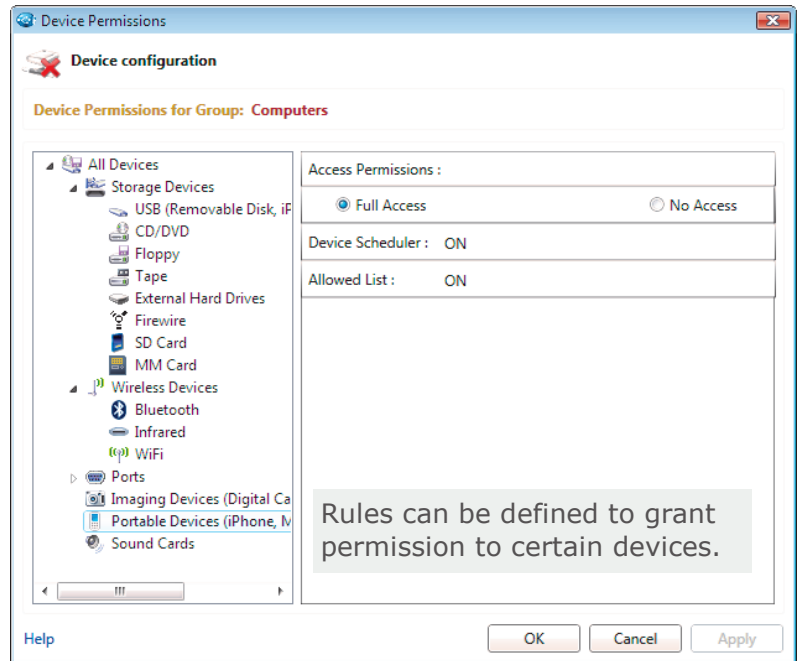
Supported Operating Systems

AccessPatrol Server/Console:

Windows 2000/2003/2008, XP, Vista and Windows 7

AccessPatrol Client:

Windows 2000/2003/2008, XP, Vista and Windows 7



"It works a treat! Simple solution, I managed to install and use within 15 minutes. We needed a simple solution to lock/unlock USB on user PCs but it also has some other features we will use too."

- www.softpicks.net

What's New

Web Based Console

Through the new Web based AccessPatrol console, device management can be accomplished through any location. Administrators can easily configure and manage the AccessPatrol policies remotely. With a few simple clicks, endpoint security can be readily implemented through the centralized console.

Additional Device Support

AccessPatrol now supports the blocking/unblocking of iPhones and SD/MM Card slots.

For more details, please visit
www.currentware.com