DESKTOP MANAGEMENT SYSTEM

Enterprise-class IT Desktop Management Suite for any business that is simple to use, quick to deploy and easy to master.

LEP-Desktop Management System

LEP-DMS is the top choice by IT professional for controlling, monitoring, and auditing the IT environment. With LEP-DMS, various tasks can be automated and this increase your IT professional's efficiency in dealing with their daily job. LEP-DMS is highly scalable and suitable for all organizations big or small.

BEYOND SECURITY LINKDOOD

Table of Content

Introduction

The need for endpoint security management technology arises due to the increase in network management requirements and flaws of traditional data security solutions. Endpoint security management complements the development of network management technology and is an important component of a modern network security system. Therefore, endpoint security management solution should be the foundation of a network security system.

Network endpoint security management is one of the key requirements of a comprehensive modern network security management system. Our expertise and comprehensive understanding of the data security sector makes our endpoint management product the top choice for clients.

Data security surveys and reports from the past two years revealed that more than 80% of management and security issues happened at large scale organizations such as governmental, enterprises and financial securities. Computers play a large part in everybody's daily life. However, due to the factors such as ignorance of human beings and lack of security policies, endpoints are becoming the weak link of an information security system.

Background

A common misconception is to relate network security risks with outside intrusion. However, the reality is that most of the security risks are originally present within the network. Conventional data security concept is limited to the level of the gateway, network boundaries (firewalls, IDS, vulnerability scanning) and etc.

Critical computer devices are commonly located on an isolated network in the server room. These devices are often under strict monitoring to greatly reduce the risk of intrusion from the outside network. Security threats that are present within the network pose a bigger challenge to security managers.

As a summary, common requirements from network managers of governmental agencies and enterprises are as follow:

- Identify system vulnerabilities from endpoints and automatically distribute patches;
- Manage the usage of mobile storage mediums such as USB drives;
- Effectively solves the problem of endpoints accessing random networks;
- Prevent intranet only devices from connecting to the Internet to perform harmful activity;
- Manage endpoint assets to ensure the normal operation of network equipment;
- Creates a unified security policy for the whole network;
- Discover the endpoints that utilize high network bandwidth;
- Conveniently perform maintenance remotely;
- Prevents the leakage of confidential information from intranet;
- Unified monitoring and management on trusted application software installed on endpoint;
- Quickly and efficiently locate vulnerable point of entry for viruses, worms and hackers in the network. Also addresses the problem in real-time;
- A powerful unified network security alerting platform for security incident response and event query with the aim of comprehensively managing the network resources.

The hidden endpoint security risk may threaten the normal network operations of other users. Taking into consideration of the above mentioned requirements, Linkdood Technologies Sdn. Bhd. aims to provide industry leading endpoint security management products and application solutions.

System Architecture

By adhering to the concept of equal attention to network protection and endpoint protection, Linkdood endpoint security products provide solutions assisting network administrator. The network administrators may face problems in the process of network management and endpoint management as well as implementing controllable management of endpoints. Linkdood endpoint security products solve these problems.

Linkdood endpoint security management products improves the state of management, behavior and event of networked endpoint as well as provide protection beyond the capabilities of firewall, IDS, anti-virus system, and professional network management software can provide. The products are useful to monitor management blind spots, provide security integration and linkage with other security equipment and alert triggering.

Linkdood Endpoint Protection (LEP) has five functional modules to provide comprehensive security management service. The five modules consist of:

1. Basic product module.

2. Endpoint management module.

3. Endpoint security management module.

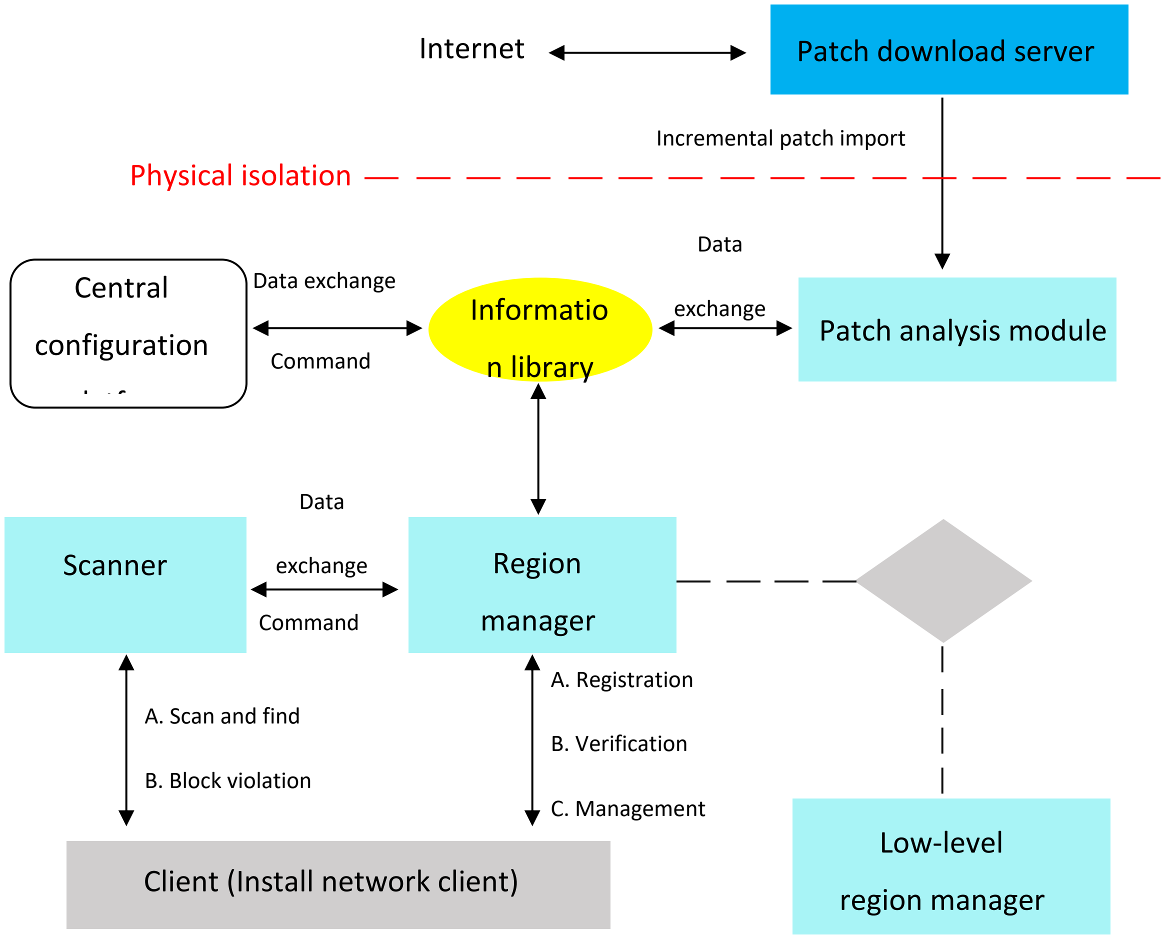
4. Network host operation module.

5. Invalid outward connection management module.

Deployment and Management Framework (LAN)

LEP stores device information of network clients in a database. The server side application requires the installation of a system database, web management platform and region manager software. Clients are required to undergo a registration process before being able to use LEP. The registration process will request for the user to input certain information such as username, department, contact information and etc. Hardware and software information of the endpoint is automatically retrieved from the endpoint by the LEP client. The information will be stored in the database for the network administrator's future reference. The region manager functions primarily to provide real-time push of policies created by the network administrators. Additionally, network administrators are also able to push system patches, commands as well as files to a group or a specific endpoint that has LEP installed. The region manager also functions to detect malicious behavior based on the predefined policies and enforces the policies on the endpoint. Upon successful deployment of LEP and network clients, the entire system is managed through the WEB management platform. An IP address is assigned for region manager and the scanner. A centralized management which has a cascade style architecture for multiple regions can be configured for large-scale organizations with multiple LAN or WAN across wide physical regions. Using the cascade style architecture eases the lower-level management of the system and is able to link all the equipment information from a lower level to the higher-level management database. This allows the higher-level management to monitor the equipment status of devices in the entire network.

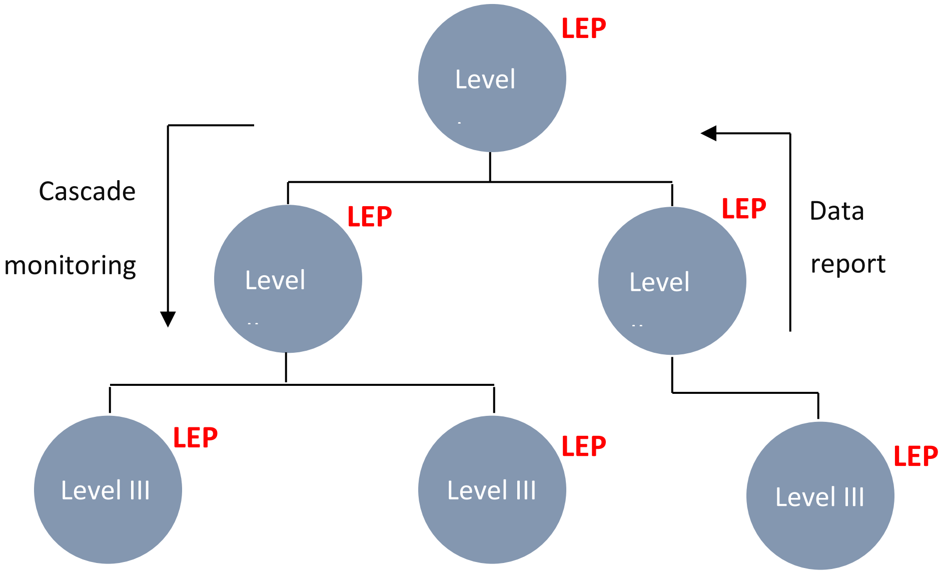
Multiple region managers are allowed to be installed in a network. Each region manager manages network clients in a certain range. Each region manager can have more than one scanner, providing segmented scanning of the local network and checking network client registration in a timely manner.



Logical Diagram of System

Deployment and Management Framework (WAN)

Large-scale multiple LAN or WAN across regions may utilize LEP to provide multiple region with a cascaded centralized management architecture. Deployment with this architecture suits network scenarios that are segregated into multiple segments. Statistics and alarm information from lower level is able to be seen by upper level management. This provides centralized control over the entire network.



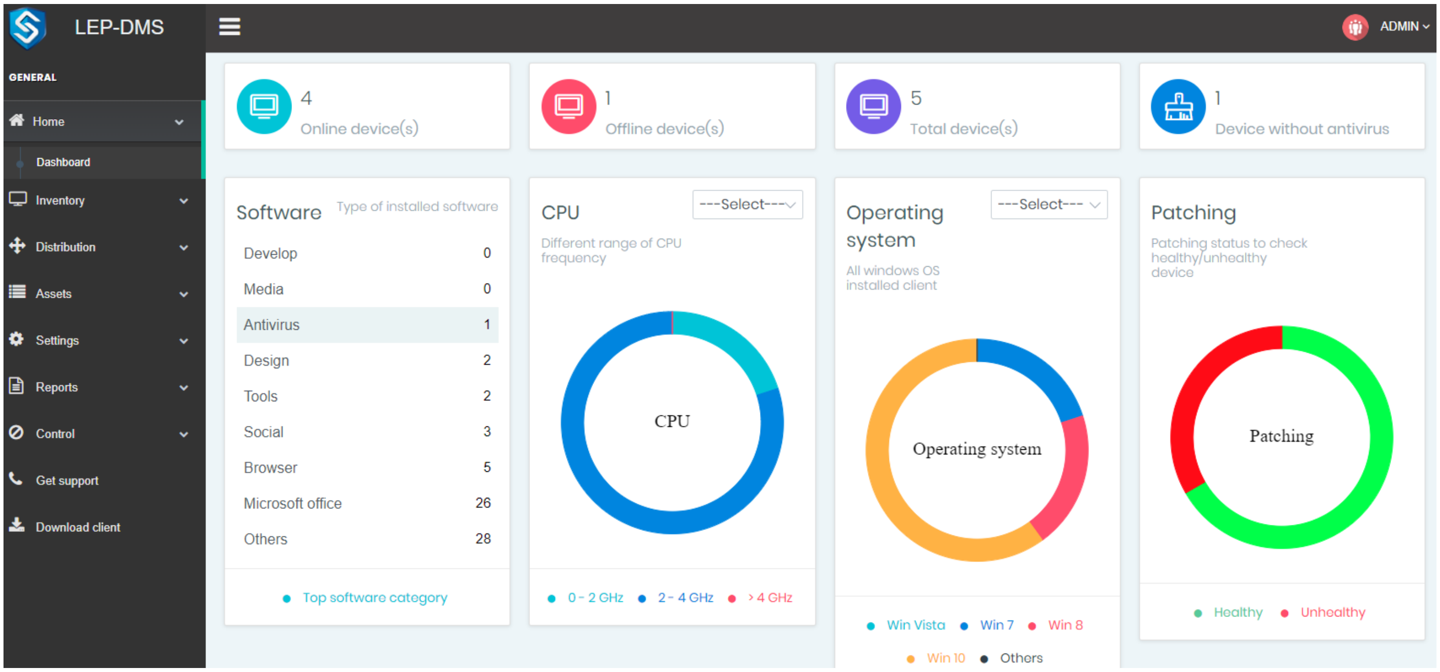
System Security Design

1. Hierarchical management: the system supports hierarchical management by administrators to allow different administrators to manage different content. Administrator's rights are divided into authorization rights, management rights and auditing rights. This feature enhances security, reliability, and suitability of authorizing many roles involved in monitoring.
2. Protection of communicated data: Data is encrypted when transmitted between components of the system. Network client and server communicate with each other using two-way authentication mechanism to prevent illegal access of computers with similar client installed into the network. This also prevents unverified clients from communicating with the server.
3. Self-protection mechanism at client application: The client application comes with a self-protection mechanism to prevent users from stopping or uninstalling without authorization.
4. Server security design: The LEP server has a self-protection function to ensure that the security of the LEP server and is able to operate normally even when IP address is maliciously modified. When computers in the network maliciously change IP address or MAC address to cause conflict with LEP's server, the server will not be blocked out of the network. Additionally, only endpoints which are performing the malicious attacks will be automatically blocked without affecting the normal operation of the server.
5. Provide rights management system: Assign authority into separates user rights group, namely: system auditor, system administrators, and system operator.
6. System logs: Audit and operation audit to ensure stable and accountable operation of the system.

Function Module

Dashboard Overview

LEP-DMS is a responsive web interface that fits all the screen resolutions. The dashboard provides an overview of all the endpoint information that visually tracks, analyzes, and monitors the health of endpoints, installed software, resource monitoring, and patch status.



4 Online device(s)

1 Offline device(s)

5 Total device(s)

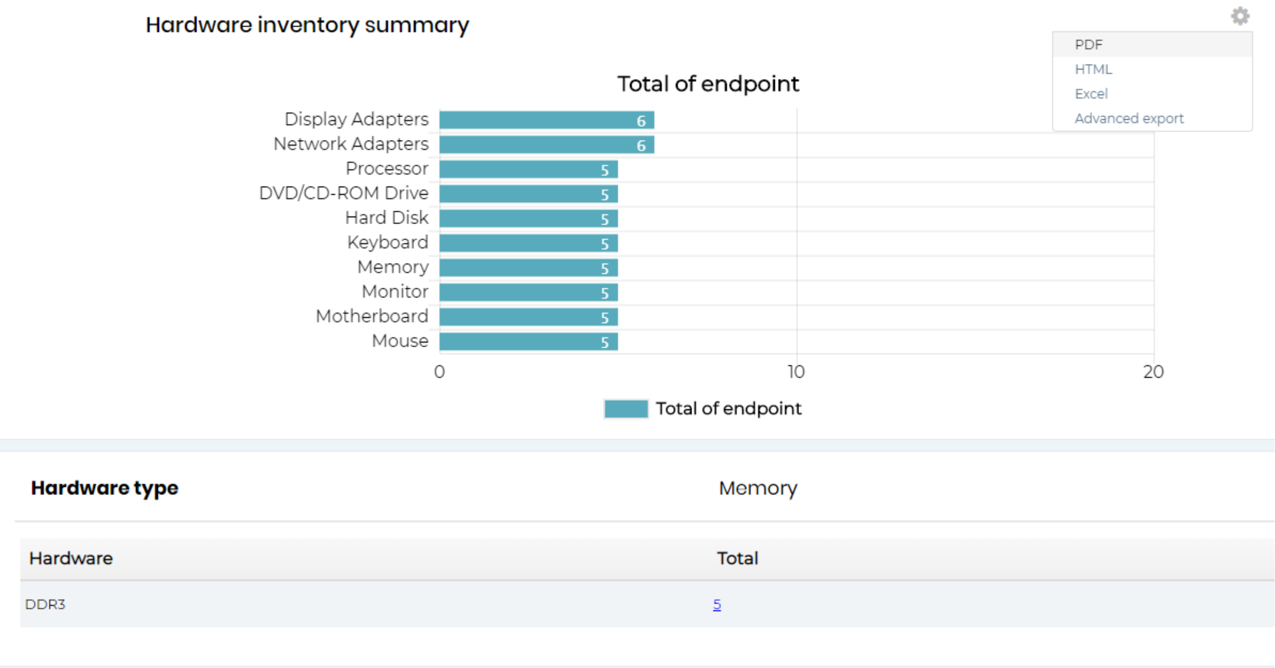
1 Device without antivirus

Software — Type of installed software

Develop	0
Media	0
Antivirus	1
Design	2
Tools	2
Social	3
Browser	5
Microsoft office	26
Others	28

Hardware Asset Management

An automation system to collect and monitor the endpoint's hardware and software information. IT administrator can automate this task in LEP-DMS asset management instead of doing the manual checking and compilation that can save up the time and reduce the cost. The hardware asset management aim to provide the details of the hardware assets by hardware type, name, OS, memory type, disk usage and etc. All the hardware information can be export in report type PDF, HTML, EXCEL.

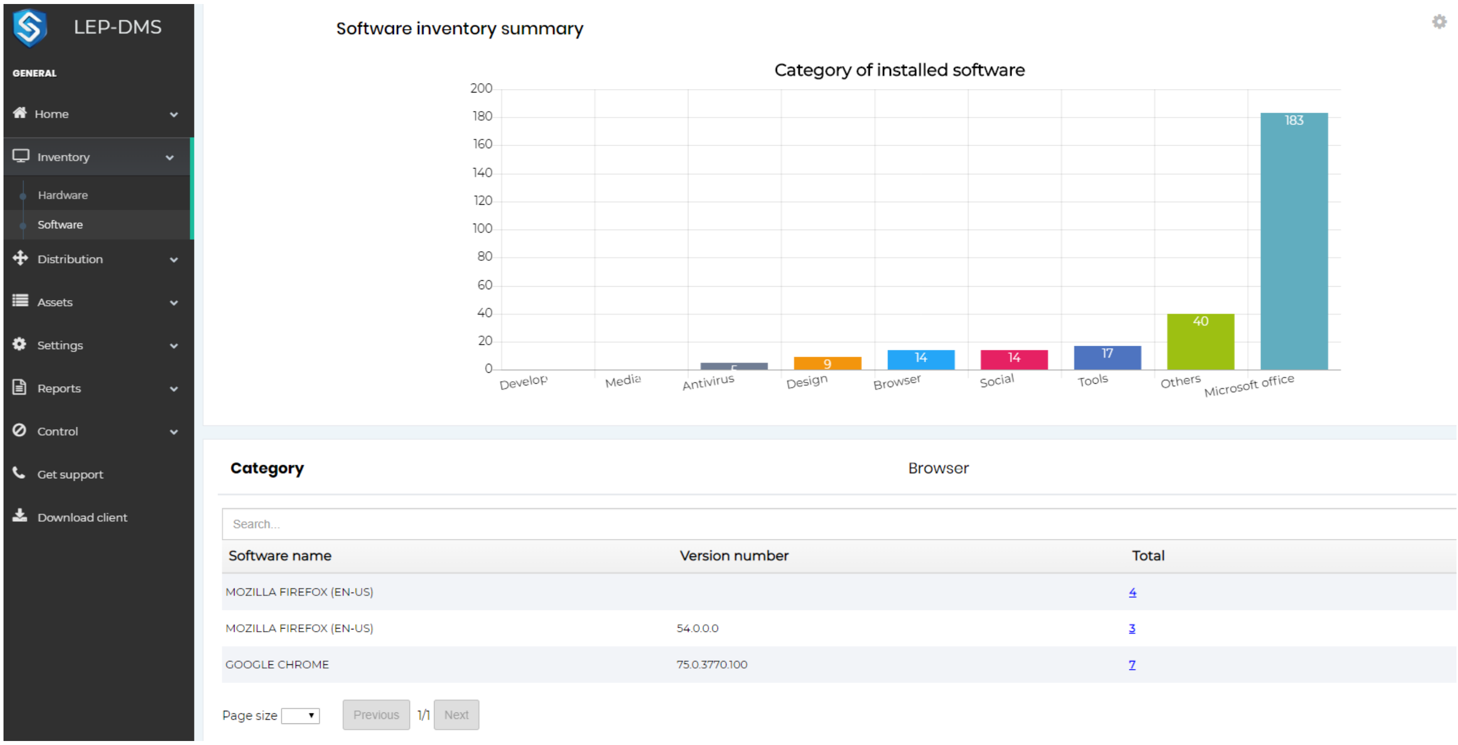


Hardware type	Memory

Hardware	Total
DDR3	5

Software Asset Management

Software asset management collecting and keeping a record of all the installed software from endpoints and categorized into the top 10 software types visually display in the bar graph. The software information is sort by type, data, installed date, version number and other related data of software installations.

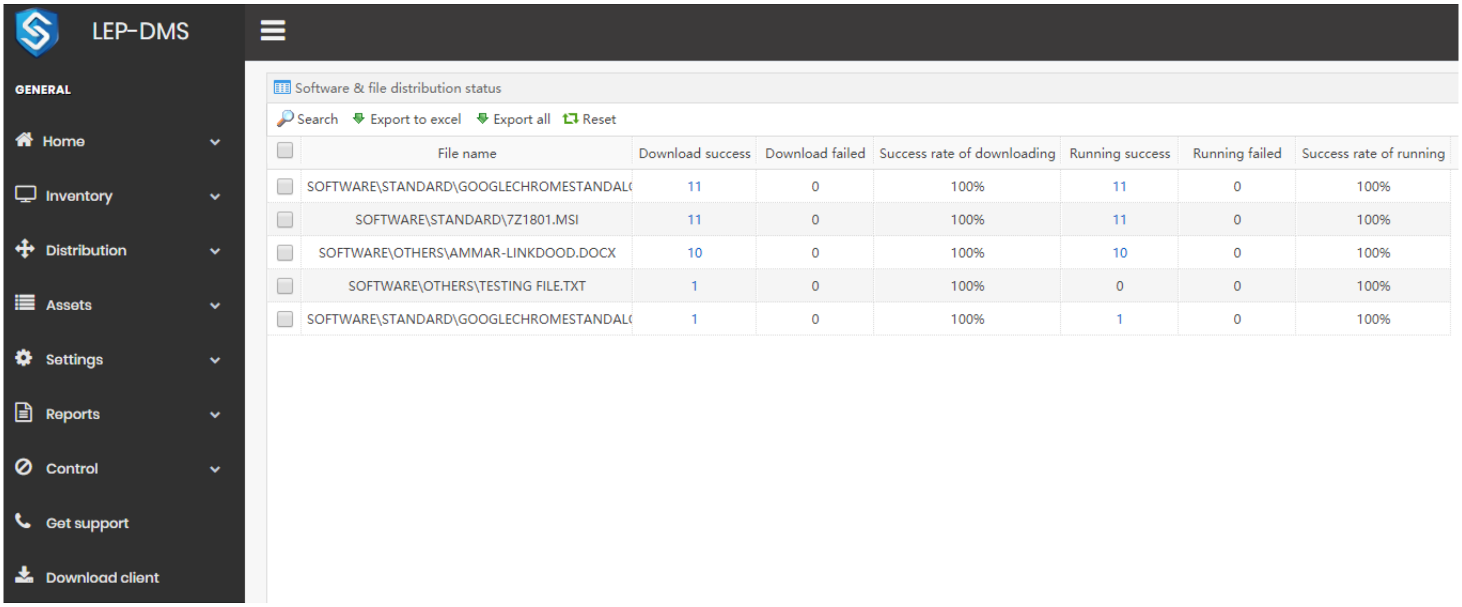


Category	Browser

Software name	Version number	Total
MOZILLA FIREFOX (EN-US)		4
MOZILLA FIREFOX (EN-US)	54.0.0.0	3
GOOGLE CHROME	75.0.3770.100	7

Software Distribution and Update

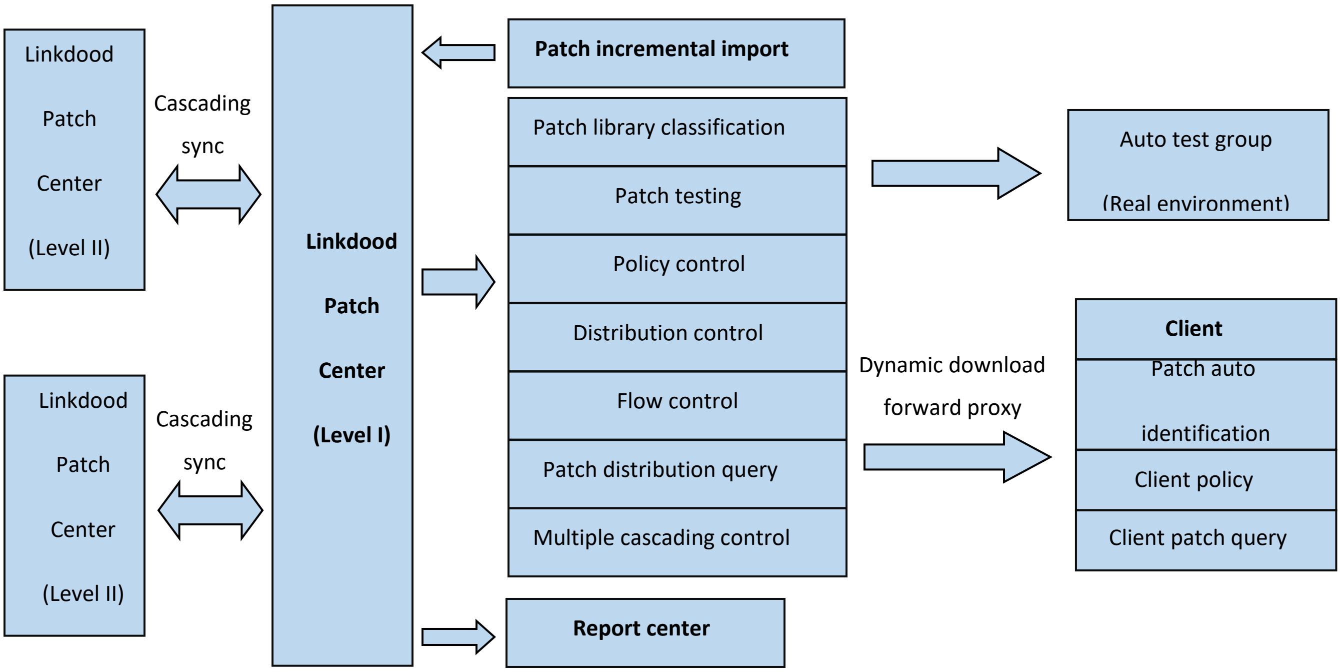
LEP-DMS can automate the software or file distribution, install and update. IT administrator is able to perform silent install software by inserting the necessary parameters to execute the files. This reduces the workload of network managers. The status of software installation is reported in real-time, this allows IT administrator to keep track of the installation status.



□	File name	Download success	Download failed	Success rate of downloading	Running success	Running failed	Success rate of running
□	SOFTWARE\STANDARD\GOOGLECHROMESTANDAL(	11	0	100%	11	0	100%
□	SOFTWARE\STANDARD\7Z1801.MSI	11	0	100%	11	0	100%
□	SOFTWARE\OTHERS\AMMAR-LINKDOOD.DOCX	10	0	100%	10	0	100%
□	SOFTWARE\OTHERS\TESTING FILE.TXT	1	0	100%	0	0	100%
□	SOFTWARE\STANDARD\GOOGLECHROMESTANDAL(	1	0	100%	1	0	100%

Windows Patching

LEP's patch distribution management system is specially developed to fulfill the needs of governmental and organizations. LEP supports two ways to automatically download any required patches. After verifying the patch file, the server will distribute patches through the patch distribution management center. Endpoints will then either automatically or manually install the patches.

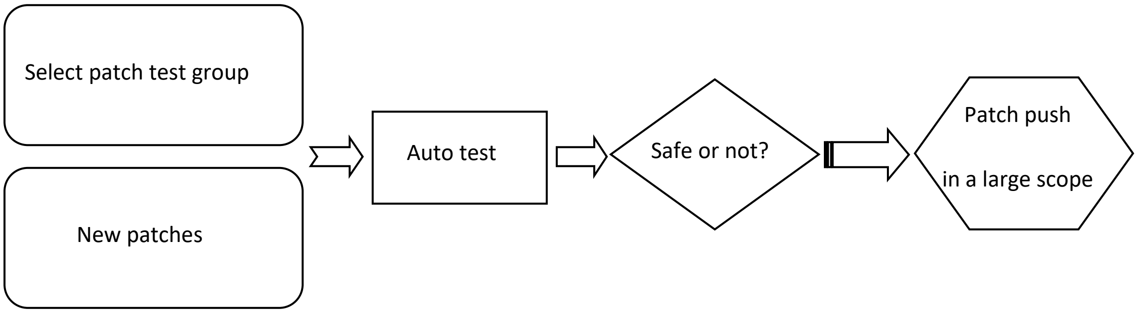

Linkdood Patch Center (Level II)
Cascading sync
Linkdood Patch Center (Level II)
Cascading sync
Linkdood Patch Center (Level I)
Patch incremental import
Patch library classification
Patch testing
Policy control
Distribution control
Flow control
Patch distribution query
Multiple cascading control
Report center
Auto test group (Real environment)
Dynamic download forward proxy
Client
Patch auto identification
Client policy
Client patch query

LEP is compatible across most Windows Operating System versions including Windows 9X, Windows 2000, Windows NT, Windows ME, Windows XP, Windows Vista, Windows 7, Windows 8 and etc.

The use of customizable index files ensures that the structure of patch index is extendable and editable. The structure can be edited to support non-Microsoft system patches, database patches as well as a wide variety of user application software patches.

Automatic Patch Testing

Certain applications or program version may require a custom patching method. Linkdood Technology uses a testing method that mimics the real environment. In the first step, network administrators will choose some endpoints to be used for testing. Patches imported will be implemented in these selected computers for testing purposes. If the patch does not negatively affect the computer, network administrators can push the patch to all the computers.



Linkdood Technology’s patching management provides powerful patch inspection, distribution, installation and other remote access functions. Network administrators are able to inspect the installation status of the patch and remotely install patches for clients that have yet to install the patch.

The system automatically inspects and maintains the OS and other applications that are installed on the client side. The system automatically collects relevant endpoint information and distributed specific patches to endpoints.

Patching Rollback

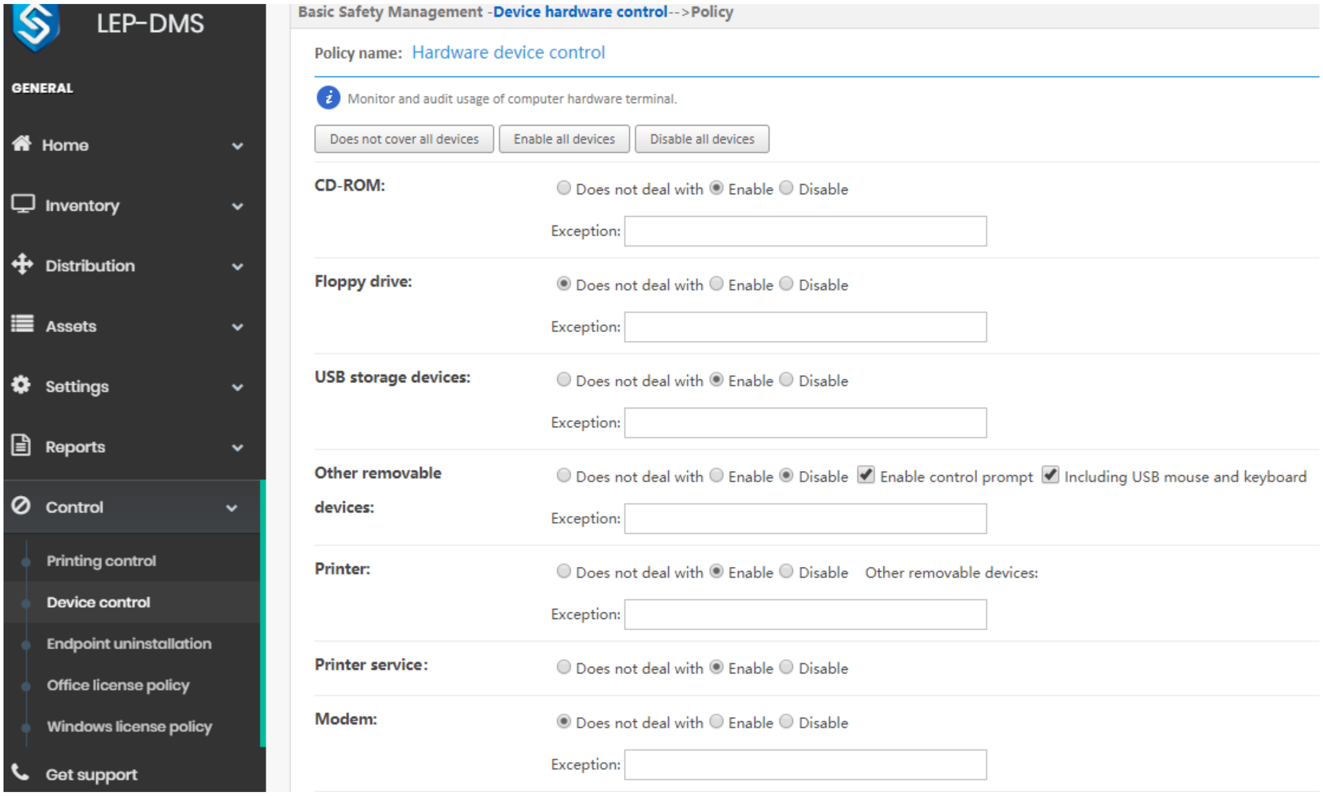
IT Administrators may rollback a patch where certain patch incompatible with system that can cause blue screen.

Hardware Control

LEP-DMS is able to limit the scope of hardware device usage to ensure that endpoint users do not perform any dangerous action. This policy help organization to avoid unwanted lost from data leakage or malware injection. IT administrator allow to distribute this policy based on the department or selected endpoints. This allow IT administrator to control all the IT assets in the network by disable them. LEP-DMS can be enabling or disabling the following hardware device:-

- CD-ROM
- Flopp Drive
- USB Storage Device

- Other Removable Device
- Printer
- Printer Service
- Modem
- Serial Port
- Parallel Port
- 1394 Controller
- Infrared Device
- Bluetooth Device
- PCMCIA Card
- Tape Drive
- SCSI Device
- Wireless Network Card
- Cable Network Adapter
- Image Equipment
- Read Card Device
- Disable Mobile
- PPPOE Protocol



Basic Safety Management -Device hardware control-->Policy

Policy name: Hardware device control

Monitor and audit usage of computer hardware terminal.

CD-ROM: ○ Does not deal with ● Enable ○ Disable
Exception:

Floppy drive: ● Does not deal with ○ Enable ○ Disable
Exception:

USB storage devices: ○ Does not deal with ● Enable ○ Disable
Exception:

Other removable devices: ○ Does not deal with ○ Enable ● Disable ☑ Enable control prompt ☑ Including USB mouse and keyboard
Exception:

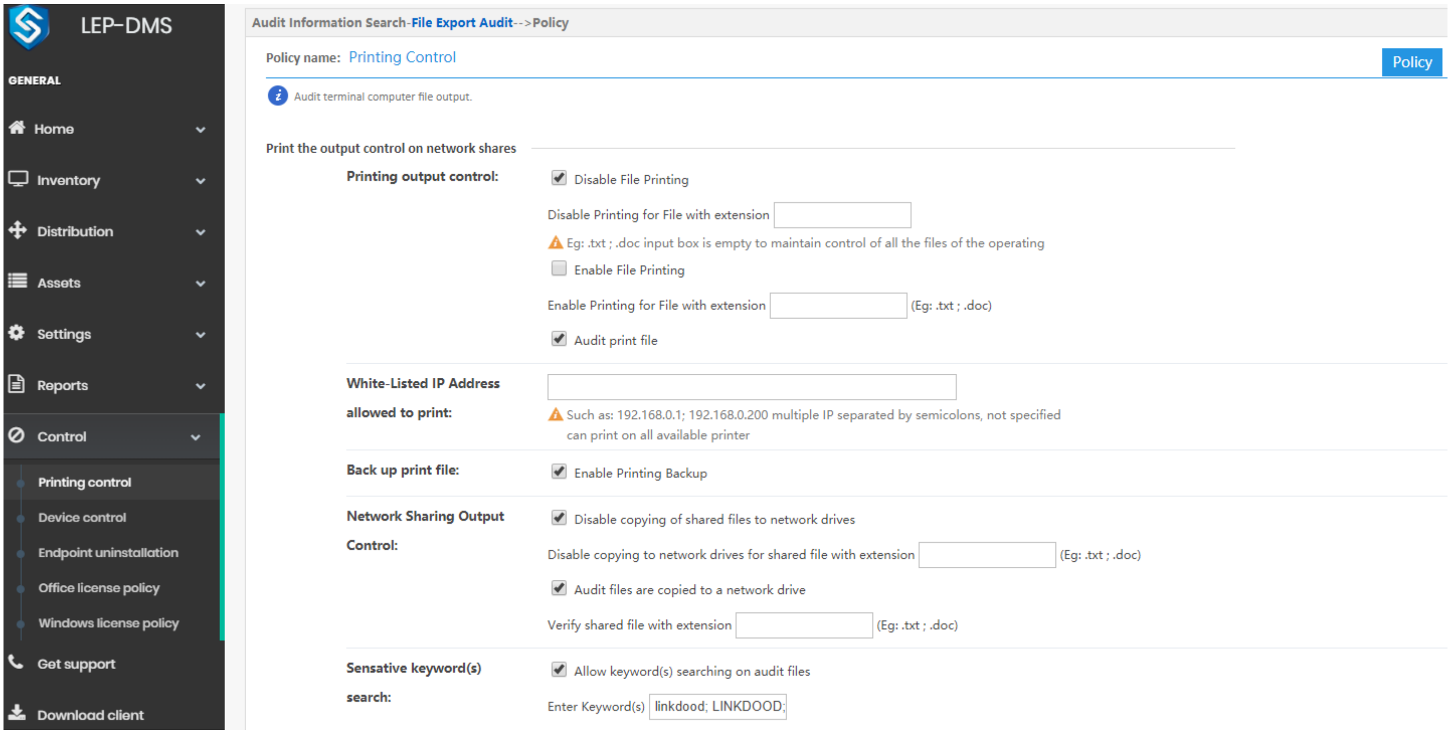
Printer: ○ Does not deal with ● Enable ○ Disable Other removable devices:
Exception:

Printer service: ○ Does not deal with ● Enable ○ Disable

Modem: ● Does not deal with ○ Enable ○ Disable
Exception:

Printing Control

IT administrator is able to monitor and control the printing activities and control the file operations to prevent users from leaking out the sensitive information. Policy can be set to prohibit endpoint copy file into shared drive. IT administrator able to pre-set the sensitive word, file will prohibit to print or copy to shared drive when a sensitive word found.



Audit Information Search-**File Export Audit**-->Policy

Policy name: Printing Control

Audit terminal computer file output.

Print the output control on network shares

Printing output control:

☑ Disable File Printing

Disable Printing for File with extension

Eg: .txt ; .doc input box is empty to maintain control of all the files of the operating

☐ Enable File Printing

Enable Printing for File with extension (Eg: .txt ; .doc)

☑ Audit print file

White-Listed IP Address allowed to print:

Such as: 192.168.0.1; 192.168.0.200 multiple IP separated by semicolons, not specified can print on all available printer

Back up print file:

☑ Enable Printing Backup

Network Sharing Output Control:

☑ Disable copying of shared files to network drives

Disable copying to network drives for shared file with extension (Eg: .txt ; .doc)

☑ Audit files are copied to a network drive

Verify shared file with extension (Eg: .txt ; .doc)

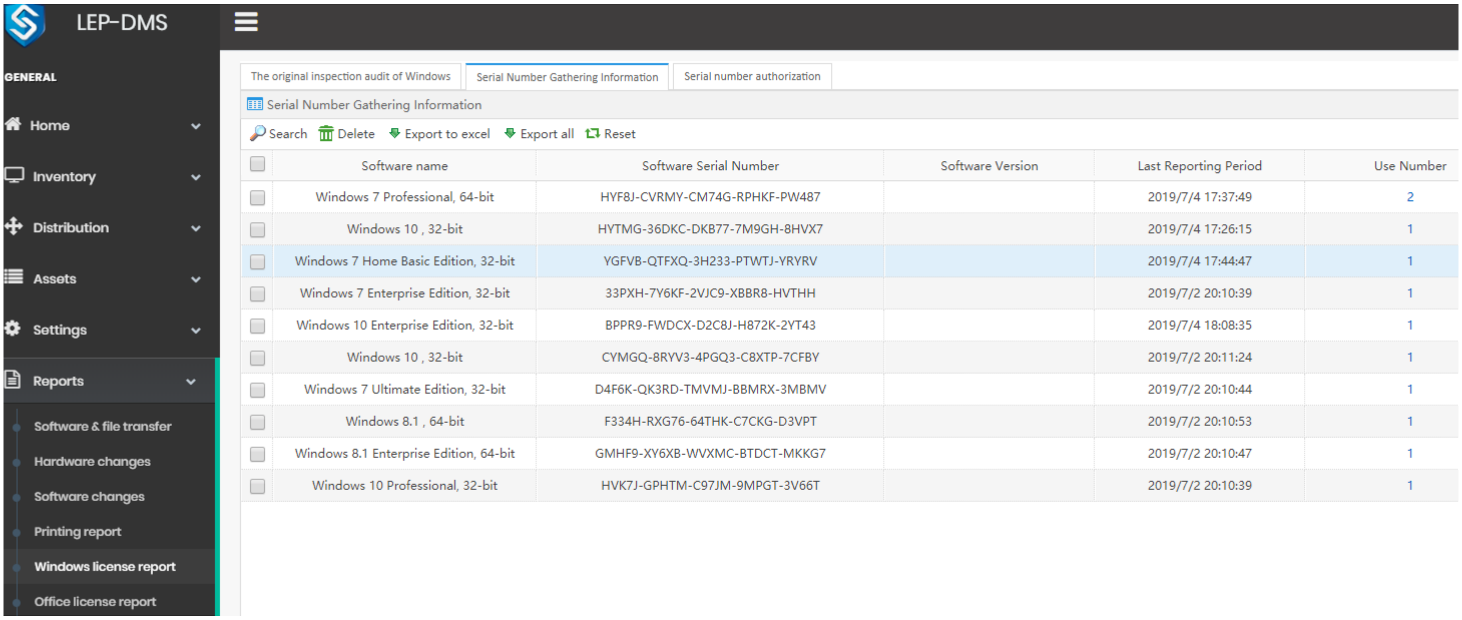
Sensative keyword(s) search:

☑ Allow keyword(s) searching on audit files

Enter Keyword(s) linkdood; LINKDOOD;

Genuine Windows and Microsoft Detection

LEP-DMS able to collect the license number of Windows and Microsoft products and listed in audit report. Certain action will be perform when endpoint found that using illegal license. This policy is set to ensure that the company assets are using legal license for Windows and Microsoft products.



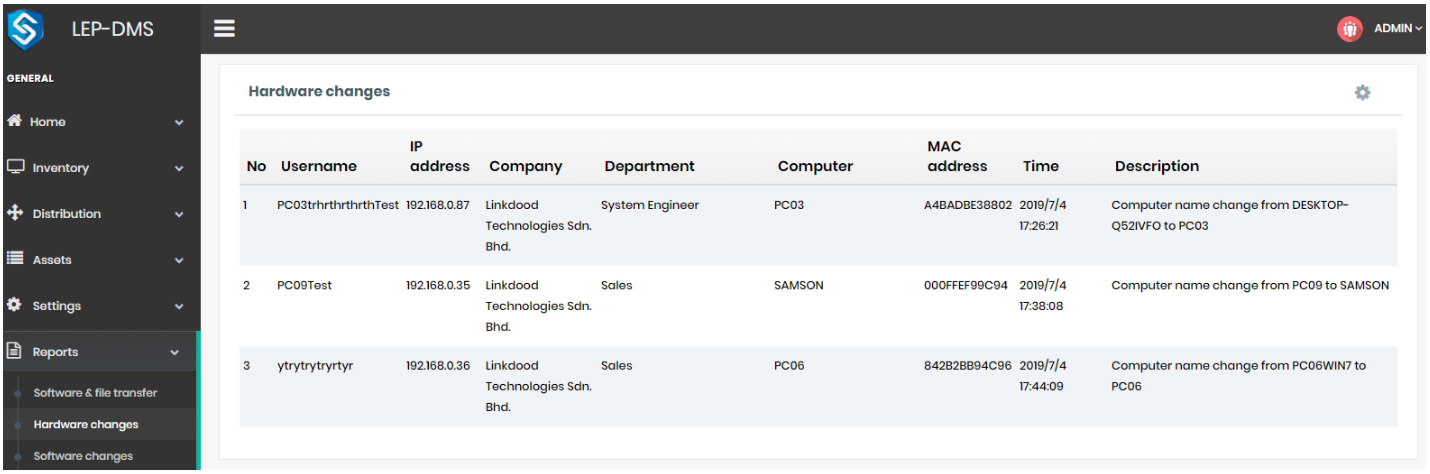
Serial Number Gathering Information

□	Software name	Software Serial Number	Software Version	Last Reporting Period	Use Number
□	Windows 7 Professional, 64-bit	HYF8J-CVRMY-CM74G-RPHKF-PW487		2019/7/4 17:37:49	2
□	Windows 10 , 32-bit	HYTMG-36DKC-DKB77-7M9GH-8HVX7		2019/7/4 17:26:15	1
□	Windows 7 Home Basic Edition, 32-bit	YGFVB-QTFXQ-3H233-PTWTJ-YRYRV		2019/7/4 17:44:47	1
□	Windows 7 Enterprise Edition, 32-bit	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH		2019/7/2 20:10:39	1
□	Windows 10 Enterprise Edition, 32-bit	BPPR9-FWDCX-D2C8J-H872K-2YT43		2019/7/4 18:08:35	1
□	Windows 10 , 32-bit	CYMGQ-8RYV3-4PGQ3-C8XTP-7CFBY		2019/7/2 20:11:24	1
□	Windows 7 Ultimate Edition, 32-bit	D4F6K-QK3RD-TMVMJ-BBMRX-3MBMV		2019/7/2 20:10:44	1
□	Windows 8.1 , 64-bit	F334H-RXG76-64THK-C7CKG-D3VPT		2019/7/2 20:10:53	1
□	Windows 8.1 Enterprise Edition, 64-bit	GMHF9-XY6XB-WVXMC-BTDCT-MKKG7		2019/7/2 20:10:47	1
□	Windows 10 Professional, 32-bit	HVK7J-GPHTM-C97JM-9MPGT-3V66T		2019/7/2 20:10:39	1

Hardware or Software Changes

LEP-DMS will notify IT administrator for the following events:-

- Any hardware that was new added or removed from the endpoints.
- Modification on the computer name.
- Any software that was new installed or uninstalled from the endpoints.



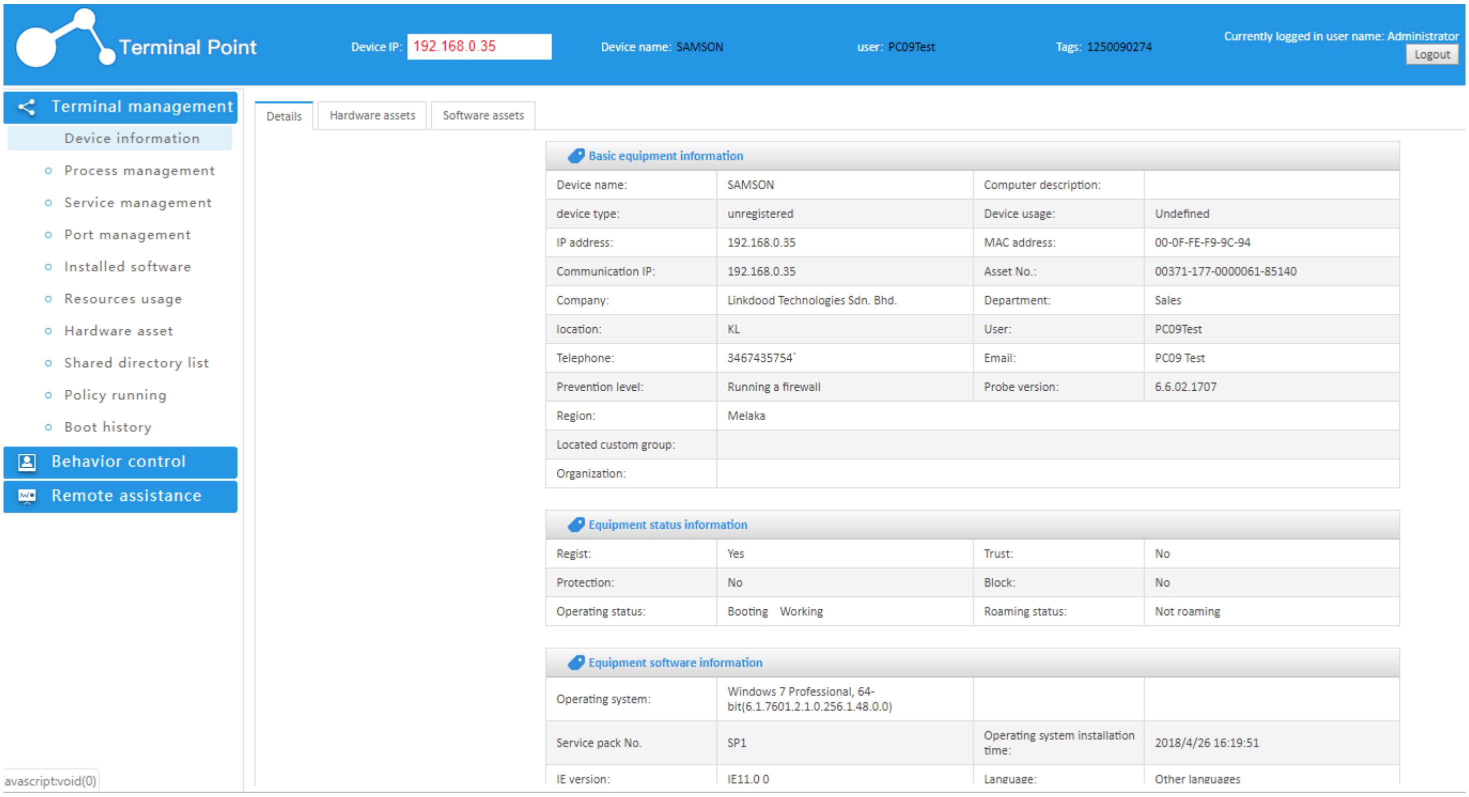
Hardware changes

No	Username	IP address	Company	Department	Computer	MAC address	Time	Description
1	PC03trhrthrthrthTest	192.168.0.87	Linkdood Technologies Sdn. Bhd.	System Engineer	PC03	A4BADBE38802	2019/7/4 17:26:21	Computer name change from DESKTOP-Q52IVFO to PC03
2	PC09Test	192.168.0.35	Linkdood Technologies Sdn. Bhd.	Sales	SAMSON	000FFEF99C94	2019/7/4 17:38:08	Computer name change from PC09 to SAMSON
3	ytrytrytryrtyr	192.168.0.36	Linkdood Technologies Sdn. Bhd.	Sales	PC06	842B2BB94C96	2019/7/4 17:44:09	Computer name change from PC06WIN7 to PC06

Remote Control

LEP-DMS allow IT administrator conduct a detailed monitoring and auditing of the client in a point-to-point manner. Monitoring and auditing functions include the following:-

1. Device Information: Endpoint's basic information, hardware assets and software assets.
2. Process Management: Shows the list of running processes on endpoint and terminate unnecessary processes.
3. Service Management: Shows the list of running services and remotely execute or terminate services according to requirements.
4. Port Management: Shows the list of listening port and terminate the unnecessary ports.
5. Installed Software: Shows the list of installed software on the endpoint.
6. Resource Usage: Shows the CPU usage, memory size / usage and size / usage of system HDD.
7. Shared Directory List: Check the shared directory of the current endpoint.
8. Policy Running: Check the running policy that distributed to endpoint.
9. Boot History: Check for endpoint's PC boot up or turn off time.
10. Message Notification: Send message to the user which may or may not require feedback confirmation from user.
11. Execute Program: Run the application remotely.
12. Network Configuration: Check for IP address, MAC address, subnet mask and gateway information of network endpoint as well as remotely perform modification to the endpoint user's IP address.
13. Network Termination: Prohibit endpoint from using network.
14. Network Restoration: Restore endpoint from using network.
15. Synchronization: Resync the endpoint's data information to server.
16. Device Control: Block/Restore from using keyboard and mouse.
17. Update Information: Update endpoint registered information.
18. Uninstall Endpoint: Uninstall endpoint remotely.
19. Shutdown Endpoint: Restart/Shutdown endpoint remotely.
20. Remote Support: Provide remote to endpoint to solve technical issues immediately.



Device IP: 192.168.0.35 Device name: SAMSON user: PC09Test Tags: 1250090274

Basic equipment information

Device name:	SAMSON	Computer description:	
device type:	unregistered	Device usage:	Undefined
IP address:	192.168.0.35	MAC address:	00-0F-FE-F9-9C-94
Communication IP:	192.168.0.35	Asset No.:	00371-177-0000061-85140
Company:	Linkdood Technologies Sdn. Bhd.	Department:	Sales
location:	KL	User:	PC09Test
Telephone:	3467435754`	Email:	PC09 Test
Prevention level:	Running a firewall	Probe version:	6.6.02.1707
Region:	Melaka		
Located custom group:			
Organization:			

Equipment status information

Regist:	Yes	Trust:	No
Protection:	No	Block:	No
Operating status:	Booting Working	Roaming status:	Not roaming

Equipment software information

Operating system:	Windows 7 Professional, 64-bit(6.1.7601.2.1.0.256.1.48.0.0)		
Service pack No.	SP1	Operating system installation time:	2018/4/26 16:19:51
IE version:	IE11.0 0	Language:	Other languages

Others common add on features

- Resource Monitoring
- Internet Behavior Control
- Network Monitor
- Directory Services
- File Content Checker
- Flow Control Policy
- Junk File Cleaner
- Desktop Policy Management
- Process Monitoring and Control
- Multi-level Admin Access Rights
- Enforcement Working Directories
- File Protection
- Registry Checker

Other add on customization function

- Burning Audit
- Wi-Fi Strategy
- Internet Settings Policy
- Process Execution and Protection Policy
- Screen Capture and Recording
- User Password Policy
- Energy Saving Policy
- Multi-OS Check
- Endpoint Tray Menu Policy
- Keyboard Behavior Management and Audit
- IP Binding Policy
- Antivirus Monitor
- Distribution of Portfolio Policy

Hardware Requirements

Recommended server specification:

- Core I5 3570k and above
- Hard Disk: 1TB and above
- Memory: 8GB and above
- Operating System: Microsoft Windows Server 2012 R2
- Database: Microsoft SQL server 2008 Express & 2008 R2 express
- IIS service version 7.0 or later

Recommended endpoint specification:

- Intel Pentium 4
- 60GB HDD
- 1GB RAM
- Microsoft Windows XP, Vista, 7, 8, 8.1, 10