

Sentinel Products Ltd

DeviceShield

Product Information Guide

June 2008

Table of Contents

DEVICESHIELD PRODUCT INFORMATION GUIDE	3
INTRODUCTION.....	3
KEY ISSUES.....	3
SOLUTION SUMMARY	3
<i>Functional Summary</i>	4
<i>Control</i>	4
<i>Management</i>	4
<i>Visibility</i>	4
SOLUTION COMPONENTS	5
<i>Setup Wizard</i>	5
<i>Dashboard</i>	5
<i>Email Updates</i>	5
<i>Policies</i>	6
<i>Network Discovery & Deployment</i>	6
<i>Reporting</i>	7
DEVICESHIELD FEATURES SUMMARY	8
SYSTEM REQUIREMENTS	9

DeviceShield Product Information Guide

DeviceShield safeguards your network by monitoring real-time traffic and applying customised, highly-granular security policies over all physical and wireless storage devices.

- Minimise exposure of risk from Viruses and Malware
- Freedom to use USB technology without fear of undermining your existing security
- Allows you to control, audit and track portable device use
- Show details of what files are being transferred to removable devices and shared between pupils
- Enables students to be able to utilise USB and other portable media devices for legitimate coursework
- Prevents the incentive to download music and games
- Report and control the use of MP3 players so the school can identify how much time is spent playing music and control as required
- Secures sensitive data leaving the network unprotected with automatic 256 AES encryption
- Solid security gives complete peace of mind

Introduction

Increasingly within your school network there is a proliferation of easily accessible computer ports, while at the same time more and more devices are designed to connect to them instantaneously and seamlessly. But as the ways to connect to a laptop or desktop have exploded – WiFi, Bluetooth, and others, on top of traditional USB, FireWire, or serial ports – the ways to see and control what is connected have not kept pace.

Key Issues

- Potential virus outbreak
- Distribution of offensive and illegal material
- Installation of unlicensed applications
- Misuse of resources, playing games, downloading /uploading music files
- Launching applications from specially formatted USB flash drives

Solution Summary

DeviceShield provides a comprehensive solution which enables schools to see what ports and devices are being used (visibility), and to define a policy that controls their usage (control). DeviceShield controls every endpoint and every device, over every network or interface. It monitors real-time traffic and applies customised, highly granular security policies over all physical and wireless storage devices.

Functional Summary

In response to these challenges the main functions of DeviceShield can be summarised as below:

	Function	
Control		
Policies	Define exactly what access each user or group has in respect to Removable Media Devices, Ports and File Types	✓
Hierarchies	Assign different policies to different users or groups	✓
Desktop	Users receive notification of any violation to DeviceShield policies	✓
Encryption	Option to encrypt selected files for selected users and groups	✓
Management		
Active Directory	Import your network computers directly from Active Directory	✓
User Accounts	Import users and groups directly from Active Directory	✓
Set and forget	Assign your policies to users and groups and DeviceShield will actively manage and police your network	✓
Management Console	Management Console shows the current state of all clients on your network	✓
Client Deploy	Deploy via Active directory Group Policies or from within the management console	✓
Wizard Set Up	Step-by-step configuration walk through	✓
Visibility		
Real time view	Dashboard graphs and charts provide an up to date at a glance view of network activity including the busiest users, devices in use and top files used.	✓
Email Updates	Automatically receive updates on activity at user defined intervals to your mailbox	✓
Reports	Produce network-wide summary and detail x`reports and graphs detailing usage over time and export them into Excel and PDF formats	✓

Solution Components

Setup Wizard

The Setup Wizard is displayed on entry to DeviceShield™ to help guide you through the initial setup and configuration. Through the Setup Wizard you can:

- Discover the PCs on your Network that are to be controlled
- Define the Policies that are to be applied to your networked PCs
- Deploy the DeviceShield™ client to your PCs



Dashboard

The DeviceShield Dashboard provides you with an at a glance summary view of usage. In "Recent Records" you will find a detailed view of each transaction made, whether someone was copying a file to or from a USB device. The display includes: time of day in which the action was taken, the type of action taken, the username of person(s) logged in on the client machine, the computer name of the client, and the device involved. The "Most Active Users" window displays a list the most active users by username. Here you will be able to take a look at the estimated number of transactions by member considered most active. In viewing "Most Used Devices", you will see a number by each device type. This number represents the number of access attempts to the device made by a user on the client machine. The "Top File Types Used" displays a basic graph showing a list of file type accessed. The list is displayed in order from most used to least used.



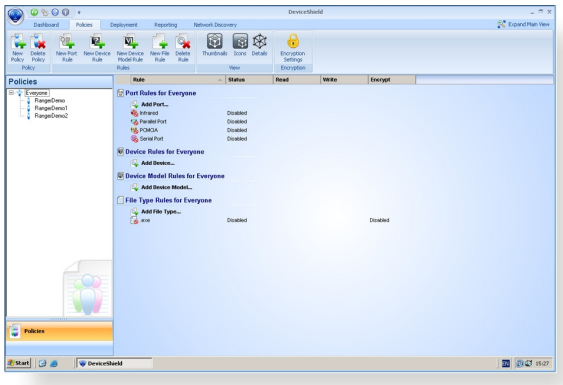
Email Updates



DeviceShield Automatic Email Updates enable set and forget reporting. Configuring your "Dashboard Email Settings" will allow you to receive a generated report via email. Simply select the frequency, enter your email address, and type in your hosting information.

Policies

A **Policy** comprises of a collection of Rules and is associated with either a Windows Group or a Windows User. **Policies** define exactly what access is afforded to the specified Group or User in respect of Removable Media Devices.



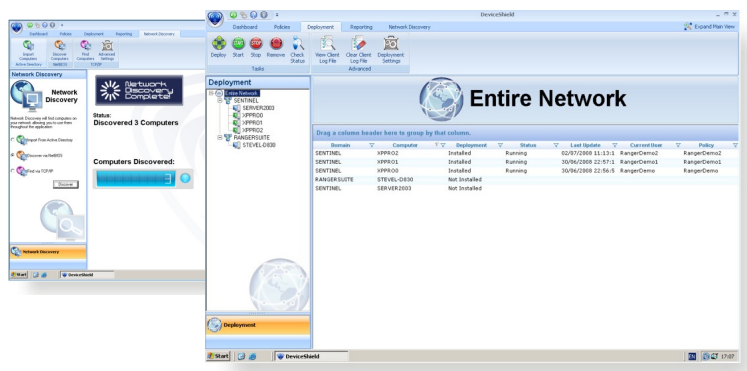
- Import users and groups direct from Active Directory
- Create rules for access to “Ports” (Serial, Infrared, Bluetooth, Wireless, Serial, Parallel, Firewire, PCMCIA)
- Allow Read Only, Write or Encrypted
- Create Rules for “Devices” (iPod, iPhone, USB Storage, USB Peripherals, Windows CE, PalmOS, Blackberry, DVD/CD, Floppy, Modem, Tape, Scanner/Camera)
- Allow or Restrict by File Type
- File restrictions by file header not name
- Tailor specific policies for different users and groups, helping to protect your network, students, staff and data.

Network Discovery & Deployment

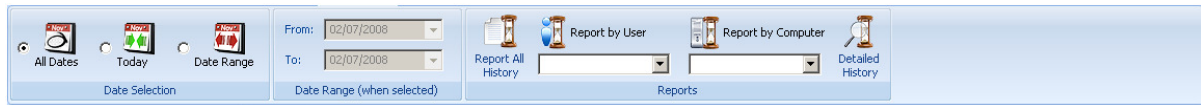
DeviceShield will automatically import all of your domains and computers using one of the following methods: -

- Active Directory
- TCP/IP
- NetBios

Following “Network Discovery” you can deploy the small client service to each workstation that you wish to manage with DeviceShield. You can deploy via the management console or create an MSI to deploy via Active Directory GPO



Reporting



DeviceShield enables summary and detail reports to be quickly and easily generated and disseminated in a choice of user friendly formats such as Excel and PDF.

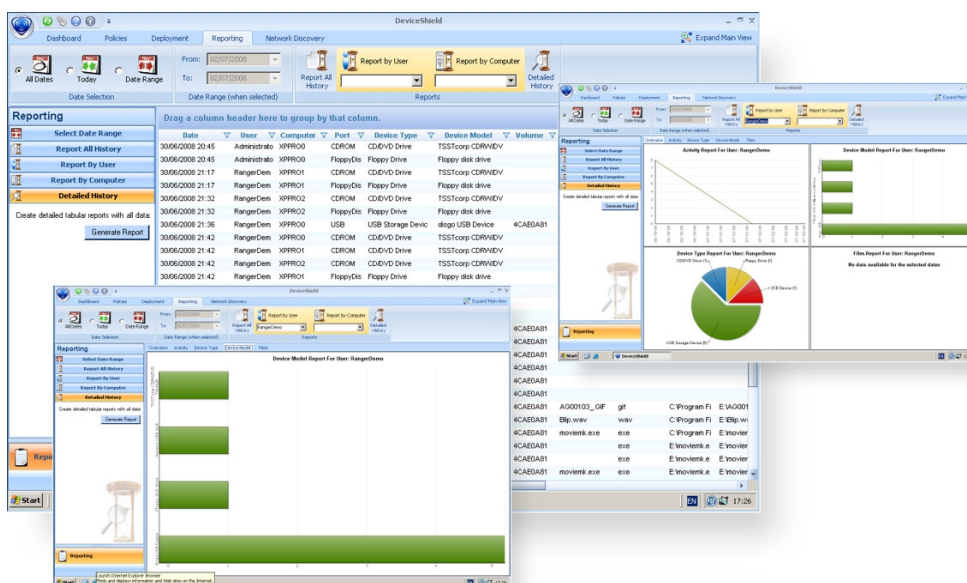
Built-in reports are designed to accommodate the security and operational needs of the establishment and its ICT personnel. The information is provided in a clear, easy to understand format for the benefit of non-technical viewers. Summary reports allow easy detection of specific students that frequently disregard acceptable use policies, while the administrative detail reports assist in the deployment, policy distribution and overall visibility of endpoint activity within the school.

The DeviceShield interface allows a step-by-step drill down into different aspects of the report, and enables a quick and intuitive transition from a high-level view to specific detailed information.

The reports can either be viewed from within the DeviceShield Management Console or be exported to popular formats for viewing and analysis outside of the Management Console.

The following reports can be generated and further customised by selecting a pre-defined or bespoke date range:

- Detailed Report - Generates a grid-view style report with detailed information.
- Report all History - Generates graphical reports based on all traffic for all users.
- Report by User - Displays list by the username specified
- Report by Computer - Displays list by the computer name specified



DeviceShield Features Summary

Key Features	
Dashboard Visibility – Find out who’s connecting what devices to your network	✓
Port & Device Control – Control who uses what when and how	✓
Granular - multiple policies for every level in your school: School wide, Domain wide, Groups and individual users.	✓
Allow/ block - all USB, FireWire, PCMCIA, Bluetooth, WiFi , Infrared, Serial & Parallel Ports	✓
Simple and powerful reporting with export to Excel and PDF	✓
Device Control - iPod, iPhone, USB Storage, USB Peripherals, Windows CE Devices, Palm OS Devices, Blackberry Devices, DVD/CD Devices, Floppy Drive Modem, Tape, Scanner/Camera, Printers	✓
Centrally managed & seamlessly integrates with Active Directory	✓
Encryption - Transparently encrypts data copied to removable media devices	✓
File header based classification - Not by extension (Tamper resistant)	✓
Policies - Flexible White/Black List and Read/Write control	✓
Intuitive Management Console	✓
Automatically Email latest file and audit information	✓
Client Suspension –Temporarily suspend client without uninstalling	✓
Wizards – guides you through the deployment process	✓
Specific device model and volume control	✓
Offline – works even when not connected to the network	✓
File Type control	✓
Windows Vista Support	✓
Deployed from Central Management Console	✓
Policies working on and off the network	✓
Minimal interaction with the end-user...user does not know it is installed	✓

System Requirements

Software	DeviceShield
Server	1GHz CPU or greater
Server Operating system	Windows 2000, XP, 2003
Server RAM	512 MB RAM or higher
Disk Space	75 MB for program installation 150 MB hard drive space for system database
Database	MSDE, SQL Server Express, SQL Server 2000 or higher
Client OS	Windows Vista Windows XP Windows 2000 Windows 2003

If you have any queries regarding system pre-requisites, please contact your Ranger reseller or visit the Ranger web site: www.rangersuite.com