

Safeguard against internal data loss

Portable storage mediums are used everywhere. Employees, students, even your grandmother can now plug these devices into a PC, access your network, and introduce potentially harmful viruses into your environment or remove confidential information from your network. Do you know what proprietary information is being taken away on these removable media devices?

Numara[®] FootPrints[®] Device Manager Benefits

- Establish and enforce data protection with minimal effort
- Restrict and control access to data
- Detailed data collection and reporting to comply with audit standards
- Covers upload/download activity for multiple devices

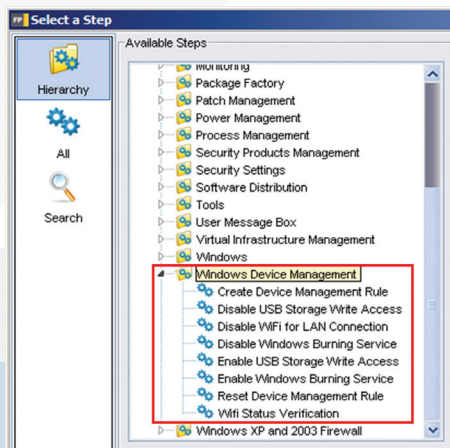
Most organizations use firewalls and anti-virus software to prevent against external threats. However, many are just now realizing that the need to protect against internal threats is just as critical. The loss of sensitive information and intellectual property can be detrimental to your business and can quickly become very expensive due to data recovery, downtime, loss of business, legal liability and a potentially damaged reputation.

Numara FootPrints Device Manager helps safeguard your organization against these consequences, protecting your business by minimizing the risks associated with unauthorized use of prohibited devices and storage media. Footprints Device Manager allows you to define policies that specify which devices are explicitly enabled or disabled and reduces the risk of non-compliance and the manual effort of managing or resolving issues caused by malicious use of unsanctioned devices. Usage policies, also known as "operational rules", allow you to determine which devices will be targeted with a given policy based on any combination of individual devices or established groups. As a result, Footprints Device Manager enables you to establish and enforce data protection with minimal effort.

Stay compliant

Footprints Device Manager centrally controls uploading and downloading activity from Bluetooth[®] devices, CD/DVD drives, FireWire devices, floppy drives, modems, wireless and USB devices. As part of the Numara Security & Compliance Suite, you will have an interface to control and log all peripheral device events. If data leakage is suspected, you can easily audit the unwanted activity, review the available event logs and adjust your policy accordingly.

Preventing data leakage is a primary concern for IT from a compliance perspective. Many organizations have not included the threat of removable media devices in their overall data protection plan, but with the focus on risks related to data leakage becoming increasingly important, one thing is clear – you must protect your sensitive and confidential data or pay the price for security breaches.



There are several options for Windows[®] Device management available and the ability to create customized rules to fit your organizational requirements.

This focus has driven many industries to develop regulations that mandate the safeguards of personal or financial information housed in their systems. Some of the more well-known include:

- Payment Card Industry Data Security Standard (PCI DSS) — applies to any organization gathering, storing or processing credit cardholder information
- Gramm-Leach-Bliley Act (GLB) — applies to any financial organization
- Health Insurance Portability and Accountability Act (HIPAA) — applies to any healthcare provider or insurer
- Sarbanes-Oxley Act (SOX) — applies to any publicly traded organization, public accounting firm or auditing organization

With FootPrints Device Manager, many of the issues related to the most widely adopted industry regulations are easily managed. Coupled with strong organizational security policies and user awareness, Numara Software can help you mitigate risk and quickly provide auditors with the information they require to demonstrate compliance.

Features

- **Device coverage** – centrally control uploading and downloading activity from Bluetooth devices, CD/DVD drives, FireWire devices, modems, wireless and USB devices
- **Group policy alternative** – manage and apply policies that control uploading/downloading activity on devices without the complexities often present when using group policy
- **Event log management** – understand which policy has been breached by collecting and reporting on individual machines or groups of machines' event logs
- **Operational rules** – determine which devices will be targeted with a given policy based on any combination of individual devices or established groups
- **Report now** – demonstrate results with executive dashboards and comprehensive reporting

The freedom to simply...choose

FootPrints Device Manager is part of a fully integrated line of IT Operations Management solutions. The FootPrints family is a modular solution designed to simplify a diverse set of complex service management, asset management, and PC Lifecycle needs.

Imagine...having the choice to:

- Decide which components or products are relevant to your business
- Manage various platforms from one console
- Invest in one point product, a solution set of multiple products, or the entire suite
- Buy what you need and not what the vendor dictates

For more information on the minimum requirements necessary to use FootPrints Device Manager, please refer to our Technical Specifications document available online

FootPrints family

- FP Incident&ProblemManager
- FP ChangeManager
- FP ConfigurationManager
- FP ServiceCatalogManager
- FP InventoryManager
- FP RemoteManager
- FP DeploymentManager
- FP PatchManager
- FP DeviceManager**
- FP VulnerabilityManager
- FP ComplianceManager
- FP PowerManager
- FP MigrationManager

Who are we?

Founded in 1991, Numara® Software is a leading global provider of integrated IT Operations Management solutions. Numara's family of integrated products solve Endpoint Lifecycle Management, Mobile Device Management, Help Desk and Service Desk challenges for physical, virtual and mobile devices, simplifying and optimizing IT Operations Management.



freedom
to simply **choose**
the right solution for you