IP-guard™

IT Management System

IP-guard is powerful and comprehensive IT management software for enterprise.
It can help you

- protect your information security maximumly
- regulate your staff's working behavior
- manage your IT assets and maintain your system centrally

With IP-guard, everything is in your control.
IP-guard absolutely is your excellent helper in IT management.

Protect Information Security

IP-guard provides you with matchless secure experience.

Secure means everything is transparent and be controlled. IP-guard empowers you the powerful ability to control everything so as to enhance your information security. IP-guard can

- cover and control all aspects (e.g., document operation, email, instant messaging, device usage) which might have information leakage likelihood to reduce the risks of information leakage by authorizing specific operation.
- provide encryption and backup features to safeguard your information security.
- record every operation in detail to facilitate all your operation.

Regulate Work Behavior

IP-guard helps you to improve work efficiency.

High efficiency comes from effective and strong management. IP-guard enables you to carry out flexible and efficient control and management so as to standardize your staff's work behavior and improve work efficiency. IP-guard can

- block employees from speculating in the stock market, playing PC and online games, accessing illegal websites, etc. With IP-guard, you can allow and limit your employees' specific operation in specific time range.
- limit the bandwidth of Peer-to-Peer (P2P) applications even block it and stop illegal as well as unwanted ports. Therefore, bandwidth can be reasonably allocated and network security can be enhanced.
- offer detailed operation log and visual figure of statistic analysis report to help you quickly and easily master the use status of IT resource and your staff's working status.

Manage and Maintain IT System

IP-guard assists you with centralized asset management and system maintenance to reduce IT management cost.

Nowadays, the key point of system management is how to ensure the high usability and long stability of IT system with lowest cost so as to sustain the smooth development of key business. IP-guard can

- manage all assets comprehensively and master the information of all IT assets and asset changes within the whole network.
- support software deployment and patch management.
- support remote maintenance and remote control to help you quickly find out and fix the problem.

Application Management

Control and monitor the usage of application to improve work efficiency

Module Description

Application Management module aims to control and monitor software usage. With appropriate policy setting, improper applications can be blocked easily and the detailed logs help administrators understand user behavior about application usage.

Features

- Easily block improper applications
- Detailed application usage log
- Complete analysis report about application usage
- Real-time alerts on unauthorized access

Application Management Challenge

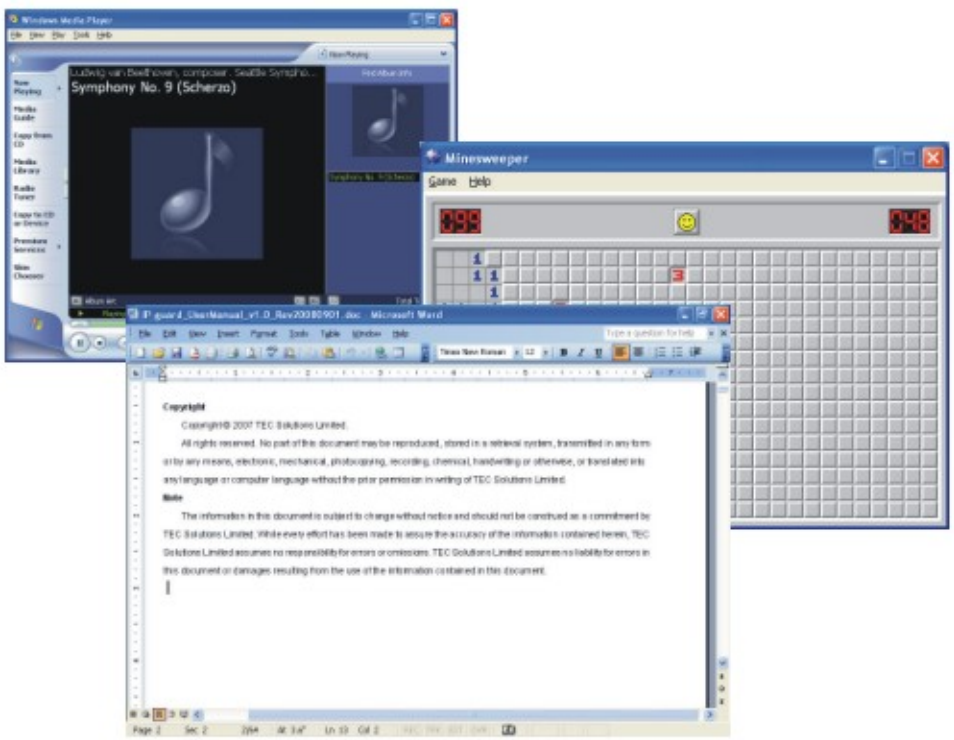
Managers may concern about whether

- illegal software is being used within the company
- software usage is appropriate

Improper use or management of application may not only affect staff's productivity, the usage of resources, but also involve a violation of company regulation as well as the law.

IP-guard Solution

The Application Management module aims to control and monitor application usage. It provides system administrators with detailed logs, application statistics and complete analysis reports which can assist them in understanding user behavior. Moreover, it is useful for management purpose. For example, its statistics will serve as a reference for answering issues like what applications should be controlled in order to increase work efficiency.



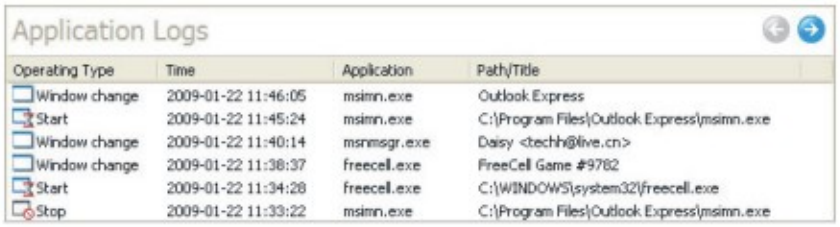
IP-guard helps you manage the usage of various applications such as Minesweeper, Windows Media Player and Microsoft Word.

Application Control

Many enterprises prohibit their staff from using their own software such as BT, chatting and online gaming software. Application control can help to prohibit or limit the use of unwanted applications.

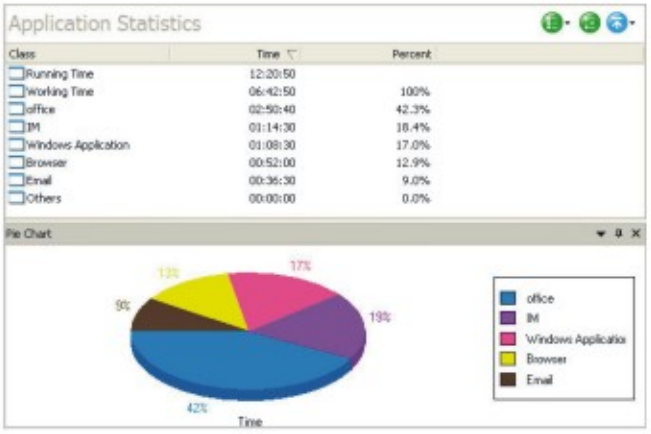
Application Logs

The contents of Application Logs include operating type, time, computer, user, application name, and corresponding path/title.



Application Statistics

Application Statistics provides powerful statistical function which focuses on the daily operations of computer and application usage so as to provide detailed records and complete analysis reports for managers to assess employees' work behavior.



Gather application statistics by application category

Gather application statistics by department

More Suggestions

Combining with Web Management function, IP-guard can effectively regulate employees' work behavior. For details, please refer to Web Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Asset Management

Manage IT assets to reduce the cost of management

Module Description

Asset Management module aims to manage hardware and software inventory; windows patch update and installation; and software deployment.

Features

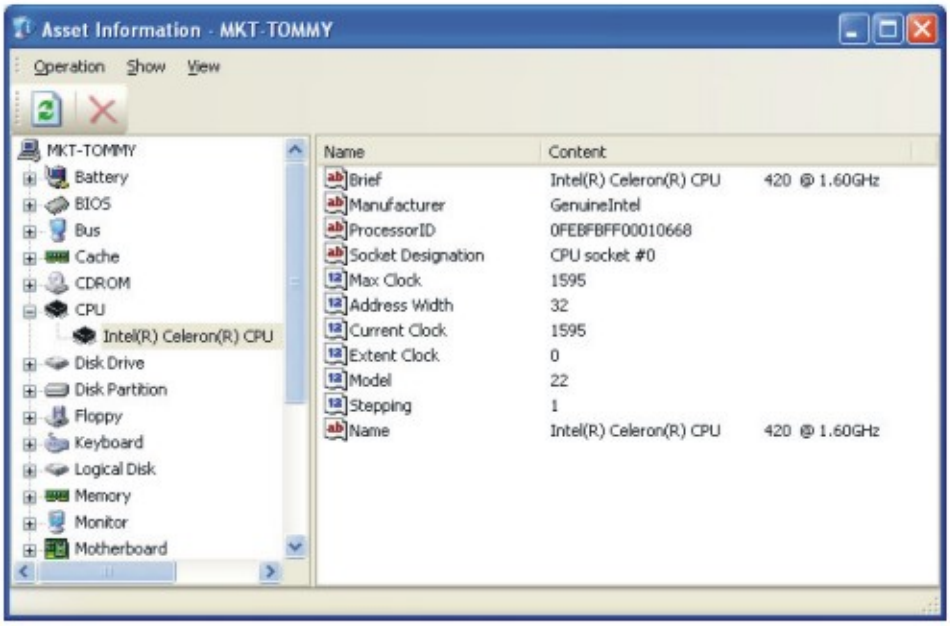
- Complete hardware and software inventory
- Detailed log on hardware and software change
- Add customized asset
- Update windows patches consistently
- Speed up mass software deployment or upgrade
- Generate reports for further analysis and data mining

Asset Management Challenge

As hardware and software constitute an increasing portion of the IT budget, corporations are making great efforts on finding ways to reduce costs on both hardware and software management. IT directors are frustrated by the need to audit and maintain a massive number of computers every day. How many computers are installed with Windows XP or Vista? Do we need to buy more licenses? Can we have an asset inventory database to store all IT assets? How to keep the Windows patches consistently updating? No doubt that all IT directors and support staff face one or more of these questions everyday. The Asset Management module of IP-guard helps to solve these questions in an efficient manner.

IP-guard Solution

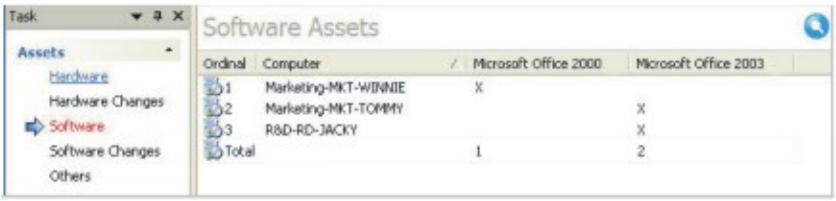
The Asset Management module aims to manage hardware and software inventory; windows patch update and installation; and software deployment. By using the powerful search engine, administrator can easily query how many computers are installed with specific hardware or software. Then, the patch management function helps to make sure all computers are installed with consistent windows patches so as to avoid virus and Trojan horse intrusion. Finally, the software deployment function helps system administrator to save much more time especially in mass deployment of software installation or upgrade.



Detailed software and hardware information can be checked on IP-guard console.

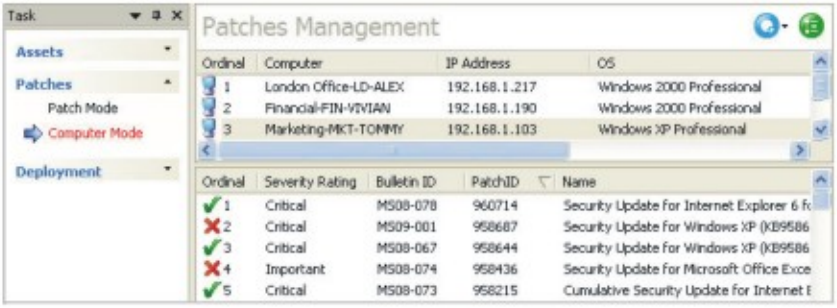
Asset Management

- Record software and hardware asset information of every workstation in detail
- Record changes in hardware/software assets
- Manage software license



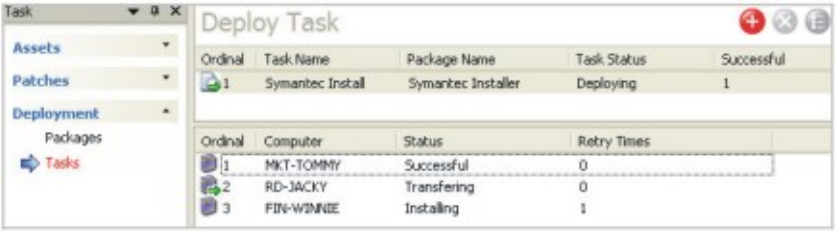
Patch Management

- Provide patch scanning report
- Download, distribute and install patches automatically



Software Deployment

- Deploy and install software automatically
- Distribute documents to designated agent computers
- Support breakpoint transmission
- Support background installation



More Suggestions

The saving of time and costs on maintaining the highly diverse and widely distributed IT infrastructure has become an absolute necessity for organizations, whether big or small. IP-guard System Management Solution provides IT managers with tools to gather software and hardware asset information automatically and maintain enterprise IT assets with convenience.

The comprehensive capabilities of IP-guard System Management Solution include Asset Management and Remote Maintenance.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Bandwidth Management

Limit and allocate bandwidth reasonably to avoid network drain

Module Description

Bandwidth Management module aims to limit and control bandwidth usage. With appropriate control at specified times, directions, network address and ports, bandwidth can be allocated to each computer specifically. The detailed traffic statistics help administrators trace abnormal activities. Real-time alerts are given in case any abnormal traffic is detected.

Features

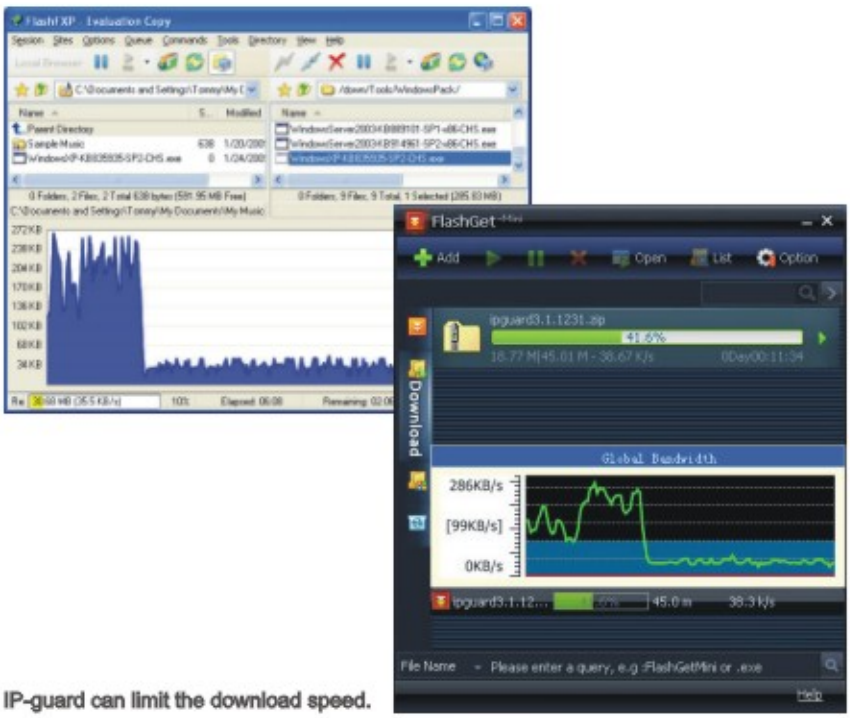
- Easy to adopt policy to control the bandwidth of every computer
- Real-time alerts are sent to administrator if any abnormal traffic is detected
- Detailed traffic statistics and complete analysis report

Bandwidth Management Challenge

Nowadays, many enterprises set up high-speed internet services in order to facilitate the whole workflow among different departments and business parties. But network drain, leading to a decrease in workflow efficiency, may be caused by improper uses of network resources, such as way of using Peer-to-Peer and FTP download. How to limit and allocate the bandwidth to prevent network drain? Are there any mechanisms to allocate bandwidth fairly or specifically to each user? Are there any tools to provide real-time alerts for administrator when abnormal activities are detected?

IP-guard Solution

The Bandwidth Management module aims to control bandwidth and gather statistics of traffic. With the collected traffic statistics and complete analysis report, system administrator can trace any abnormal traffic efficiently. Real-time alert is notified to administrators immediately if any abnormal traffic is detected. System administrators can adopt appropriate policies to deal with the problem instantly. During peak hours, administrator can easily assign fixed bandwidth to every user to ensure that every user has stable connection to the internal systems and the Internet.



IP-guard can limit the download speed.

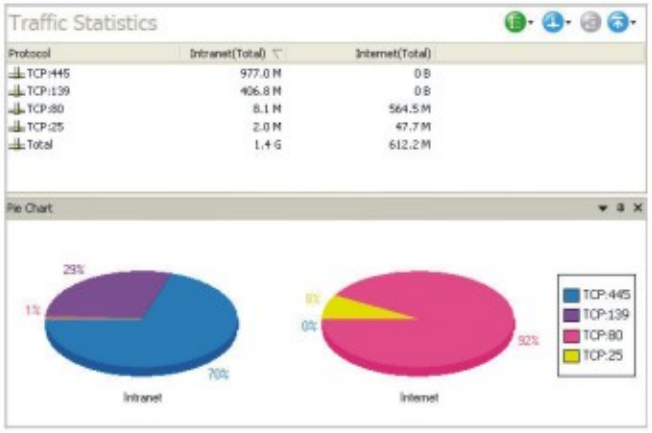
Bandwidth Control

Bandwidth Policy is used to limit the network bandwidth so as to avoid improper use causing network congestion. Also, the bandwidth can be controlled based on the specified network port.

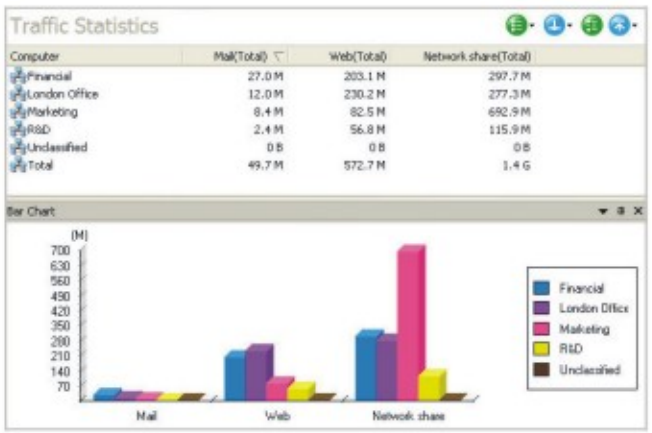
- Limit the download speed of agent computer
- Control the traffic of specific network port or network address
- Allocate different bandwidth to different ports

Traffic Statistics

The Network Traffic Statistics helps administrator to quickly trace network obstruction problems so that appropriate response measures can be taken to fix the problems. Traffic Statistics includes network addresses of both sides of communications, ports and bandwidth. Such information provides administrators with an overview of the current network status.



Gather traffic statistics by port



Gather traffic statistics by department

More Suggestions

Combining with the use of Network Management function, IP-guard not only can enhance the internal security level, but also can prevent illegal computers from accessing internal protected servers with its intrusion detection and blocking functions. For details, please refer to Network Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Basic Management

The essential module of IP-guard

Module Description

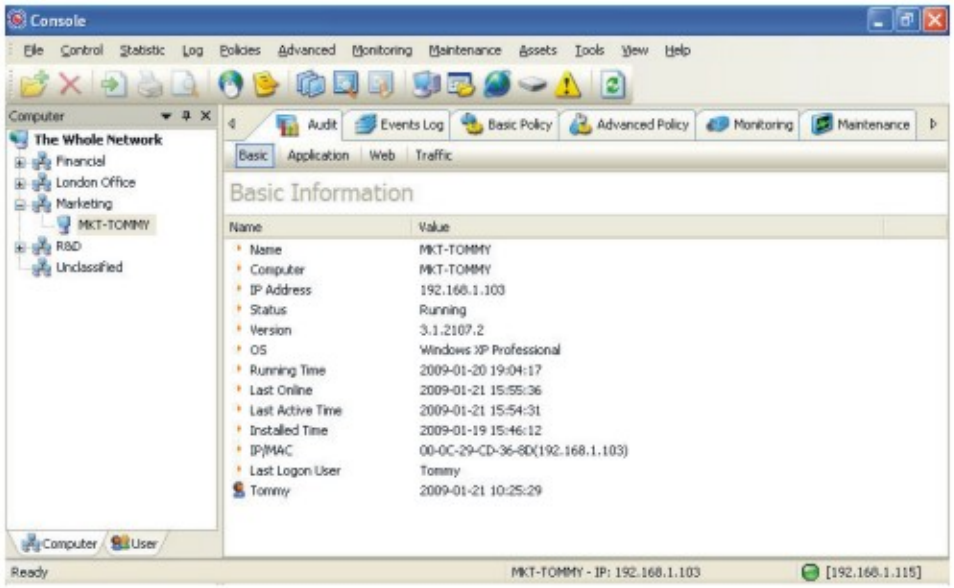
Basic Management module is the essential part of IP-guard. It includes all basic functions such as basic information, basic control basic event log, basic policy, system alert, etc.

Features

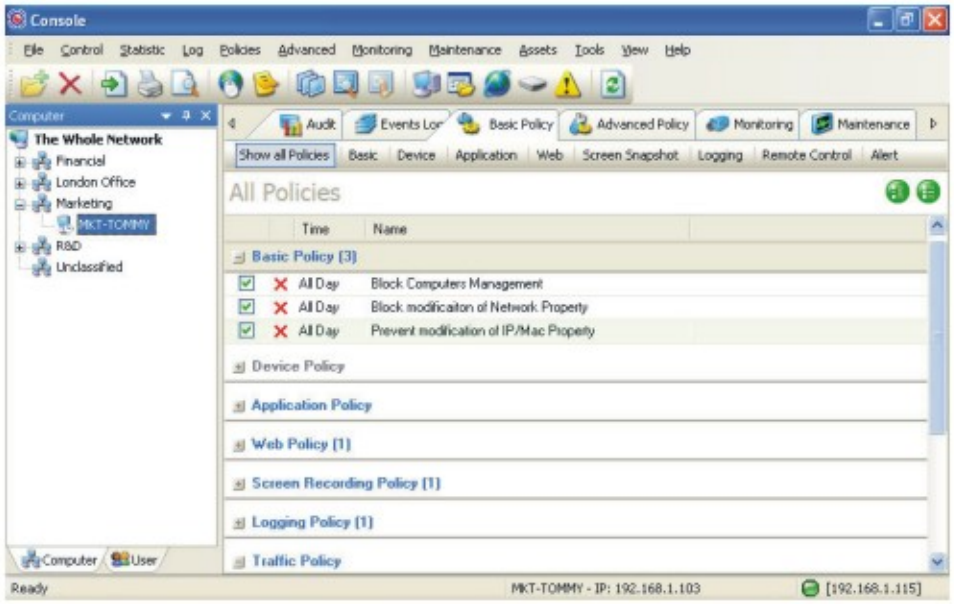
- Support multi-language interface
- Control the setting of control panel, computer management, network configuration, IP/MAC binding and ActiveX controls
- Basic controls include system lock/unlock, shutdown, restart and logoff agents
- Powerful search engine to retrieve target information
- Export and import event logs

Basic Management of IP-guard

Basic Management module is the basic part of IP-guard and includes all basic functions. It includes basic information, basic control (e.g, lock, shutdown, restart and logoff agents), basic log, basic policy and system alert.



Basic information (e.g., computer name, IP address, logon user, status) of selected computer can be viewed on IP-guard console.



All policies are showed such as Application Policy, Basic Policy and Device Policy.

Basic Control

- Block Control Panel
- Block Computers Management
- Block Task Manager and Regedit
- Block Command Prompt
- Block modification of Network Property
- Prevent modification of IP/Mac Property
- Block ActiveX

Basic Logs

- Log system startup/shutdown
- Log user logon/logoff
- Provide dial-up logs

System Alert

- Give alert when hardware and software assets change
- Give alert when plug in/off storage device and communication device
- Give alert when system information changes
- Give alert when network configuration changes

More Suggestions

There are thirteen more modules in IP-guard available for your selection. Customers can select their desired modules based on their requirements. For details, please refer to the information of corresponding modules.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Device Management

Control device usage to prevent information leakage

Module Description

Device Management module aims to control removable storage devices such as communication devices and network devices by executing control policies.

Features

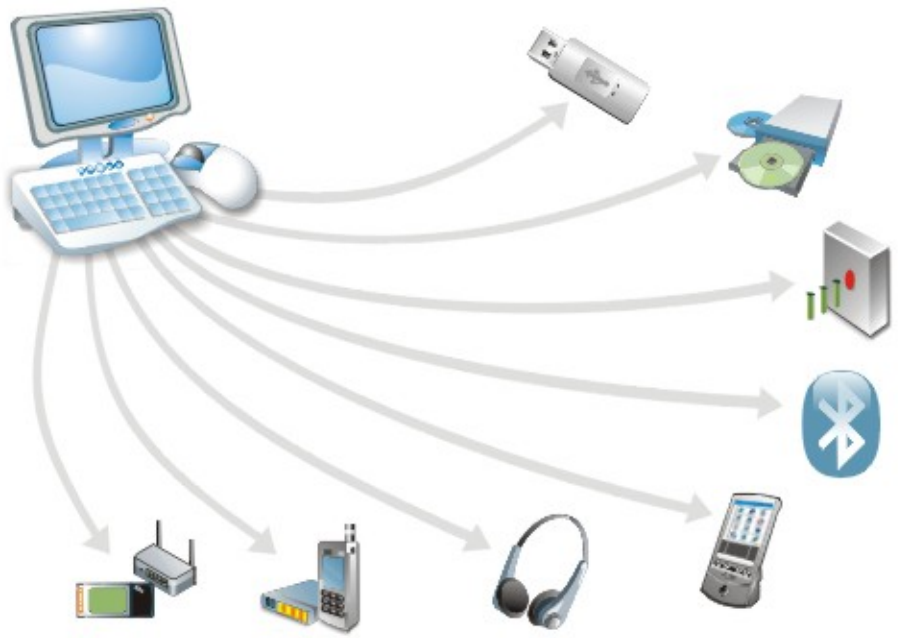
- Easy control of access rights of all devices
- Real-time policy execution with no restart action required
- Detailed log of triggered events

Device Management Challenge

Are you looking for a solution to manage endpoint devices to prevent information leakage through USB flash drive, CD/DVD burning devices, Bluetooth, Infrared, etc.? Nowadays, these devices have become common integrated pack of communication, and yet "convenient" ways of letting go of information. The ideal solution is "Single agent, Full Control and Monitoring".

IP-guard Solution

The Single Agent approach in IP-guard provides ease of logging operations of each agent computer, executing policies and monitoring. One of the modules in IP-guard called Device Management facilitates IT administrators to manage endpoint devices including storages, communication devices, dial services, USB devices, network devices and other devices such as audio and virtual CDROM, etc. What IT administrators have to do is to set control policies for specified devices and the policies will be automatically distributed to the Agent immediately and then executed instantly. All triggered events are logged and IT administrators can trace the details through the Console easily.



IP-guard can effectively control and manage various devices such as USB flash drive, Bluetooth, infrared device and headphones.

Available Devices Control

Storages

- Floppy
- CDROM
- Burning Device
- Tape
- Removable Device

Dialup

- Dial-up Connection

USB Devices

- USB Keyboard
- USB Mouse
- USB Modem
- USB Image Device
- USB CDROM
- USB Storage
- USB Hard Disk
- USB LAN Adapter
- Other USB Devices

Communication Devices

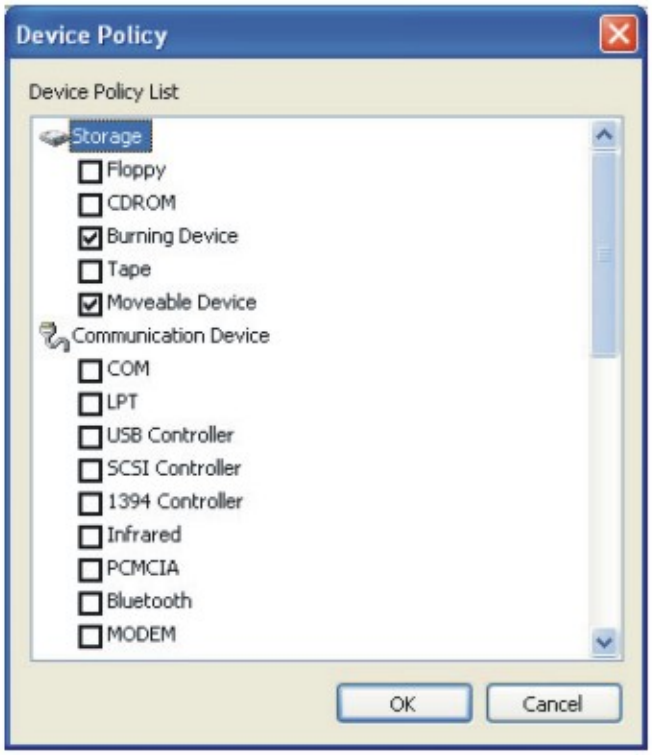
- COM
- LPT
- USB Controller
- SCSI Controller
- 1394 Controller
- Infrared
- PCMCIA
- Bluetooth
- MODEM
- Direct Line

Network Devices

- Wireless LAN Adapter
- PnP Adapter (USB, PCMCIA)
- Virtual LAN Adapter

Others

- Audio
- Virtual CDROM
- Any New Devices



More Suggestions

Concerned about the endpoint security issues, IP-guard provides another comprehensive and powerful module called Removable Storage Management to manage and control the removable storage devices. In this module, removable devices such as USB hard disk and flash drive can be fully authorized with read-write access control. Only the authorized agent computers can encrypt and decrypt the disks or files. Also, the user-friendly device management console allows IT administrators to register approved list of devices, and then apply a policy to only allow registered removable storage devices to be used within the company.

Without the need of file/disk encryption function, another module called Document Management is recommended. For details, please refer to Document Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Document Management

Manage and control document to protect your intellectual property

Module Description

Document Management module aims to control all document operations in different types of storage media, such as local hard disk, CD-ROM, Floppy, network drive and removable drive.

Features

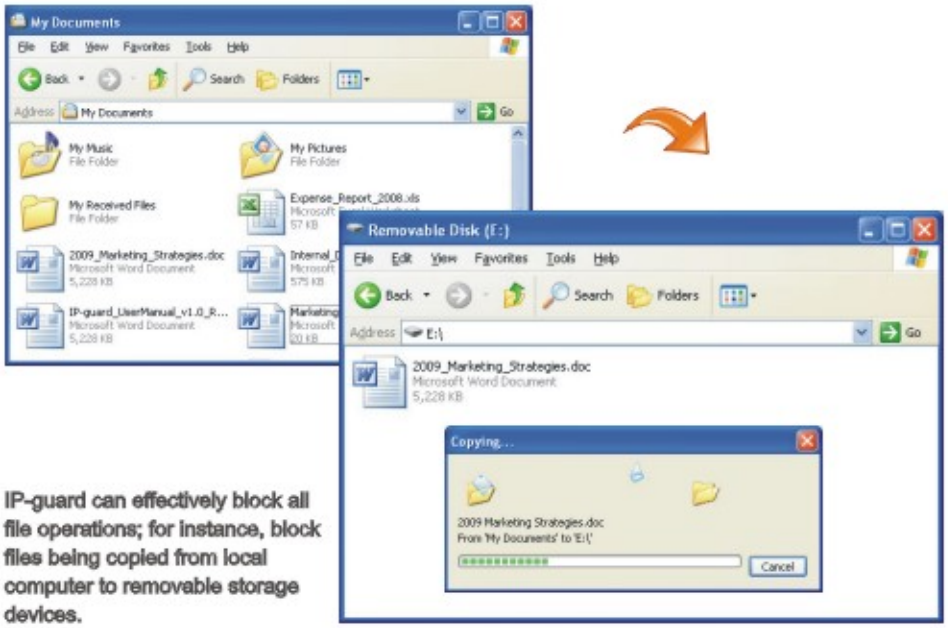
- Detailed logs about all file operations include access, modify, delete, copy, create, restore and rename actions.
- Powerful control policies on local hard disk, network shared drive, CDROM and removable storage
- Backup specified files based on certain trigger actions such as modification, copy, cut, movement and deletion
- Powerful search engine helps to trace activities in faster and more efficient ways

Document Management Challenge

If there are no controls or preventions about document management, some important files may be leaked out accidentally or maliciously by employees, or accessed by unauthorized personnel. Moreover, IT administrators may face challenges in managing and controlling documents operated in removable devices. For instance, if some confidential files are disclosed to competitors, who, when and how these files were sent out from office? Can any event logs be traced back to starting point? Could any prevention be adopted to avoid such incidents? These are some of the questions which are often asked.

IP-guard Solution

The Document Management module aims to tackle the document security challenges. It provides ways to control all documents operated in different types of storage media, including local hard disk, network drives, CDROM, floppy drive and removable disks. IT administrator can set different policies targeting on different types of disks to control the file operations such as read, modify and delete. The typical examples are to protect important files which cannot be deleted; to limit different users to access specified network shared drives; to prohibit user from playing MP3 files; all removable disks only have read-only access right and so on. All these policies can be applied to specified groups or users.



IP-guard can effectively block all file operations; for instance, block files being copied from local computer to removable storage devices.

Document Control

Administrator can control user's operating privilege of document on hard disks, removable storage devices, network disks, etc. Therefore, document security can be ensured.

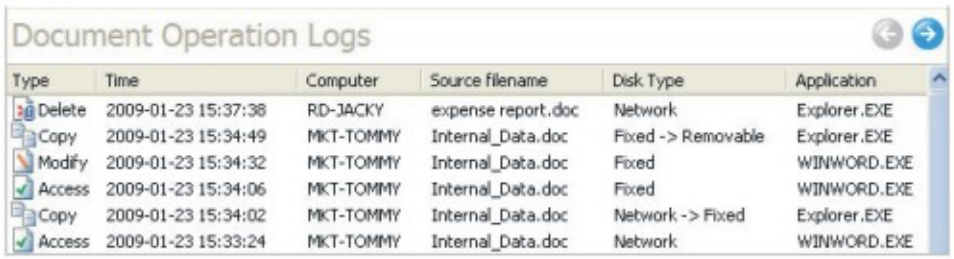
- Only allow authorized users to access specified shared folders in servers
- Prohibit users from copying any files to removable disk
- Prohibit users from modifying and deleting specific important documents

Document Backup

IP-guard can backup specified files based on certain actions, such as modify, copy, cut and delete. Administrator can view and save backed up files from Document Operation Log. Therefore, IP-guard ensures that important documents are used in managers' controlled range.

Document Operation Logs

Document Operation Logs records user's document operations on hard disks, network disks, removable storage devices, etc. It includes Type, Computer, User, Filename, Path, File Size, Disk Type, Caption, Application, etc.


Document Operation Logs

Type	Time	Computer	Source filename	Disk Type	Application
Delete	2009-01-23 15:37:38	RD-JACKY	expense report.doc	Network	Explorer.EXE
Copy	2009-01-23 15:34:49	MKT-TOMMY	Internal_Data.doc	Fixed -> Removable	Explorer.EXE
Modify	2009-01-23 15:34:32	MKT-TOMMY	Internal_Data.doc	Fixed	WINWORD.EXE
Access	2009-01-23 15:34:06	MKT-TOMMY	Internal_Data.doc	Fixed	WINWORD.EXE
Copy	2009-01-23 15:34:02	MKT-TOMMY	Internal_Data.doc	Network -> Fixed	Explorer.EXE
Access	2009-01-23 15:33:24	MKT-TOMMY	Internal_Data.doc	Network	WINWORD.EXE

Shared File Logs

Shared File Logs records operations of remote host in shared files of agent computers. It includes Type, Remote Host, Filename, Path, etc.

More Suggestions

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

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Email Management

Control and monitor emails to prevent information leakage

Module Description

Email Management module aims to help system administrator to control outgoing emails and log all emails with attachments including supported SMTP/POP3 email, Exchange email, webmail and Lotus Notes email.

Features

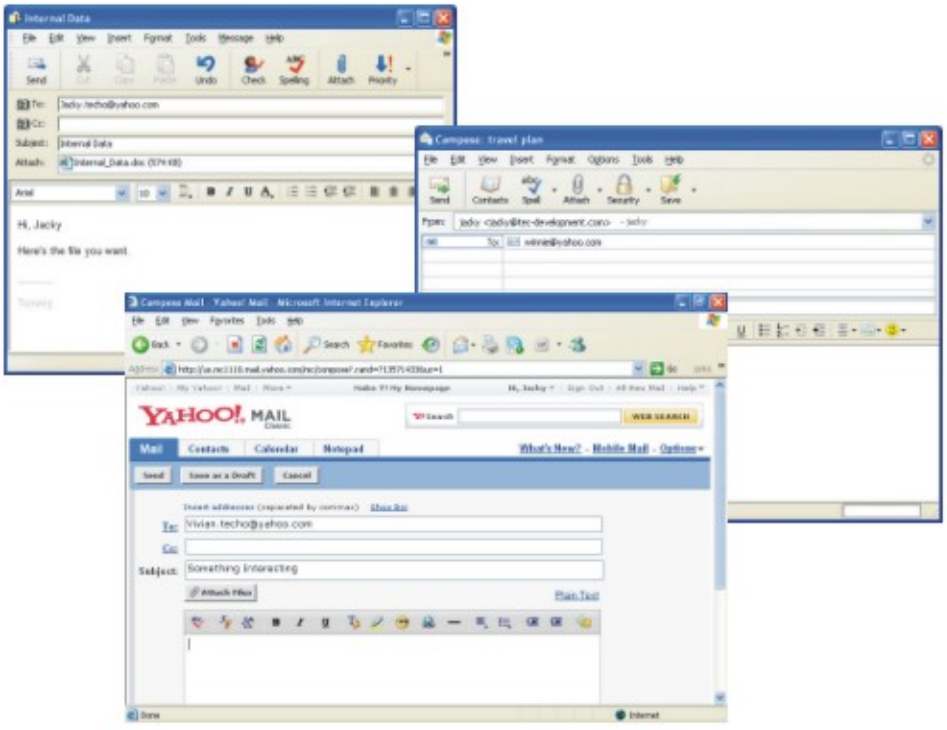
- Control outgoing mails by specifying sender, recipients, email subject and size of attachment
- Log emails with attachments including supported SMTP/POP3 email, Exchange email, webmail and Lotus Notes email
- Easy to search the suspect email by specified email type, address, subject, content, attachment name and size

Email Management Challenge

Email is very common no matter in business or personal communication. But how do you know the users use the email in proper ways? Does your company have some policies to control the flow of email so as to make sure that emails are appropriate? For instance, no email should be sent to competitors; general staff cannot broadcast email to all other accounts. How do you keep track of users' personal emails? Do they send some confidential files out through their personal email? Such concerns should not be neglected by system administrator indeed.

IP-guard Solution

Email Management module includes logging supported webmail such as Hotmail, Yahoo! Mail, Gmail, etc; logging Exchange and Lotus Notes email. According to different company policies, system administrator can make different policies to control all outgoing emails by specified sender, recipient, email subject, with or without attachment and the size of attachment.



IP-guard can effectively monitor different kinds of email such as SMTP/POP3 email, Exchange email, webmail and Lotus Notes email.

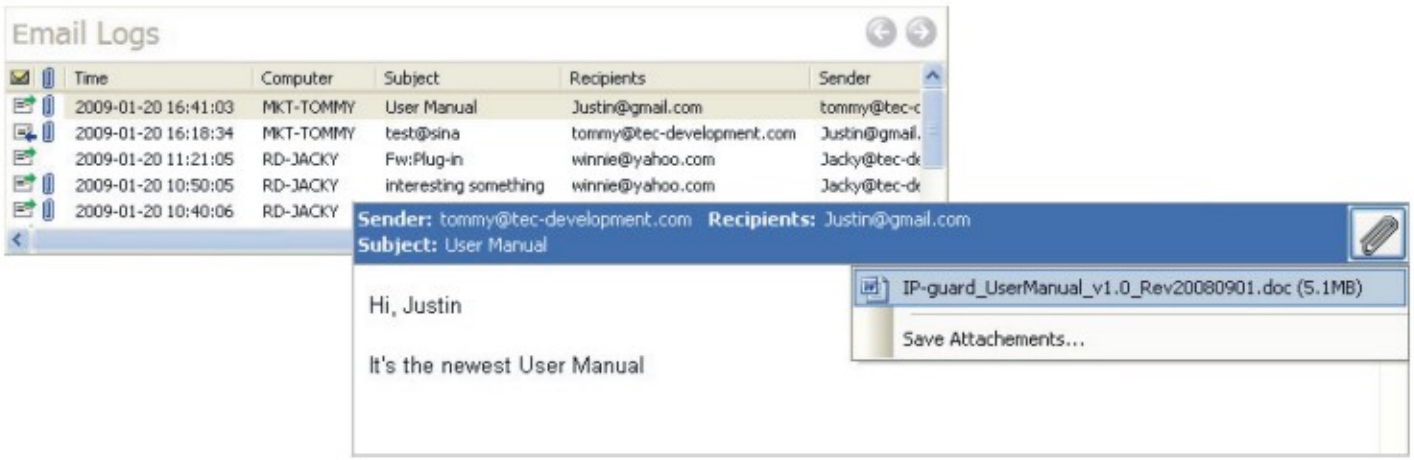
Email Control

IP-guard controls outgoing mails by specifying sender, recipients, email subject, file name, type and size of attachment.

- Block outgoing email with illegal attachment
- Block outgoing email if the recipient is an illegal account

Email Logs

IP-guard records emails with attachments including supported SMTP/POP3 email, Exchange email, webmail and Lotus Notes email.



More Suggestions

Besides email, there are many ways to cause information leakage such as IM tools, printing and removable storage media (e.g., Bluetooth, infrared devices, USB storage devices). We would recommend you further reading of the information of IM Management, Printing Management, Document Management, Device Management and Removable Storage Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Instant Messaging (IM) Management

Control and monitor IM tools to protect information security and improve work efficiency

Module Description

The IM Management module aims to control outgoing files which are transferred through IM tools so as to prevent information leakage via this channel. Also, the IM conversation contents can be logged and saved for your review in the future.

Features

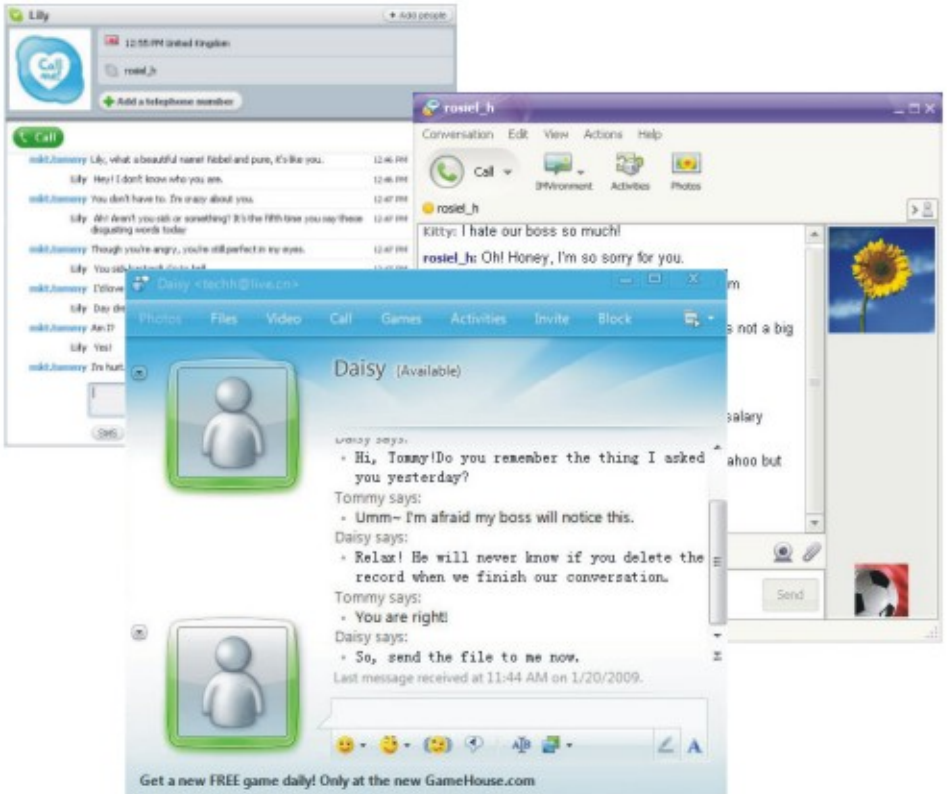
- Support most common IM tools such as MSN, Yahoo! Messenger, SKYPE, ICQ, QQ, etc.
- Record chat conversations and instant messages
- Easily block outgoing files
- Backup all outgoing files

IM Management Challenge

IM tools are typically used for personal reasons, but also increasingly used to facilitate business communications. Employees may be allowed to use IM tools in the office environment. How can the use of IM tools be effectively monitored? How could you know what files are sent through IM tools? Are there any ways to restrict users to send out files? Or, in case files are sent out, are there any ways to trace them back?

IP-guard Solution

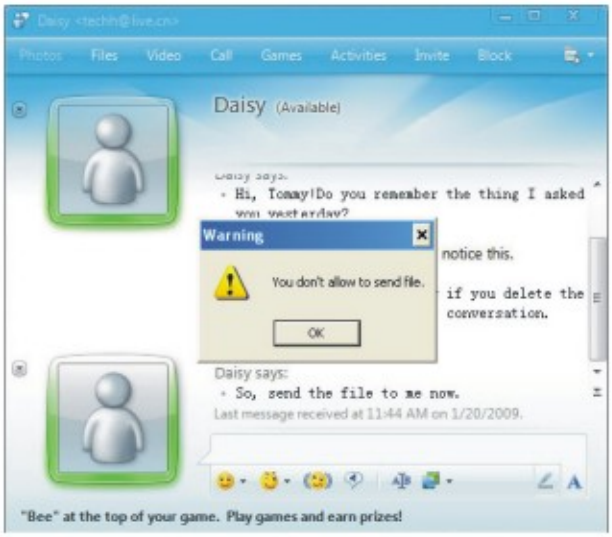
The IM Management module aims to control and monitor the use of IM tools. With the setting of appropriate IM file policies, all outgoing files can be prohibited and backed-up at the option of system administrator. IP-guard supports over ten common IM tools including MSN Messenger, Skype, ICQ, Yahoo! Messenger, Lotus Sametime, Tencent QQ, etc. Moreover, system administrator could select the option to log the IM conversation contents.



IP-guard can record the instant messaging content of various IM tools such as MSN Messenger, Skype and Yahoo! Messenger.

IM File Control

In order to prevent important file from leaking through IM tools, IM File Policy is used to prohibit outgoing files. Real-time alert is sent to administrator if any prohibited action is taken.



IM File Backup

IP-guard can backup all files sending out via IM tools so that administrator can check the backups on IP-guard console. Therefore, IP-guard effectively prevents information leakage.

IM Monitoring

System administrators are able to monitor instant message history of agent computers. Supported instant messaging tools include MSN Messenger, ICQ, Skype, Yahoo! Messenger, Tencent QQ, etc.

More Suggestions

Other IP-guard modules, namely, those relating to Document Management, Email Management, Device Management and Removable Storage Management, are also recommended.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Network Management

Prevent unauthorized external computers from accessing internal network

Module Description

Network Management module aims to control and monitor network communications. With policy control based on various parameters, including IP address, network ports, traffic directions and agent properties, etc. System administrator can effectively block selected network ports or download ports to minimize virus attack or network drain. Also, the intrusion detection and blocking functions help to protect your internal network away from illegal external access.

Features

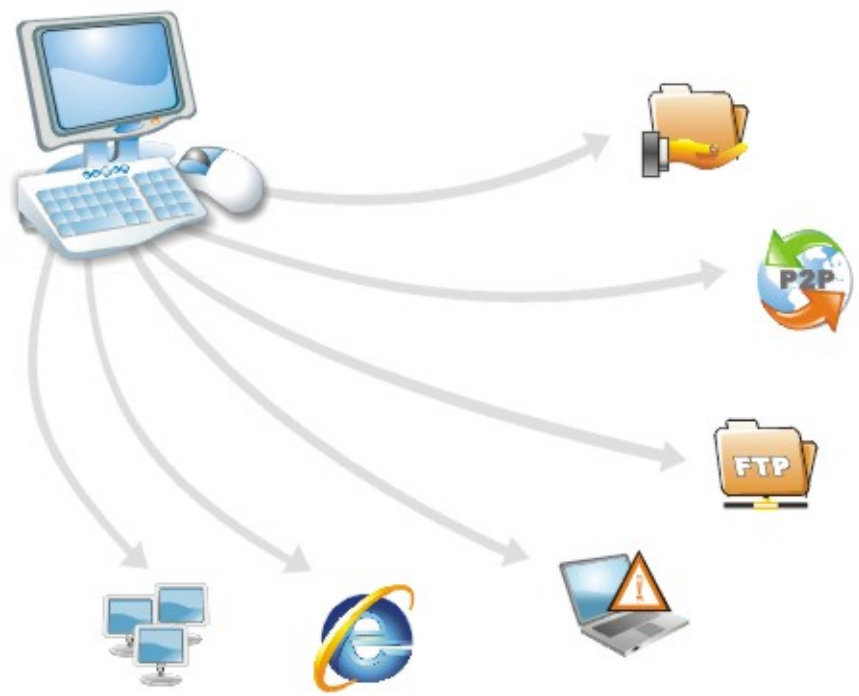
- Easy-to-adopt policy, based on parameters of network address, port and traffic directions and so on to control network communications
- Intrusion detection and blocking functions to prevent illegal external access
- Real-time alerts are sent to administrator upon the detection of any prohibited actions
- Easy to assign network access rights to different groups

Network Management Challenge

Today, for most companies, confidential and sensitive data are archived in computers. However, some companies do not have standard management to safeguard information security and give intruders a chance to access internal computers to steal data and spread virus. Therefore, information security is facing a great challenge. How to protect information security, maintain system stability and keep away from intrusion and virus attrack have become a heated question for lots of mangers.

IP-guard Solution

Network Management module can effectively stop illegal computers from accessing computers within the internal network to prevent information leakage. By controlling network ports, administrators can block malicious ports and download ports in order to keep away from virus and protect internal network security. Moreover, administrator can reasonably control the access rights of different apartments so as to standardize company management.



IP-guard can effectively control the communication among computers, block illegal share, illegal connection and protect network security.

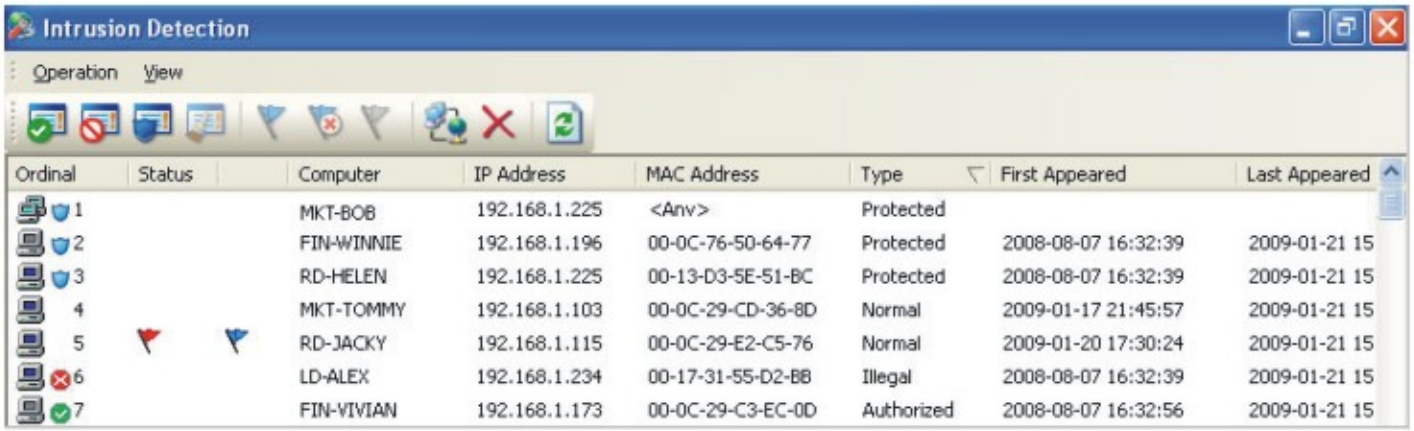
Network Control

By specifying specific network port, network address and direction, administrator can realize network communication control.

- Block unauthorized computers from communicating with computers with IP-guard agents installed
- Block illegal network share
- Block FTP port and other download ports

Intrusion Detection

The Intrusion Detection function of IP-guard is used to discover any illegal or unauthorized computers accessing the internal network of enterprise and then apply corresponding policies to block their communications within the internal network.



Ordinal	Status	Computer	IP Address	MAC Address	Type	First Appeared	Last Appeared
1		MKT-BOB	192.168.1.225	<Anv>	Protected		
2		FIN-WINNIE	192.168.1.196	00-0C-76-50-64-77	Protected	2008-08-07 16:32:39	2009-01-21 15
3		RD-HELEN	192.168.1.225	00-13-D3-5E-51-BC	Protected	2008-08-07 16:32:39	2009-01-21 15
4		MKT-TOMMY	192.168.1.103	00-0C-29-CD-36-8D	Normal	2009-01-17 21:45:57	2009-01-21 15
5		RD-JACKY	192.168.1.115	00-0C-29-E2-C5-76	Normal	2009-01-20 17:30:24	2009-01-21 15
6		LD-ALEX	192.168.1.234	00-17-31-55-D2-BB	Illegal	2008-08-07 16:32:39	2009-01-21 15
7		FIN-VIVIAN	192.168.1.173	00-0C-29-C3-EC-0D	Authorized	2008-08-07 16:32:56	2009-01-21 15

More Suggestions

Combined with the use of Bandwidth Management function, the problem of network drain can also be prevented. For details, please refer to the information of Bandwidth Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Printing Management

Monitor and control printing to prevent information leakage

Module Description

Printing Management module aims to help enterprises to manage printing facilities and optionally backup the image of printed documentsfor record.

Features

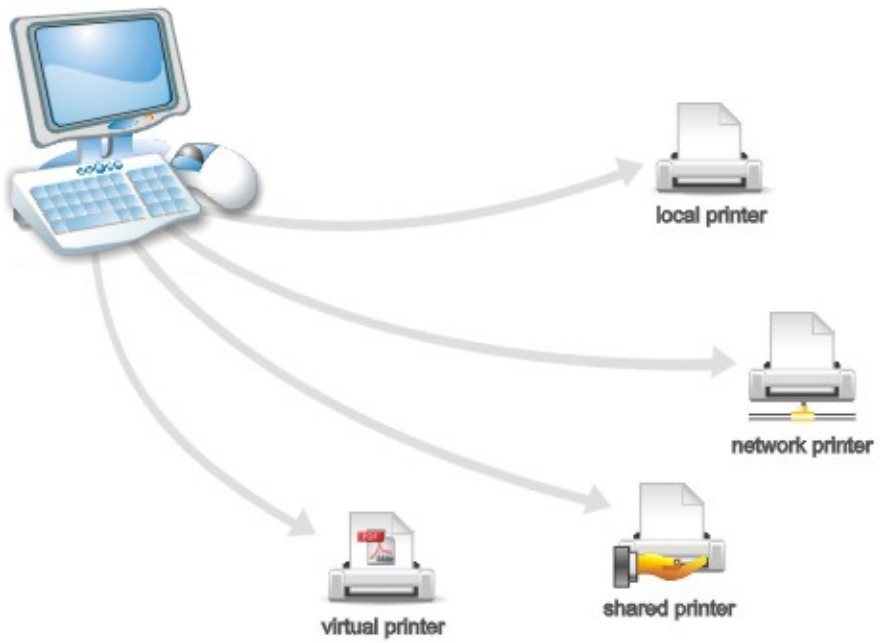
- Limit users to use printers
- Detailed printing log about local, network, shared and virtual printers usages
- Backup printed document in image file

Printing Management Challenge

How do you know the printing services are used properly in your office? Are you concerned that some important files may have been printed? Can you centrally control and monitor the usage of printers? Sometimes, files may be converted to PDF or image files and then sent out by way of email or IM tools. To prevent information leakage, whether through physical or virtual printers, printing management should not be neglected.

IP-guard Solution

Printing Management module includes printer access control and log. For printer access control, system administrator can control agent computers to access different types of printers including local, shared, network and virtual printers. Also, if Record Printed Image is optionally selected, all backup printed files are saved into image formats. Moreover, the detailed printing log includes printer type, time, computer name, user name, printing task, printer name, number of pages, document caption and application by which the file was printed.



IP-guard effectively controls various types of printer such as local printer, shared printer, network printer and virtual printer.

Printing Control

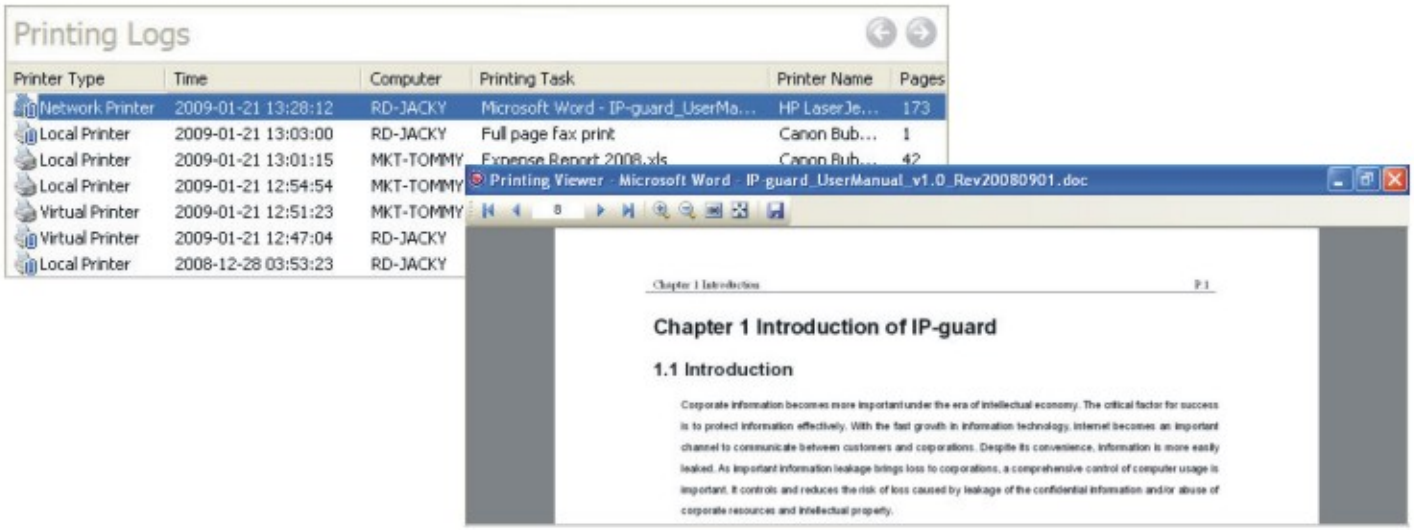
Administrator can prevent users from using specified printer types including local, shared, network and virtual printers.

Printing Backup

IP-guard can backup the image of printed files. Moreover, backup images can be saved and viewed in Printing Log.

Printing Logs

Contents of Printing Logs include printer type, time, computer name, user name, printing task, printer name, number of pages, document caption and application by which the file was printed.



More Suggestions

There are many ways to cause information leakage apart from printing, such as email, IM tools and end-point communication (e.g., Bluetooth, USB storage devices). We would recommend you reading the details relating to Email Management, IM Management, Device Management, Removable Storage Management and Document Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

IP-guard™

Remote Maintenance

Offer remote technical support to shorten fault fix time and quickly solve problems

Module Description

Remote Maintenance module aims to help system administrator or technical support staff shorten their support time. With information such as real-time report computer status, and functions such as remote control and remote file transfer, support tasks are facilitated whether agent computers are located in the headquarter office, branch office or remote site. System administrator can easily control all computers from IP-guard console.

Features

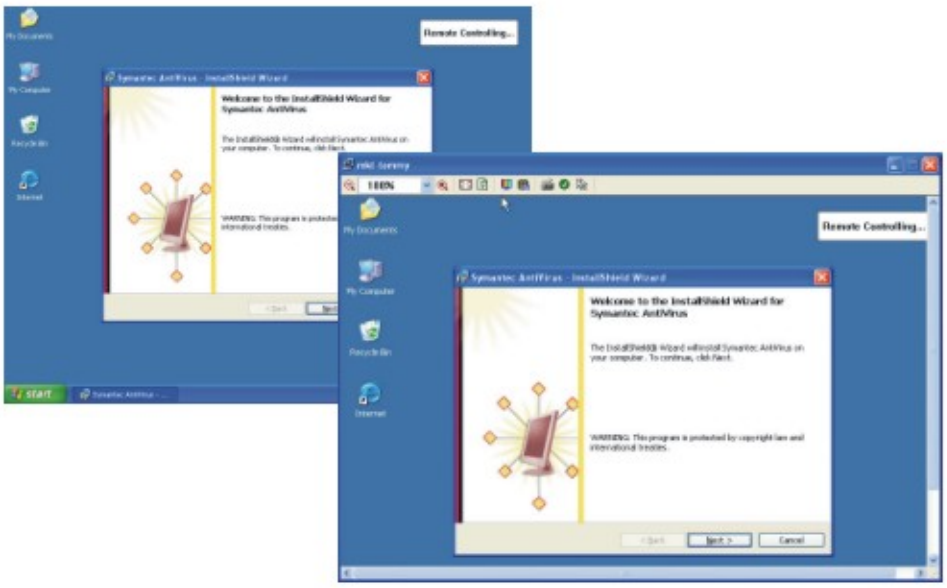
- Report computer status covering all running applications, processes, performance, device manager, services, disks, shared status, schedule, user and group status
- Support remote control
- Support remote file transfer

Remote Maintenance Challenge

According to researches of the Gartner Group and Forrester Research, nearly 50% of time within the MIS department has been spent on computer installation and software upgrading which occupies a large proportion of the computer cost. System administrators spend 70-80% of time working on daily maintenance tasks which increases the cost of computers. Moreover, productivity drops when computer problems cannot be solved immediately. Therefore, it is necessary to reduce the workload of system administrators on minor tasks so that they can concentrate on higher-level computer management tasks and information system enhancement.

IP-guard Solution

Remote Maintenance module includes real-time information checking, remote control and remote file transfer. Administrator can check the real-time computer information such as current running applications, processes and services on the console to analyse problems and then fix them immediately. In addition, remote control and remote file transfer functions enable administrators to connect to any IP-guard agent computers and transfer files respectively via Internet. These functions substantially shorten the investigation time and provide a means for the administrator to directly diagnose the problems of agent computers.



With IP-guard, administrator can make remote installation of antivirus software to remote host.

Remote Control

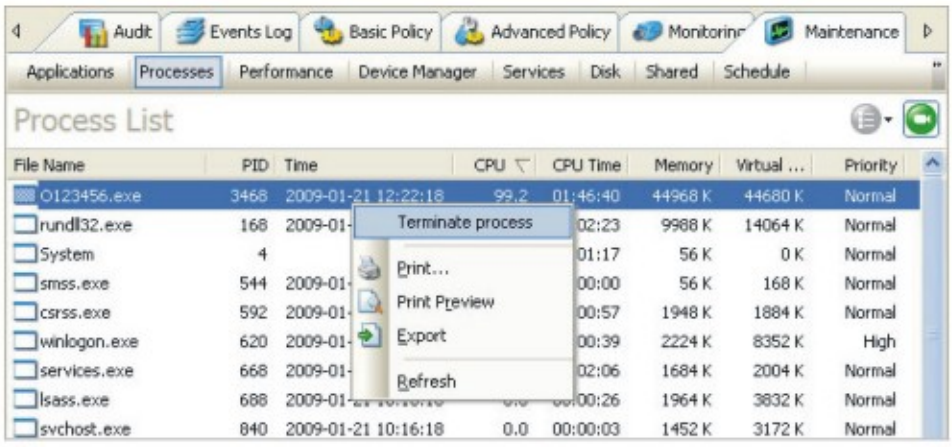
- Administrators can remotely control agent computers just like using their own computers
- Administrators can easily demonstrate system operations to users

Remote File Transfer

- Deliver files between local and remote computers
- Collect fault samples from the designed folder of remote computers

Remote Maintenance

- Real time information checking
- Remotely diagnose problems of agent computers



IP-guard enables you to view the processes of agent computer and terminate any abnormal process.

More Suggestions

To reduce time and cost constraints on maintaining the highly diverse and widely distributed IT infrastructure has become an absolute necessity for organizations, whether big or small. IP-guard System Management Solution provides IT managers with tools to gather software and hardware asset information automatically and maintain enterprise IT assets with convenience.

The comprehensive capabilities of IP-guard System Management Solution include Asset Management and Remote Maintenance.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Removable Storage Management

Authorize and encrypt removable storage devices to give you reliable information security

Module Description

Removable Storage Management module aims to authorize and encrypt removable devices such as USB flash drive and hard disk. Only authorized personnel can access removable storage device and decrypt their contents.

Features

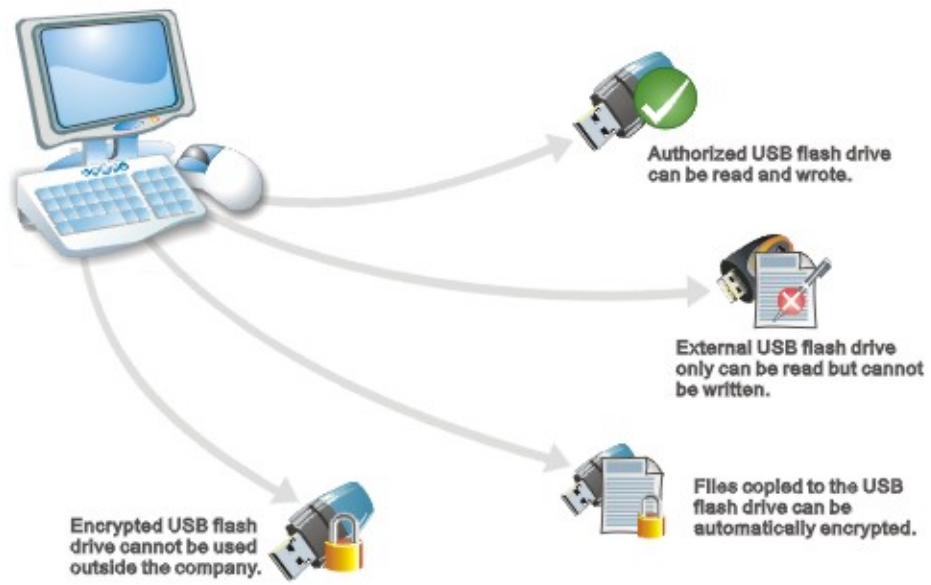
- Disk-based removable storage authorization
- File-based disk and removable storage encryption
- Only authorized agent computers can access the encrypted removable storage device
- Allow system administrator to register the approved list of removable device and only registered devices can be used with access right 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 great loss. In addition, virus and Trojan horses may intrude 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 manage all removable storage devices, but also can grant different use privileges 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.

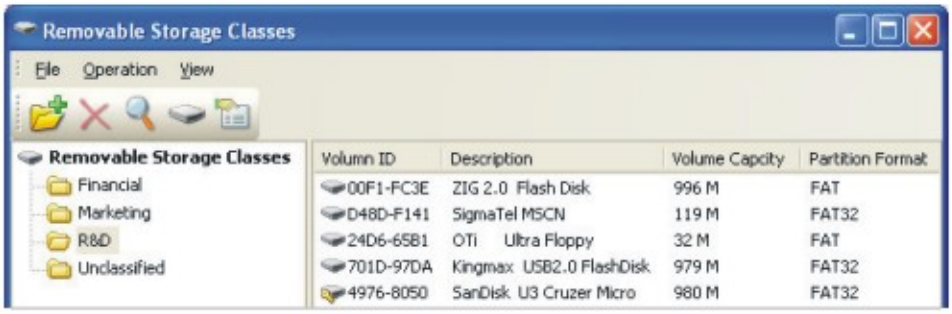
Removable Storage Control

Removable Storage Management module can control the usage rights of all removable storage devices so as 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

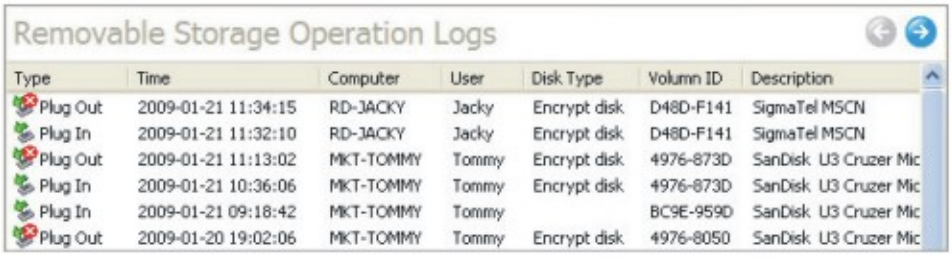
Removable Storage Classes

In Removable Storage Classes, administrators can manage all removable storage devices, register and classify them into different catalogues based on their needs.



Removable Storage Operation Logs

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



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
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

Screen Monitoring

Capture and playback screen activities to completely understand user behavior

Module Description

Screen Monitoring module captures screen activities in real time and supports multi-screen monitoring. All screen snapshots are saved in proprietary formats. Only authorized users can playback the contents using the built-in viewer of IP-guard console.

Features

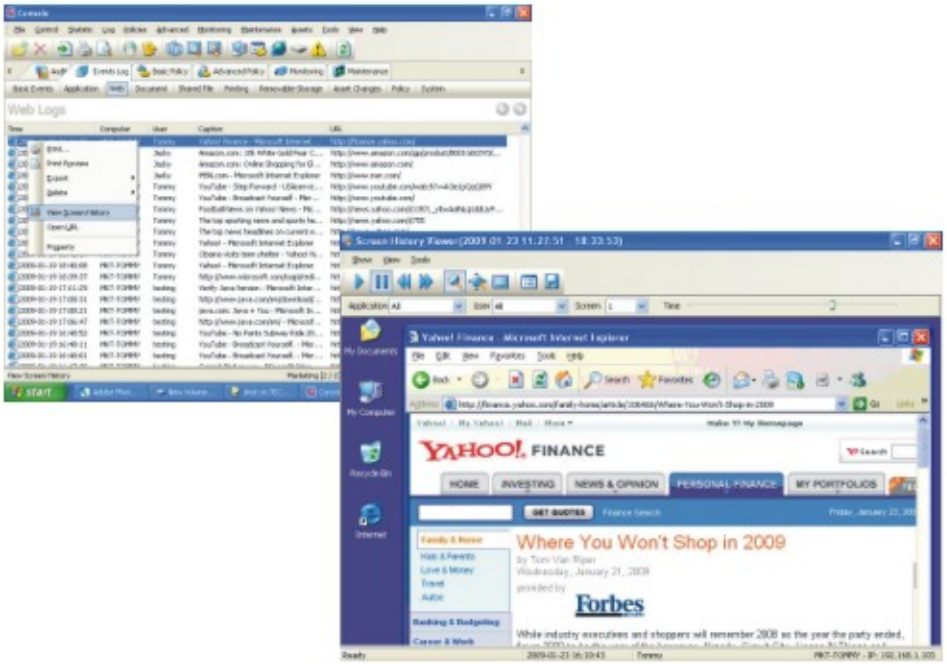
- Monitor screen activities in real time
- Support multi-screen monitoring
- Support screen history review
- Screen history can be exported to video and played by Windows Media Player.

Screen Monitoring Challenge

Do you want to know whether all your employees are doing work related things with their computers? Are you looking to find a way to estimate your employees' performance? Have you ever experienced confidential information leakage but could not put your finger on the culprit? Annoying? With the Screen Monitoring module of IP-guard, all your problems can be solved with ease.

IP-guard Solution

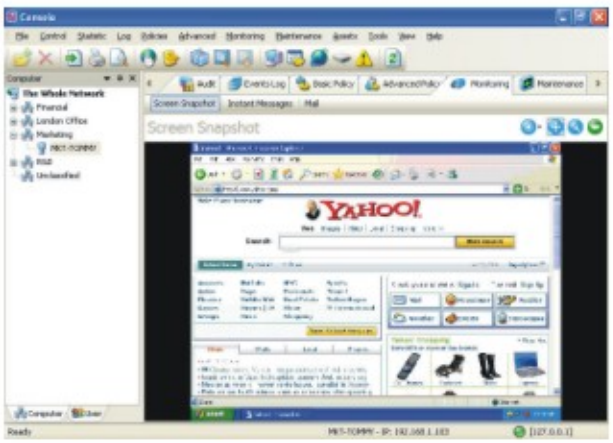
The Screen Monitoring module of IP-guard enables you to monitor your employees' on-screen activities and know what they do with their computers. Moreover, it also provides multi-screen viewing and screen history viewing functions. With multi-screen monitoring function, you can monitor several employees at one time. By viewing screen history, you can easily obtain pure and impartial proof of any illegal operations. In addition, screen history can be exported to video and played by Windows Media Player for your review in the future. Screen Monitoring is the most powerful way to visually record and review everything your employees do online and offline.



With IP-guard, you can optionally view the screen history of specified event log.

Real-time Screen Monitoring

Real-time screen monitoring enables you to monitor and track your employees' on-screen activities. Distance is no longer an obstacle. You can monitor and watch what your employees are doing no matter where you are at any time.



Multi-screen Monitoring

Multi-screen monitoring function enables you to monitor and track many screens (maximum 4x4 matrix screens) at one time. When you find out someone is doing things unrelated to work, you can lock that computer or send notify message to the user.

Screen History Review

By viewing screen history, you can easily obtain pure and impartial proof of user's illegal operation. Moreover, specific screen snapshots revealing that users may have committed illegal operations can be saved as evidence.

More Suggestions

The following modules support reviewing screen snapshot with corresponding event log. They are Application Management, Web Management, Printing Management and Document Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com

IP-guard™

Web Management

Record visited websites and limit site accessing rights to evaluate and regulate user behavior

Module Description

Web Management module aims to control and monitor users' web browsing behavior. With appropriate policy control, improper websites can be blocked easily and detailed logs help administrators understand user behavior on web usage.

Features

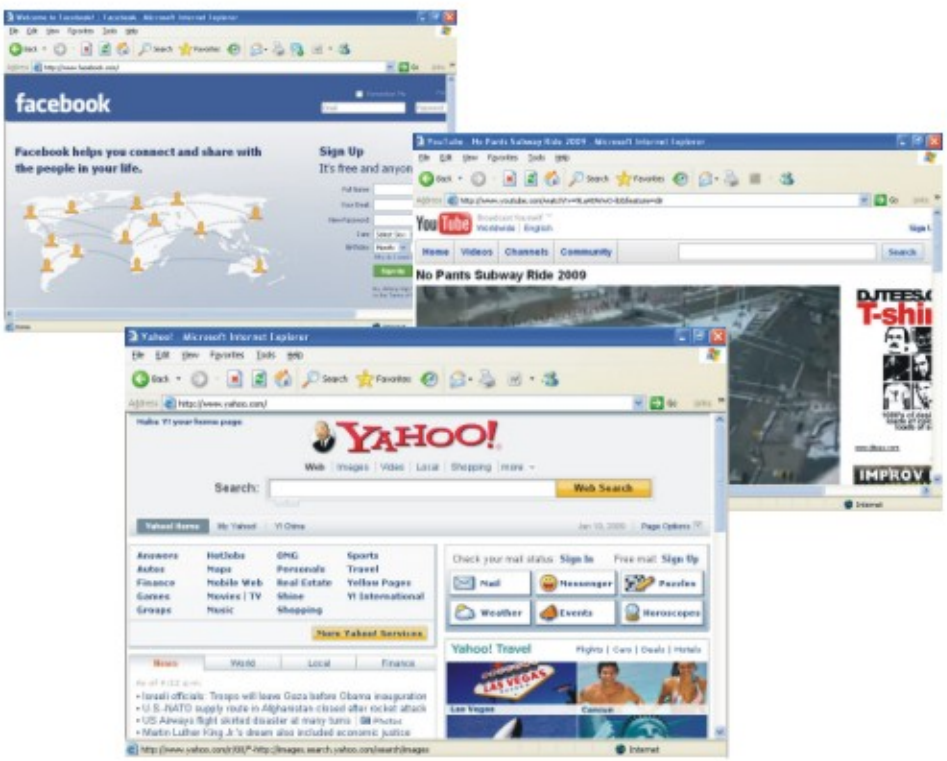
- Easily block improper websites by policies
- Real-time alerts are notified to administrator upon any unauthorized access
- Detailed web browsing log
- Complete web browsing analysis report

Web Management Challenge

More and more employees spend their time in browsing websites which are unrelated to work during working hours. Many employees may think that office computers are their personal property and they could do whatever they want with the computers. Such behavior may decrease work productivity and increase the risk of the misuse of corporate resources.

IP-guard Solution

The Web Management module aims to control and monitor users' web browsing behavior. Based on collected detailed log, web statistics and complete analysis report, administrators can have a better understanding of users' web browsing behavior. Such data could also be used as a reference for policy planning and management purposes; for instance, as an indication of which websites to be blocked or limited in order to increase work efficiency.



IP-guard controls the accessing rights of various websites such as entertainment websites, news websites and financial websites.

Web Control

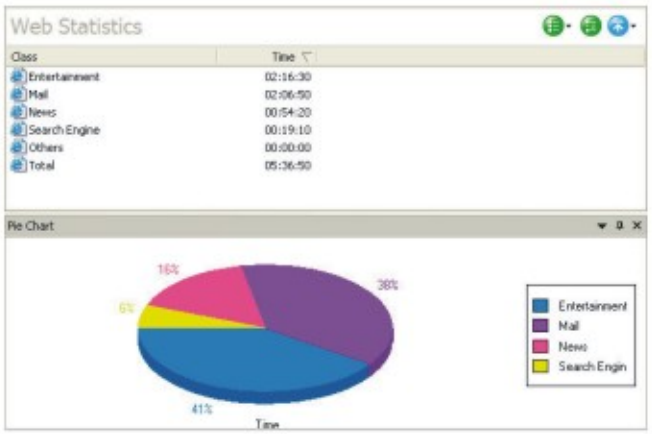
Web Policy provides settings for administrators to effectively control users' access rights of websites. By setting appropriate web policies, administrators can easily control users' access rights of selected websites.

Web Logs

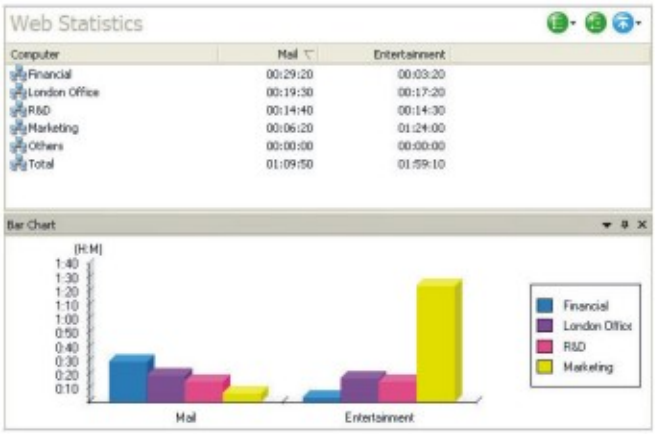
The contents of Web Logs include browsing time, computer, user, caption of browser and URL.

Web Statistics

Web Statistics affords statistics on what websites users have visited. The statistical data provide references for administrators to easily understand the web browsing behavior of users.



Gather web browsing statistics by class



Gather web browsing statistics by department

More Suggestions

Combining with Application Management function, IP-guard can effectively regulate employees' work behavior. For details, please refer to Application Management.

Available Modules for Your Selection

- Application Management
- Asset Management
- Bandwidth Management
- Basic Management
- Device Management
- Document Management
- Email Management
- IM Management
- Network Management
- Printing Management
- Remote Maintenance
- Removable Storage Management
- Screen Monitoring
- Web Management

Hong Kong Office
Tel: (852) 2950 0067 Fax: (852) 2950 0709

Guangzhou Office
Tel: (8620) 8555 8747 Fax: (8620) 8554 1091

Contact Email
sales@ip-guard.com