

Command Center for Removable Drive Security

Highlighted Features

- ◇ Automatic device enrollment, user identify & password management for USB devices
- ◇ Dynamically revoke access to lost or stolen drives
- ◇ Configure and enforce policies for out of network & offline device use
- ◇ Administrative audit trail of USB device contents & chain-of-custody tracking of USB devices
- ◇ Integration with Microsoft Windows single sign-on to allow automatic USB drive access when logged in to corporate network domain
- ◇ Create and enforce strong password policies and periodic password resets

Technical Specifications

Removable Media

- ◇ Any NTFS formatted drive
- ◇ Any FAT, FAT32, ExFAT formatted flash drives or memory cards.
- ◇ UDF formatted CDs & DVDs
- ◇ ISO formatted CDs & DVDs

Operating System

- ◇ Microsoft® Windows 2000, XP Home, XP Professional, Vista (All Versions)
- ◇ Server 2000, Server 2003, Server 2008

System Requirements

- ◇ Pentium or AMD (800 MHZ or higher)
- ◇ 256MB Memory
- ◇ JAVA Runtime Environment (JRE) 6 or higher on the PC or Server.



COMMAND CENTER FOR DATA AND DRIVES

DeviceDefender Administrative Server is a web-based software application that tracks information or devices that have been encrypted by SecurFlash® or DeviceDefender products.

When users are creating or accessing encrypted removable drives and media, user activities and actions are tracked by the DeviceDefender Administrative Server.

Administrators can configure organizational security policies through the Administrative Server such as strong passwords, offline or out-of-network access to encrypted drives and data, and remote password recovery requirements.

COMPREHENSIVE ADMINISTRATIVE CONTROL AND POLICY ENFORCEMENT FOR REMOVABLE DRIVES AND MEDIA

AUDIT AND TRACK DATA AND DRIVES

The Administrative Server retains an audit trail of what files are encrypted and stored on the user hard drive, removable drive or media protected by SecurFlash or DeviceDefender.

The audit trail contains meta-data about the contents of the drives and media, from what PCs or servers the files came from, the users that are accessing these devices and files, on which PCs and servers, and the type of user operations being performed with the files (e.g. open, copy, delete, modify, etc.).

POLICY MANAGEMENT

Controls for Administrators, Security and Compliance Officers

Password creation and enforcement – Configure minimum password lengths and password character usage requirements, as well as require users to automatically change passwords at regular intervals.

Master key access – Configure master keys for administrative access to the encrypted contents of drives — optimal during employee investigations or when re-issuing previously used drives to new users.

Re-authorization interval – Specify how often users need to be online with the protected device or media. Online connection communicates the audit trail to the Administrative Server and any pending user or device revocation commands are enforced automatically.

Automatic drive authorization and encryption – When used in conjunction with DeviceDefender software, administrators can configure policies related to which type of devices can be used in the organization, if unprotected devices are allowed and if automatic encryption should be enforced for USB devices.

ADDED CONTROL AND SIMPLICITY

Revoke access to lost drives and data – Revoke access to encrypted data through a remote command for lost or stolen drives, CDs or emails.

Domain authentication/Single sign-on – Username and password are not required to access protected devices, data and email when the user is logged onto the corporate network. When the user is disconnected from the corporate network, username and password must be entered.

GSA and DAR BPS Schedule Approved **GS-35F-0307N**