Removable Storage Management Module

Authorize and encrypt removable storage devices to safeguard your data security

Module Description

Removable Storage Management module aims to help corporations manage the usage of various removable storage devices (e.g., USB flash drive, USB hard disk and MP3 Player) to prevent data leakage and protect system security.

Features

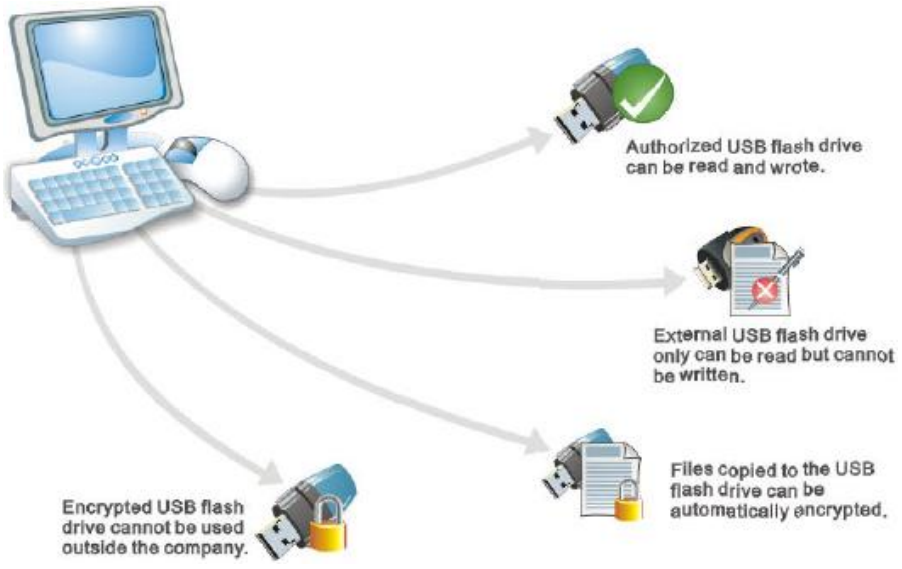
- Disk-based removable storage authorization
- File-based disk and removable storage encryption
- Only authorized agent computers can access the encrypted removable storage device
- Allow system administrator to register the approved list of removable device and only registered device can be used with access control

Removable Storage Management Challenge

Nowadays, removable storage devices are widely used in enterprises. The popularization of removable storage devices brings convenience but also brings great challenges for management. Information may leak out via these devices accidentally or purposely and managers may suffer a huge loss. In addition, virus and malware may intrude the internal network of enterprise and threaten system security when these devices are plugged in. To sum up, the risk of information leakage is increasing and how to protect the usage security of removable storage becomes a vital question.

IP-guard Solution

The Removable Storage Management module of IP-guard not only can help you well manages all removable storage devices, but also can grant different permissions to various computers. By setting flexible and diverse policies, you can block all removable storage devices foreign to your company and only allow the use of authorized removable storage devices within your company. Moreover, authorized removable storage devices cannot be used outside your company, and consequently, your information is secure and away from leakage.

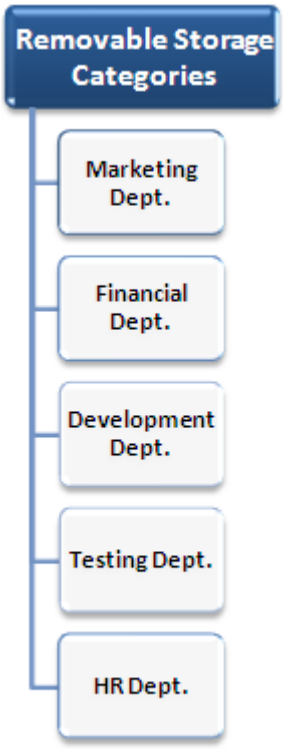


IP-guard can control the usage of removable storage devices by authorization control and enforce information security through data encryption.

Removable Storage Control

Removable Storage Management module can control the usage rights of all removable storage devices as so to manage the usage of removable storage device and protect information security.

- Block users from using unauthorized removable storage devices
- Encrypt files when they are copied to removable storage devices
- Decrypt encrypted files only by authorized users
- Encrypt removable storage devices to make sure they are only used within the company



Category Management

Category Management

System administrator can manage all removable storage devices and divide them into different customized categories to facilitate removable storage management.

Removable Storage Operation Log

Removable Storage Operation Logs records plug-in and remove actions. Detailed contents include Type, Time, Computer, User, Disk Type, Volume ID, Description and Volume Label.

Removable Storage Operation Logs

Type	Time	Computer	User	Disk Type	Volumn ID	Description
Remove	2009-01-21 11:34:15	RD-JACKY	Jacky	Encrypt disk	D48D-F141	SigmaTel MSCN
Plug In	2009-01-21 11:32:10	RD-JACKY	Jacky	Encrypt disk	D48D-F141	SigmaTel MSCN
Remove	2009-01-21 11:13:02	MKT-TOMMY	Tommy	Encrypt disk	4976-873D	SanDisk U3 Cruzer Mic
Plug In	2009-01-21 10:36:06	MKT-TOMMY	Tommy	Encrypt disk	4976-873D	SanDisk U3 Cruzer Mic
Plug In	2009-01-21 09:18:42	MKT-TOMMY	Tommy		BC9E-959D	SanDisk U3 Cruzer Mic
Remove	2009-01-20 19:02:06	MKT-TOMMY	Tommy	Encrypt disk	4976-8050	SanDisk U3 Cruzer Mic

More Suggestions

Two modules of IP-guard, Device Management and Document Management, are recommended. For details, please refer to information relating to these modules.

Available Modules for Your Selection

- Application Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- IT Asset Management
- Network Management
- Print Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Website Management