Systemwalker Desktop Patrol V14g

User's Guide

Windows

B1WD-2703-04ENZ0(00)
March 2012

Preface

Purpose of this Guide

This guide gives an introduction to the following products, as well as functional overview and knowledge required to use them.

- Systemwalker Desktop Patrol V14g(14.2.0)

Systemwalker is a generic name for the distributed system management product provided by Fujitsu Limited.

Intended Readers

This guide is for the following readers.

- Those who are considering the installation of Systemwalker Desktop Patrol
- Those who wish to know the product of Systemwalker Desktop Patrol
- Those who wish to know functional overview of Systemwalker Desktop Patrol
- Those who wish to know what is need to use Systemwalker Desktop Patrol

To understand the contents of this guide, the following knowledge is essential.

- General knowledge regarding personnel computers
- General knowledge regarding Windows
- General knowledge regarding the Internet

Structure of this Guide

This guide consists of Chapter 1~4 and an appendix.

Chapter 1 Overview of Systemwalker Desktop Patrol

This chapter describes the positioning of Systemwalker Desktop Patrol in the Systemwalker product system, the effect of installation of Systemwalker Desktop Patrol and its features.

In addition, this chapter describes the knowledge and the concept required when using Systemwalker Desktop Patrol.

Chapter 2 Systemwalker Desktop Patrol Functions

This chapter describes functions of Systemwalker Desktop Patrol.

Chapter 3 Operating Environment

This chapter describes the necessary environment for running the Systemwalker Desktop Patrol.

Chapter 4 Link with Other Products

This chapter describes the linkage methods of Systemwalker Desktop Patrol with other products.

Appendix A Term Table

This appendix lists the items changed from Systemwalker Desktop Patrol V13.0.0.

Glossary

This glossary explains the terms used in Systemwalker Desktop Patrol.

Location of This Guide

In Systemwalker Desktop Patrol manual, location of this guide is shown as follows.

Manual Name	Contents
Systemwalker Desktop Patrol User's Guide (This Guide)	Basic knowledge of Systemwalker Desktop Patrol, such as overview, features, functions, etc.
Systemwalker Desktop Patrol Installation Guide	How to perform installation settings, change operation environment, maintain and manage Systemwalker Desktop Patrol.
Systemwalker Desktop Patrol Operation Guide: for Administrators	How to collect PC information, install security patches, distribute software, license management, management ledger, and environment setup of Systemwalker Desktop Keeper.
Systemwalker Desktop Patrol Operation Guide: for Clients	How to install, operate and change the settings of the client side. In addition, it explains how to handle error messages output from client side.
Systemwalker Desktop Patrol Reference Manual	Commands, files and port numbers used in Systemwalker Desktop Patrol. In addition, it explains how to handle error message output from Systemwalker Desktop Patrol.

Also, the following manuals are enclosed as Systemwalker Live Help manuals. Please refer to them when you use the remote operation function (Systemwalker Live Help Function).

Manual Name	Contents
Systemwalker Live Help User's Guide	It explains how to install Systemwalker Live Help, how to use the hardware and software and set the support center. In addition, it also explains how to manage by Live Help Connection Manager.
Systemwalker Live Help Client Guide	It explains how to install, use and set Systemwalker Live Help Client.

Symbols used in this guide

This guide uses the following names, symbols and abbreviations for explications.

Symbols used in commands

This subsection describes the symbols used in the examples of commands.

Meaning of Symbols

Symbol	Meaning
[ ]	Indicates that the items enclosed in these brackets can be omitted.
l	Indicates that one of the items separated by this symbol should be selected.

Symbols used in this guide

The following symbols are used in this guide.

Meaning of Symbols

Symbol	Meaning
n	Indicates variable value.

Note

Indicates an item requires special attention.

Point

Indicates useful information.

DTP installation directory

The directory in which “Systemwalker Desktop Patrol CS”, “Systemwalker Desktop Patrol DS”, “Systemwalker Desktop Patrol AC”, “Systemwalker Desktop Patrol ADT” or “Systemwalker Desktop Patrol CT” is installed is indicated as the DTP installation directory.

Abbreviations

In this guide, the product names are abbreviated as follows.

Product Name	Abbreviation
Systemwalker Desktop Patrol CS	CS
Systemwalker Desktop Patrol DS	DS
Systemwalker Desktop Patrol AC	AC
Systemwalker Desktop Patrol ADT	ADT
Systemwalker Desktop Patrol CT	CT

In this guide, the operating system names are abbreviated as follows.

Abbreviation	Full Name
Windows Server® 2008	Microsoft® Windows Server® 2008 Foundation Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Standard without Hyper-V™ Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise
Windows Server® 2003	Microsoft® Windows Server® 2003, Standard Edition Microsoft® Windows Server® 2003, Enterprise Edition Microsoft® Windows Server® 2003, Standard x64 Edition Microsoft® Windows Server® 2003, Enterprise x64 Edition Microsoft® Windows Server® 2003 R2, Standard Edition Microsoft® Windows Server® 2003 R2, Enterprise Edition Microsoft® Windows Server® 2003 R2, Standard x64 Edition Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition
Windows® 7	Windows® 7 Enterprise Windows® 7 Ultimate Windows® 7 Professional Windows® 7 Home Premium
Windows Vista®	Microsoft® Windows Vista® Ultimate Microsoft® Windows Vista® Enterprise Microsoft® Windows Vista® Business Microsoft® Windows Vista® Home Premium Microsoft® Windows Vista® Home Basic Microsoft® Windows Vista® Ultimate 64-bit Edition Microsoft® Windows Vista® Enterprise 64-bit Edition

Abbreviation	Full Name
	Microsoft® Windows Vista® Business 64-bit Edition Microsoft® Windows Vista® Home Premium 64-bit Edition Microsoft® Windows Vista® Home Basic 64-bit Edition
Windows® XP	Microsoft® Windows® XP Professional Microsoft® Windows® XP Home Edition
Windows	Microsoft® Windows Server® 2008 Foundation Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Standard without Hyper-V™ Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2003, Standard Edition Microsoft® Windows Server® 2003, Enterprise Edition Microsoft® Windows Server® 2003, Standard x64 Edition Microsoft® Windows Server® 2003, Enterprise x64 Edition Microsoft® Windows Server® 2003 R2, Standard Edition Microsoft® Windows Server® 2003 R2, Enterprise Edition Microsoft® Windows Server® 2003 R2, Standard x64 Edition Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Windows® 7 Enterprise Windows® 7 Ultimate Windows® 7 Professional Windows® 7 Home Premium Microsoft® Windows Vista® Ultimate Microsoft® Windows Vista® Enterprise Microsoft® Windows Vista® Business Microsoft® Windows Vista® Home Premium Microsoft® Windows Vista® Home Basic Microsoft® Windows Vista® Ultimate 64-bit Edition Microsoft® Windows Vista® Enterprise 64-bit Edition Microsoft® Windows Vista® Business 64-bit Edition Microsoft® Windows Vista® Home Premium 64-bit Edition Microsoft® Windows Vista® Home Basic 64-bit Edition Microsoft® Windows® XP Professional Microsoft® Windows® XP Home Edition
IIS	Internet Information Services 6.0 Internet Information Services 7.0 Internet Information Services 7.5
IE	Microsoft® Internet Explorer® 6.0 Windows® Internet Explorer® 7 Windows® Internet Explorer® 8 Windows® Internet Explorer® 9

Export Management Regulations

Our documentation may include special technology based on Foreign Exchange and Foreign Trade Control Law. In such a case, to export the relevant documentation(s) or to provide any overseas resident with the relevant documentation(s), permission based on the above law is necessary.

Trademark

Intel, Intel vPro and Centrino are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows NT, Windows Vista, Windows Server, Active Directory and names or product names of other Microsoft's products are registered trademarks of Microsoft Corporation in the United States and other countries

Oracle is the registered trademark of Oracle Corporation.

Symantec, the Symantec logo, and Norton AntiVirus are registered trademarks of Symantec Corporation in the United States.

VirusBuster is registered trademark of Trendmicro Ltd.

VirusScan and NetShield are trademarks or registered trademarks of Network Associate, Inc. or its affiliates.

QND are trademarks of Quality Ltd.

NETM/DM is trademark of Hitachi Ltd.

Other product names described in this document are trademarks or registered trademarks

Screen shots are used in accordance with Microsoft Corporation's guidelines.

March 2012

First edition, March 2012

Contents

Chapter 1 Overview of Systemwalker Desktop Patrol

This chapter describes the positioning of Systemwalker Desktop Patrol in the Systemwalker suite, the benefits of installing Systemwalker Desktop Patrol and an overview of its features.

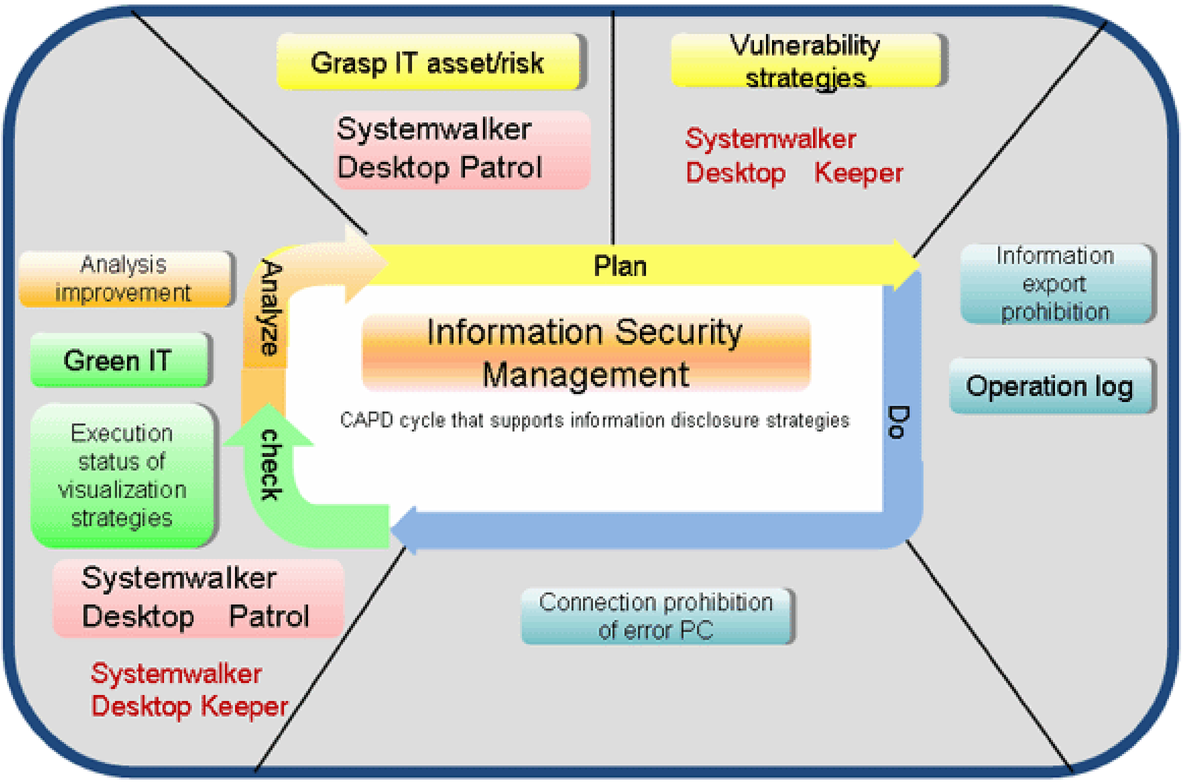
1.1 Product Positioning

This section describes the concept of Systemwalker Desktop series and the positioning of Systemwalker Desktop Patrol.

Definition of the Systemwalker Desktop Series

By mastering assets and according to services and environmental risks, Systemwalker Desktop series can take measures such as adding application security patches, checking security settings, encrypting files, controlling PC operations, collecting/analyzing account, controlling file operations, and supporting the CAPD period for sustainable improvement, and thus implementing the green IT plan.

Based on the previous security plan, Systemwalker Desktop V14g series implements the green IT plan that decreasing the CO2 emissions by saving electricity and reducing paper costs.


Grasp IT asset/risk
Systemwalker Desktop Patrol
Vulnerability strategies
Systemwalker Desktop Keeper
Analysis improvement
Green IT
Execution status of visualization strategies
Systemwalker Desktop Patrol
Systemwalker Desktop Keeper
Analyze
check
Plan
Do
Information Security Management
CAPD cycle that supports information disclosure strategies
Information export prohibition
Operation log
Connection prohibition of error PC

Positioning of Systemwalker Desktop Patrol

Systemwalker Desktop Patrol is a set of IT assets management software applicable for the section with dozens of PCs or large-scale system like a company. Systemwalker Desktop Patrol ensures the security, implements the Total Cost of Ownership (TCO) reduction by decreasing the PC power consumption and using the software assets more effectively, and improves the efficiency by downloading files, and control the client remotely.

Besides, Systemwalker Desktop Patrol manages the collected information and IT asset information managed by external programs like Excel, implementing the complete control of IT (ensures the normal running of the system and audits the system).

Green IT Plan

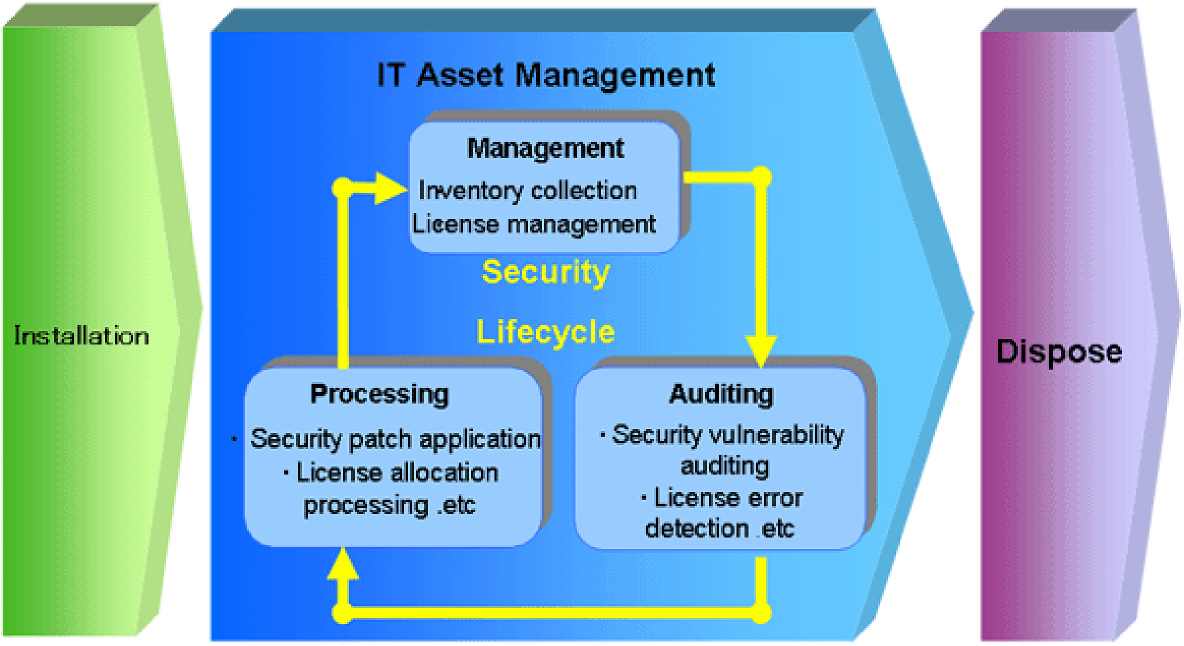
Because of the severe environmental problems, enterprises must enhance their environmental protection consciousness and improve the energy saving methods. Based on the previous client management function, Systemwalker Desktop Patrol provides the function of decreasing the PC power consumption, supporting green IT in office, and reducing the CO2 emissions.

According to the usage of the company or section, set the power saving policy and modify the PC settings that violate the policy.

Security Management

The internet is necessary for nowadays business. To prevent the disclosure of confidential and personal information, and to protect the PC from being illegally accessed or infected by virus become the most important topic. The Systemwalker security management solution prevents the important data and verified information from disclosure, and manages all types of security products uniformly, thus reducing burdens of security operations.

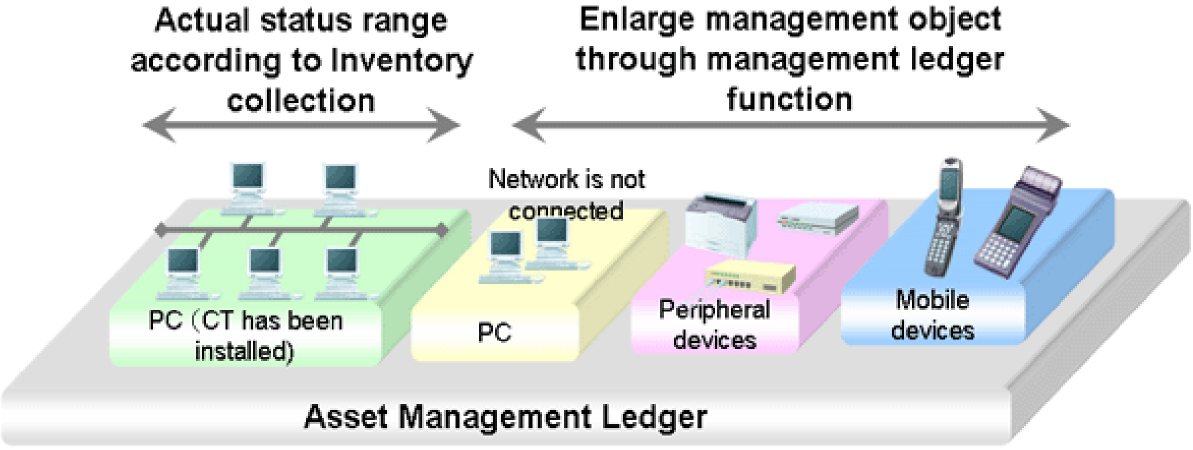
The anti-disclosure function in Systemwalker Desktop Patrol V14g is enhanced to protect the IT assets. The life cycle from software installation to discard can be protected.



Account-based Assets Management

With the popularity of the PCs in the enterprise, administrators must know the environment where the assets are used to optimize the TCO, cope with illegal duplication and virus, and make security and budget plans. The Systemwalker assets management solution masters the actual asset information and reduces costs by effectively using idle licenses and centralized purchasing.

Systemwalker Desktop Patrol V14g provides not only the client security management function, but also the assets management function. Therefore, assets management, usage management, and security auditing of the PC or equipment can be supported.


Actual status range according to Inventory collection
Enlarge management object through management ledger function
Network is not connected
PC (CT has been installed)
PC
Peripheral devices
Mobile devices
Asset Management Ledger

1.2 Features

For an enterprise, IT investment is strategic and necessary. In the IT investment, apart from the hardware and software costs, there are also invisible costs such as troubleshooting, hardware storage location management, software installation, license management, security patch application, and information disclosure prevention. It is hoped that the investment is equivalent to the effect.

In the past few years, PC importing grows rapidly, and the PCs are managed by users. Therefore, if the PCs are infected by virus or the licenses are audited, administrators may not know exactly what the problem is or cannot go on site. They need a tool that can simply solve the problems.

What's more, PC assets management and client security management are important for enterprises.

The PC assets management supports management on asset information account, lease contracts, and company asset usage. The large quantity of PCs brings more and more burden. Therefore, a tool that can simply manage those services is required.

The tool adds the internal management obligation. For the auditing standard of the internal management, the tool searches for the effectiveness and efficiency of services, credibility of financial reports, and protects assets.

Systemwalker Desktop Patrol has the following features.

Easy Installation

Systemwalker Desktop Patrol can be installed easily even without the expert's help.

Adaptability to Various Environments

Systemwalker Desktop Patrol supports customers from small-scale system with several PCs to large-scale system like a company.

PC Assets Managment

- Easily know the availability of hardware and software.
- Easily manage software licenses.

Unified IT Assets Management

Systemwalker Desktop Patrol allows you to see the setup place, quantity, and actual usage of IT assets information such as PCs, all-in-one machine, and printers, and reduces costs.

Administrators can register/update/delete asset information and manage resumes according to the automatically collected inventory information.

Periodical Check Based on Assets Management Ledger

Systemwalker Desktop Patrol detects the device loss through the periodical check, and strives for protecting the IT assets. By knowing the actual situation in the short time, you can review and use the assets, and make proper investments.

Maintain Power Saving Status

Administrators can set the power saving policy for all PCs uniformly according to the usage of the whole company or a section.

If a user modifies the power saving policy, the PC will prompt a warning or forcibly modify the settings to maintain the power saving status.

Retain and Enhance Security

- Installation of security patches and virus definition files can be easily verified.
- A security patch can be automatically obtained and installed. Administrators can install the security patches by force on PCs that is lack of patches.
- Security status of the system and login users can be easily checked. If a user modifies the security policy, the PC will prompt a warning or forcibly modify the settings to maintain the security.

Reduce Workload on Administrator

- End-to-end management can be easily performed when a problem occurs.
- Administrator can remotely operate a PC.
- Most management functions can be performed from a Web browser.

1.3 Added and Modified Functions in V14.2.0

This section describes the added and modified functions in Systemwalker Desktop Patrol V14.2.0.

Support Mobile PC Operation

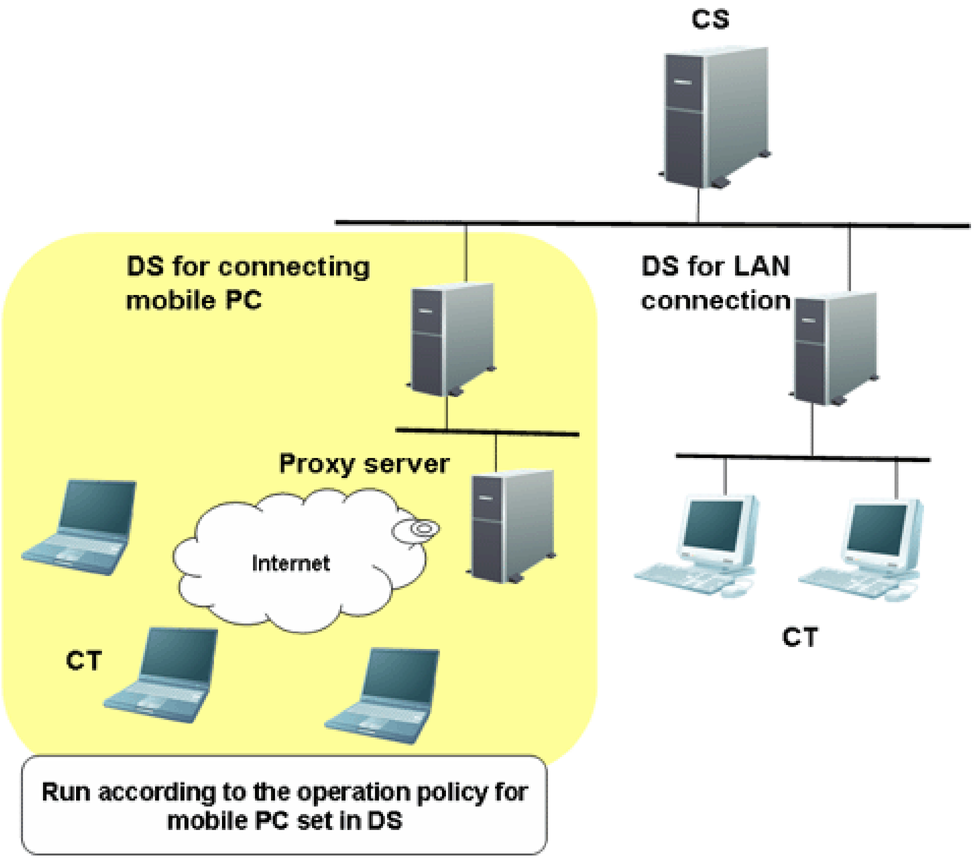
When performing mobile operation by connecting from external used VPN (Virtual Private Network) to the internal part of company, the following operating policies can be set for “Systemwalker Desktop Patrol CT” on the mobile PC. Through setting operation policy, even in the mobile PC that does not connect to network in usual time, assets management through Systemwalker Desktop Patrol should also be performed.

- Operation policy for assets management of mobile PC
- Operation policy for load reduction of mobile PC

The above settings are used for setting “Systemwalker Desktop Patrol DS” for mobile connection and performing settings for “Systemwalker Desktop Patrol DS” as well.

The mobile PC runs through connecting to the “Systemwalker Desktop Patrol DS” according to the operation policy that has been set.

The image diagram of mobile PC operation is shown below.


CS
DS for connecting mobile PC
DS for LAN connection
Proxy server
Internet
CT
CT
Run according to the operation policy for mobile PC set in DS

Enhance Security Auditing

Add the following security auditing item and enable auditing by the [PC Information] - [Security Information] window of "Desktop Patrol Main Menu".

- Hardware
  - Set BIOS hardware password
- OS
  - Set the password of Guest account to audit inappropriate password.
  - Enable/Disable automatic update of Windows Update.
  - Disable/Enable user account control (UAC) of Windows Vista®, Windows Server® 2008 and Windows® 7.
  - Existence of unsafe shared folder.
  - Set password of Windows logon user and audit inappropriate password.
- Application
  - Set firewall
  - Set real time scan of anti-virus software
  - Enable/Disable Google Desktop "Search Data on Multiple Computers"

Detect Prohibited Application

The application that is prohibited to be used can be confirmed through [PC Information] - [Software Auditing] of the Main Menu.

Alternatively, when the prohibited software has been installed, the information can be notified to the administrator through alarm notification function.

Enhance Alarm Notification Function

When software has been added to or deleted from the client, alarm notification of the modification information can be performed.

Patch Setting Function of Policy Group

When it is expected to apply security patches selectively to a particular PC, you can select the security patches to be applied in each policy group and perform settings.

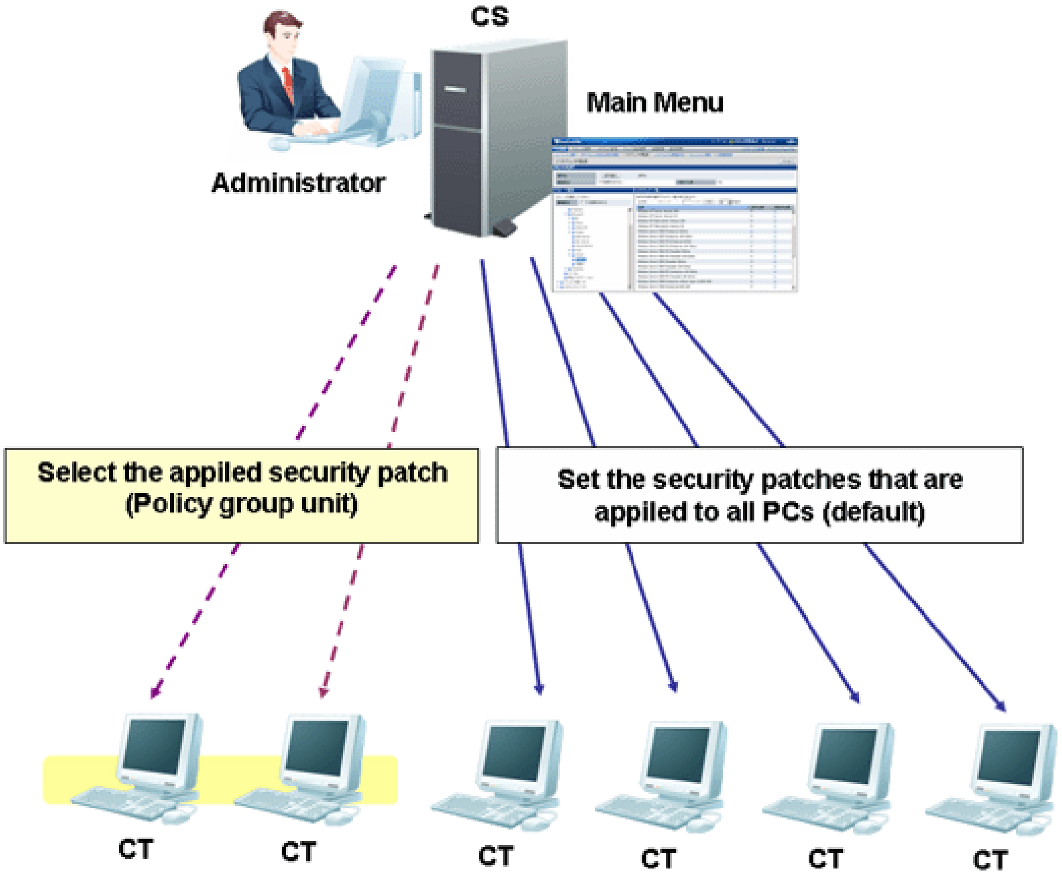
Based on this, for the PC with problem after applying a particular security patch, the exceptional patch can be applied.

When selecting the security patch to be applied, the following settings can be performed.

- Select the settings to apply security patches to a particular PC
- For a particular PC, set not to apply the security patches provided afterwards

The above settings can be used in combination.

The operation image diagram for applying security patches selectively to a particular PC is shown below.


CS
Main Menu
Administrator
Select the appiled security patch (Policy group unit)
Set the security patches that are appiled to all PCs (default)
CT
CT
CT
CT
CT
CT

For the PC that does not belong to the policy group, patch application can be performed according to the security patch settings selected in the [Distribution] - [Distribute Security Patches] window.

To apply security patches selectively to a particular PC, cancel the selection of security patch not to be applied in the [Environment Setup] - [Policy Group Management] - [Customize Various Policies] - [Patch Application Policy] tab of the Main Menu.

Based on this, for PC that belongs to the policy group, it is possible to apply security patches selectively.

Enhance Contents Execution

The software distribution function has been enhanced.

- Add the file type that can be executed after downloading

  Apart from “.exe” and “.bat”, the following file type can be specified in executable file after software distribution.

- .msi
- .vbs
- .wsf

Output Event Log of CS and DS

When the following events occurred in “Systemwalker Desktop Patrol CS” or “Systemwalker Desktop Patrol DS”, event log will be output. The event occurred in Systemwalker Desktop Patrol can be audited through Systemwalker Centric Manager and other products.

Category	Description
Information	- Start or stop service - Download security patches from the public site of Microsoft
Alarm	When small trouble without any problem will still occur in spite of automatic recovery and continued action
Error	When the exception that affects operation occurred in CS or DS

Collect CS Operation Log

The operation log through the following window (definition modification, registration, deletion) and login/logout for “Systemwalker Desktop Patrol CS” can be collected

- Desktop Patrol Main Menu
- Desktop Patrol Download Menu

Patch Application at Windows Logon

The time of Windows logon has been added to the timing of applying security patches.

Based on this, same as the version of V11.0L10 or earlier, security patches can be applied at the timing of Windows logon.

Auditing/Control of Power Saving and Security

PC can be audited according to the power saving/security policy determined by administrator. If policy is violated, the warning will be displayed in the window of PC and user will be reminded for processing.

In addition, the item that violated policy can be modified by force. (Note)

Note) Modification may not be performed by force due to item.

In the auditing/control of power saving and security, the following functions can be used.

- Modification of display/settings of warning window to PC that violates policy by force
- Confirmation of control status of security/power saving according to report output

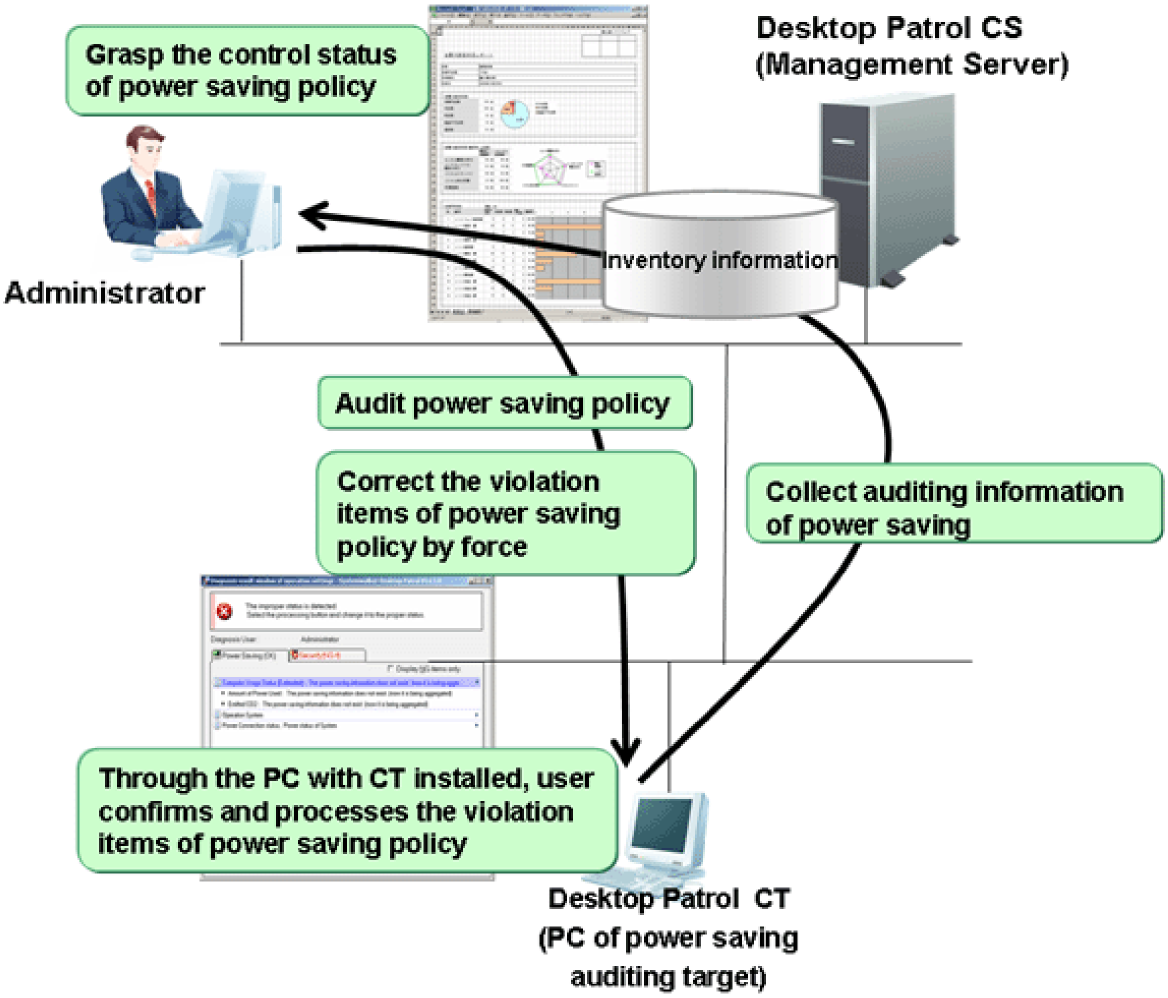
Auditing/Control of Power Saving

The operation summary when performing auditing/control of power saving is shown below.

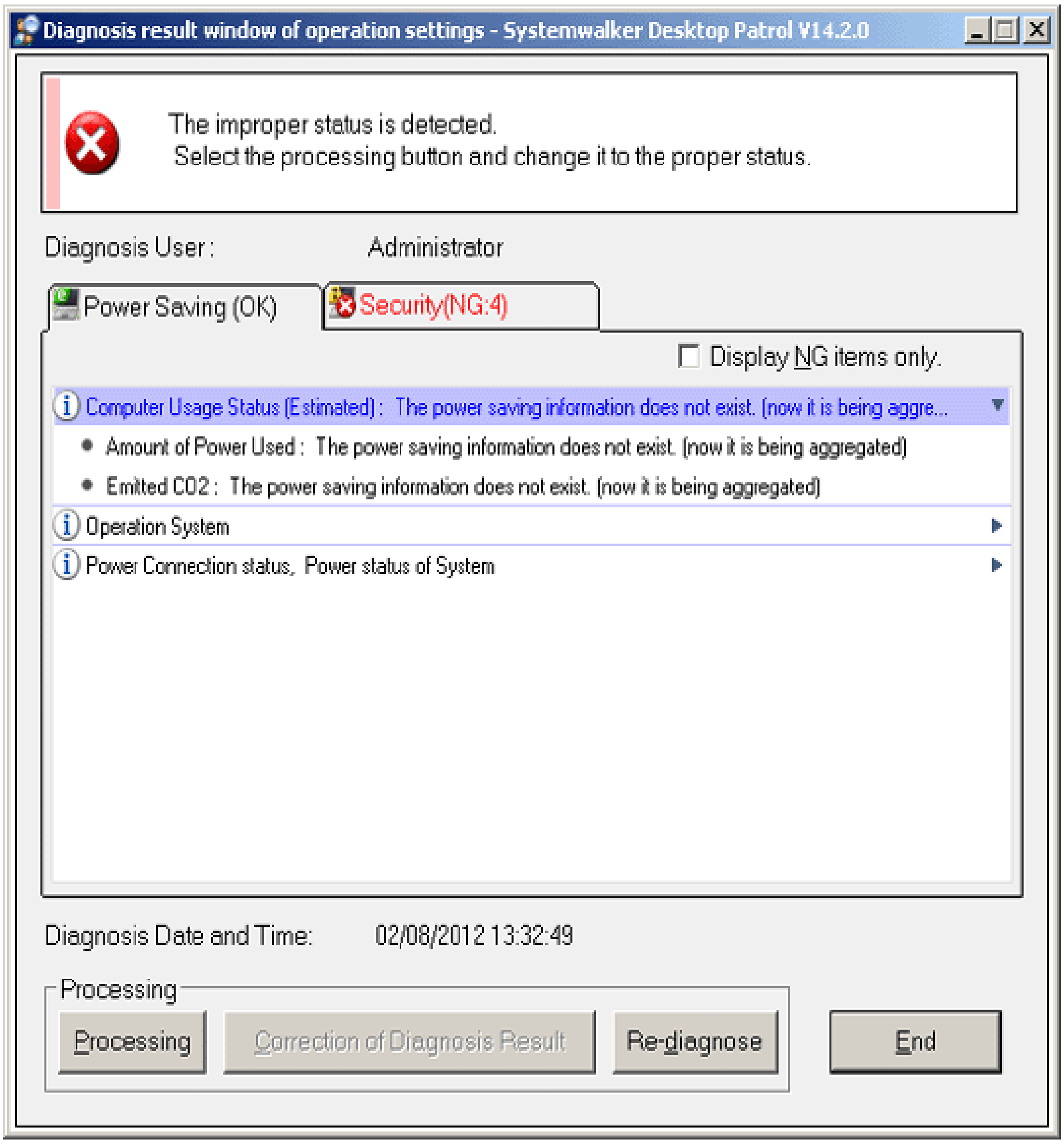
The auditing and control status of power saving and power consumption can be confirmed in the report.

- Power Saving Setting Status Report

- Power Consumption Auditing Report


Grasp the control status of power saving policy
Desktop Patrol CS
(Management Server)
Administrator
Inventory information
Audit power saving policy
Correct the violation items of power saving policy by force
Collect auditing information of power saving
Through the PC with CT installed, user confirms and processes the violation items of power saving policy
Desktop Patrol CT
(PC of power saving auditing target)

The diagnosis result window of power saving settings displayed at client is shown below.



Diagnosis result window of operation settings - Systemwalker Desktop Patrol V14.2.0

The improper status is detected.
Select the processing button and change it to the proper status.

Diagnosis User : Administrator

Computer Usage Status (Estimated) : The power saving information does not exist. (now it is being aggre...

- Amount of Power Used : The power saving information does not exist. (now it is being aggregated)
- Emitted CO2 : The power saving information does not exist. (now it is being aggregated)

Operation System

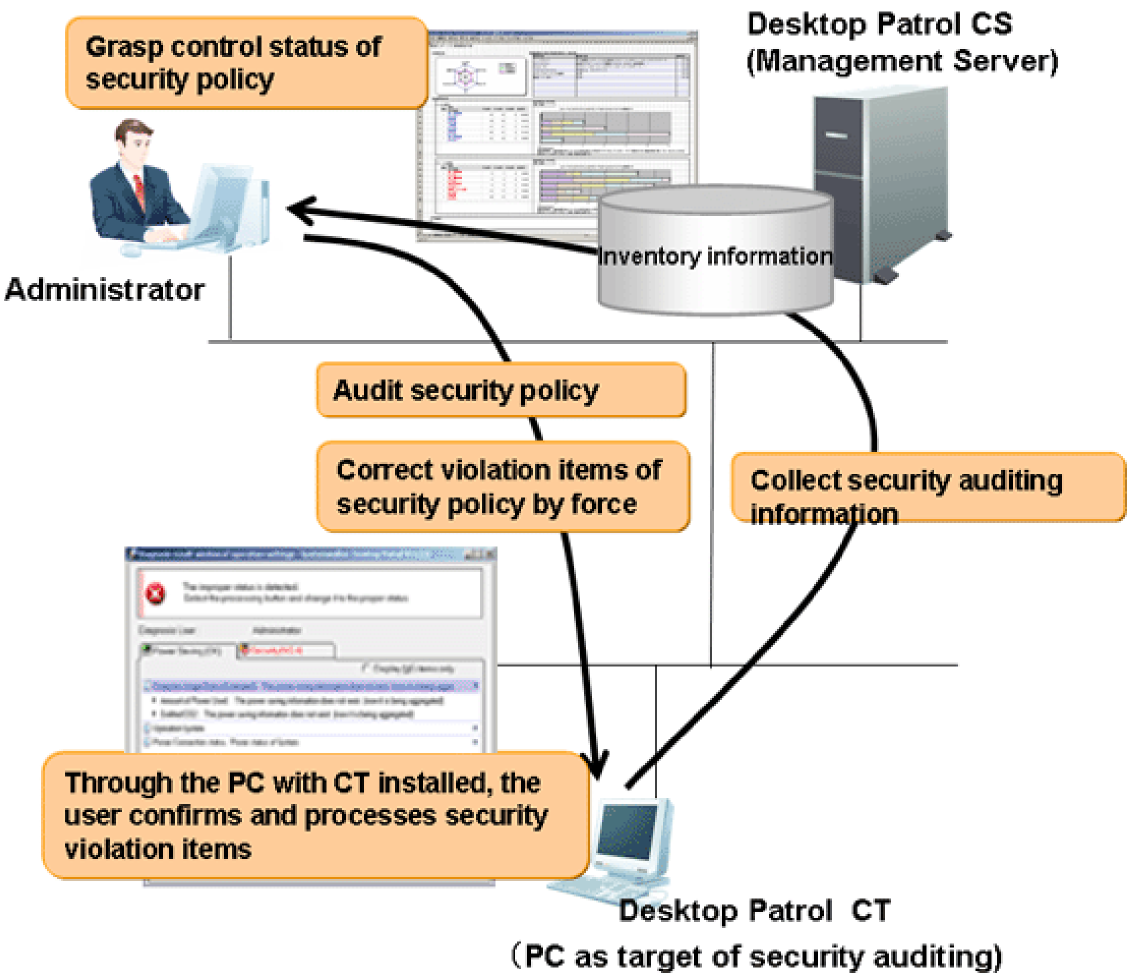
Power Connection status, Power status of System

Diagnosis Date and Time: 02/08/2012 13:32:49

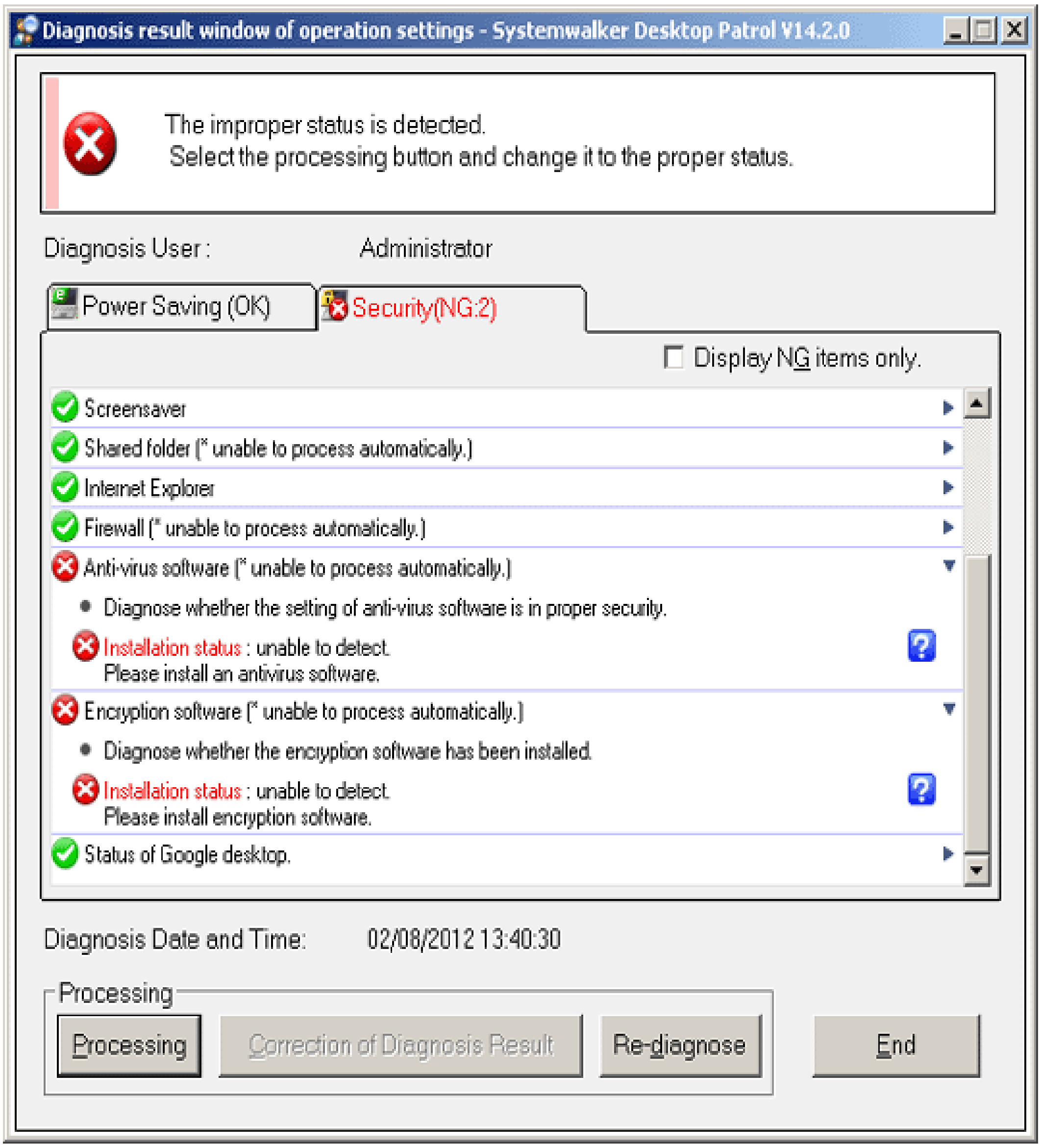
Auditing/Control

The operation summary when performing security auditing/control is shown below.

The control status of security policy can be confirmed through security auditing report.


Grasp control status of security policy
Desktop Patrol CS
(Management Server)
Administrator
Inventory information
Audit security policy
Correct violation items of security policy by force
Collect security auditing information
Through the PC with CT installed, the user confirms and processes security violation items
Desktop Patrol CT
（PC as target of security auditing)

The diagnosis result window of security setting displayed in the client is shown below.



Diagnosis result window of operation settings - Systemwalker Desktop Patrol V14.2.0

The improper status is detected.
Select the processing button and change it to the proper status.

Diagnosis User : Administrator

Power Saving (OK) | Security(NG:2)

□ Display NG items only.

- ✓ Screensaver
- ✓ Shared folder (* unable to process automatically.)
- ✓ Internet Explorer
- ✓ Firewall (* unable to process automatically.)
- ✗ Anti-virus software (* unable to process automatically.)
  - ● Diagnose whether the setting of anti-virus software is in proper security.
  - ✗ Installation status : unable to detect.
    Please install an antivirus software.
- ✗ Encryption software (* unable to process automatically.)
  - ● Diagnose whether the encryption software has been installed.
  - ✗ Installation status : unable to detect.
    Please install encryption software.
- ✓ Status of Google desktop.

Diagnosis Date and Time: 02/08/2012 13:40:30

Newly Added Management Ledger Function

The following management can be performed through the information collected using Systemwalker Desktop Patrol or the information managed by ledger.

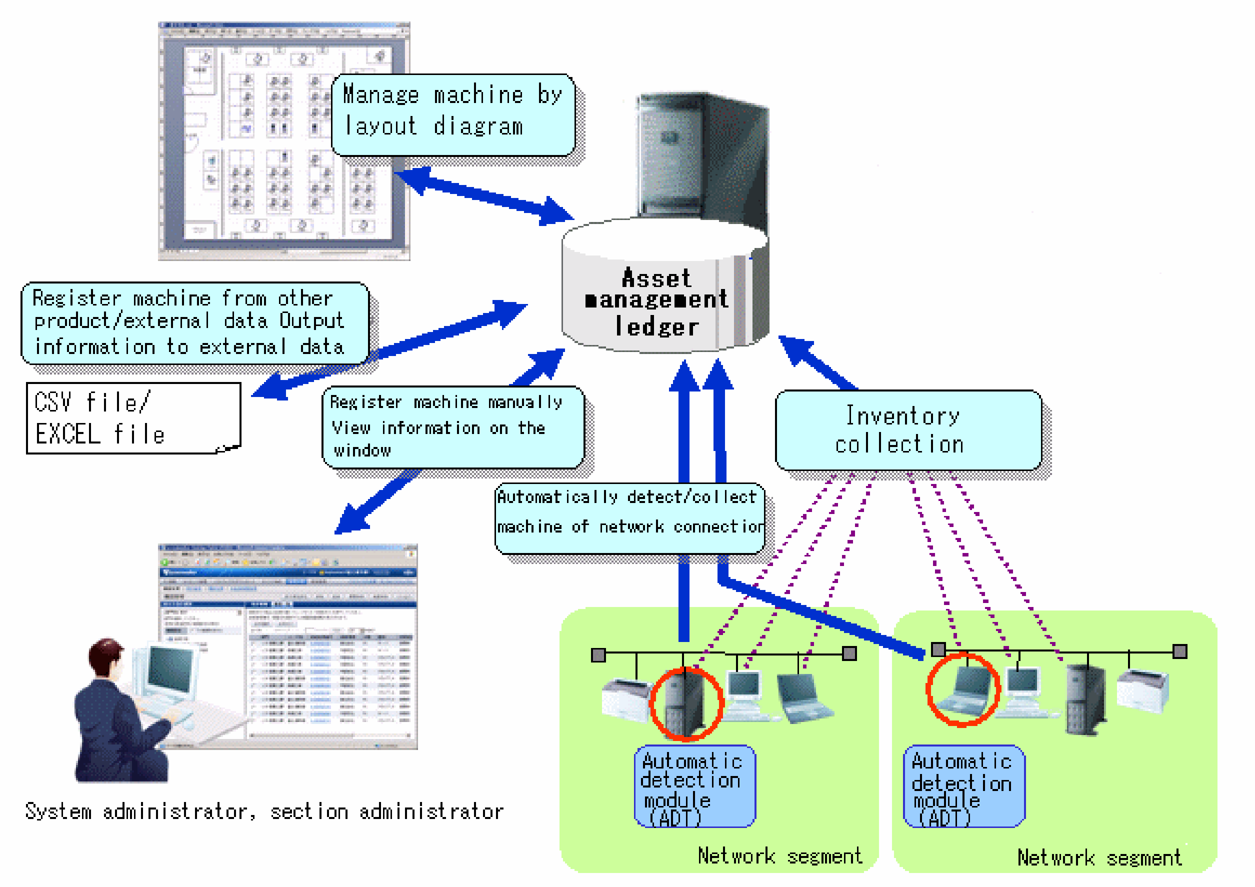
- Device Management Function
- Contract Management Function
- Stocktaking Support Function
- Report Output Function

Device Management

For management target device, there are following operations through confirming and operating the asset status of asset status (PC and devices).

- Automatic detection of device information
- Confirmation of device information by section/type/location

- Registration/Modification/Deletion of device information
- Save ledger of device information
- Confirmation of modification history
- Device management through layout diagram
- Creation of assets management ledger from other product

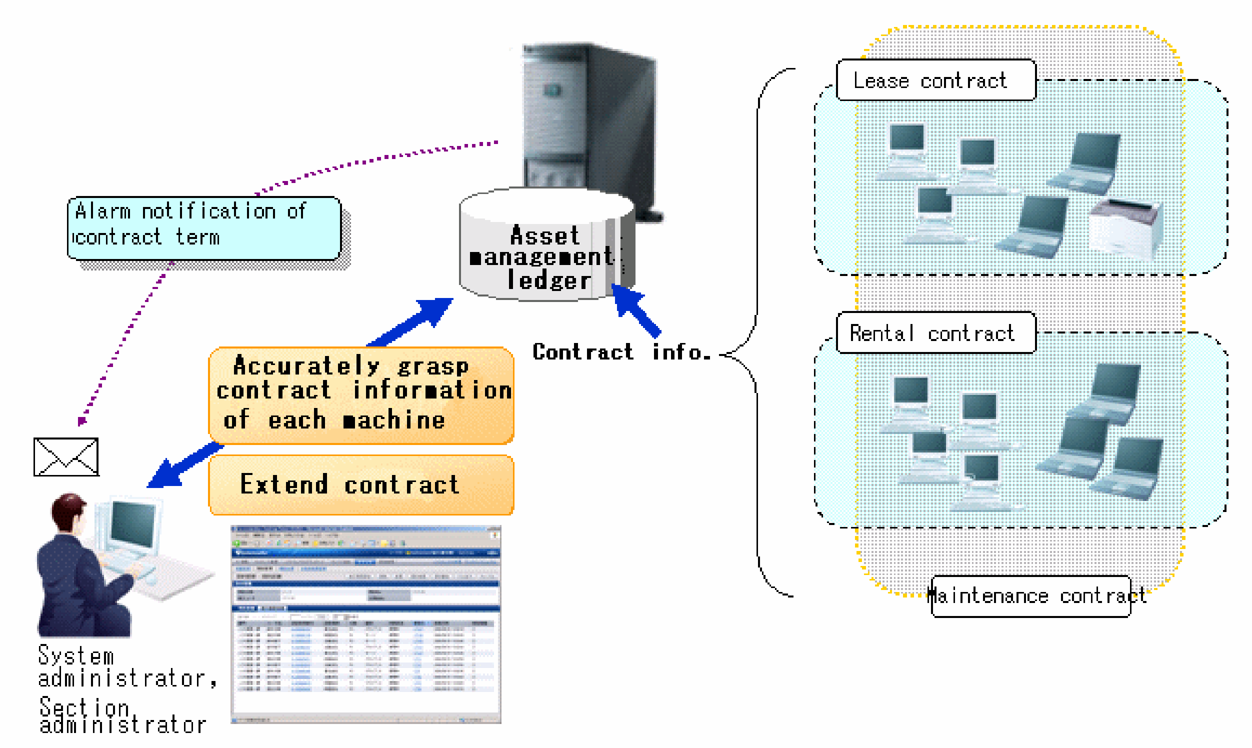

Manage machine by layout diagram
Asset management ledger
Register machine from other product/external data Output information to external data
CSV file/ EXCEL file
Register machine manually View information on the window
Inventory collection
Automatically detect/collect machine of network connection
Automatic detection module (ADT)
Automatic detection module (ADT)
System administrator, section administrator
Network segment
Network segment

Contract Management

There are following operations through the function of managing contract information of management target device.

- Confirmation of contract information by section/type
- Registration/Modification/Deletion of contract information
- Allocation of contract information
- Save ledger of contract information
- Extension of contract

- Alarm notification of contract term

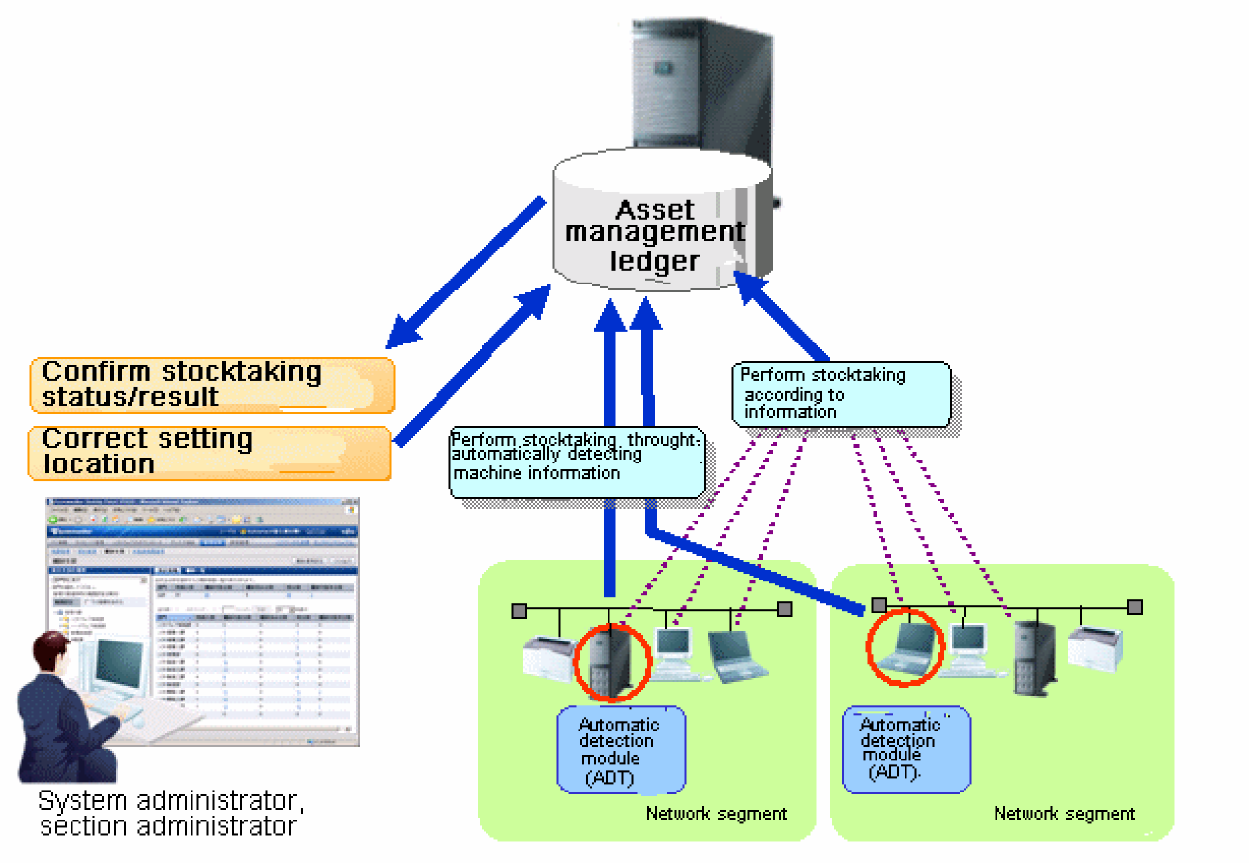

Alarm notification of contract term
Asset management ledger
Accurately grasp contract information of each machine
Extend contract
Contract info.
Lease contract
Rental contract
Maintenance contract
System administrator, Section administrator

Stocktaking Support

There are following operations in the function for supporting the stocktaking of management target device.

- Confirmation of stocktaking status by section/type/location
- Setting of whether stocktaking can be executed

- Save ledger of stocktaking status


Asset management ledger
Confirm stocktaking status/result
Correct setting location
Perform stocktaking throught automatically detecting machine information
Perform stocktaking according to information
Automatic detection module (ADT)
Automatic detection module (ADT)
Network segment
Network segment
System administrator, section administrator

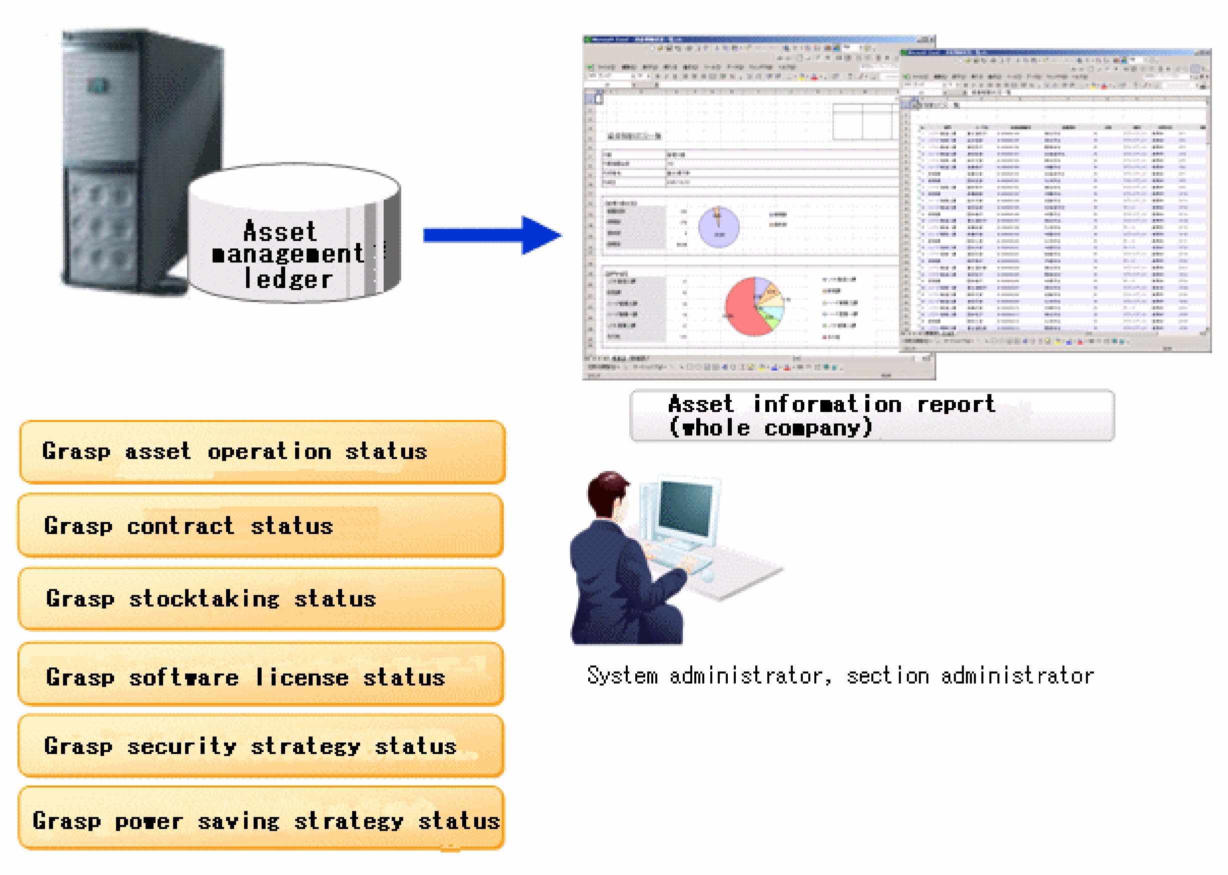
Report Output

It is the function of outputting the asset information managed in Systemwalker Desktop Patrol as file or print in report format (Microsoft(R) Excel format). Graphs and tables can be output at the time of outputting report, so that the current status and problems can be known visually.

The following operations can be performed in the output of report format of asset information.

- Output file in report format

- Edit report layout

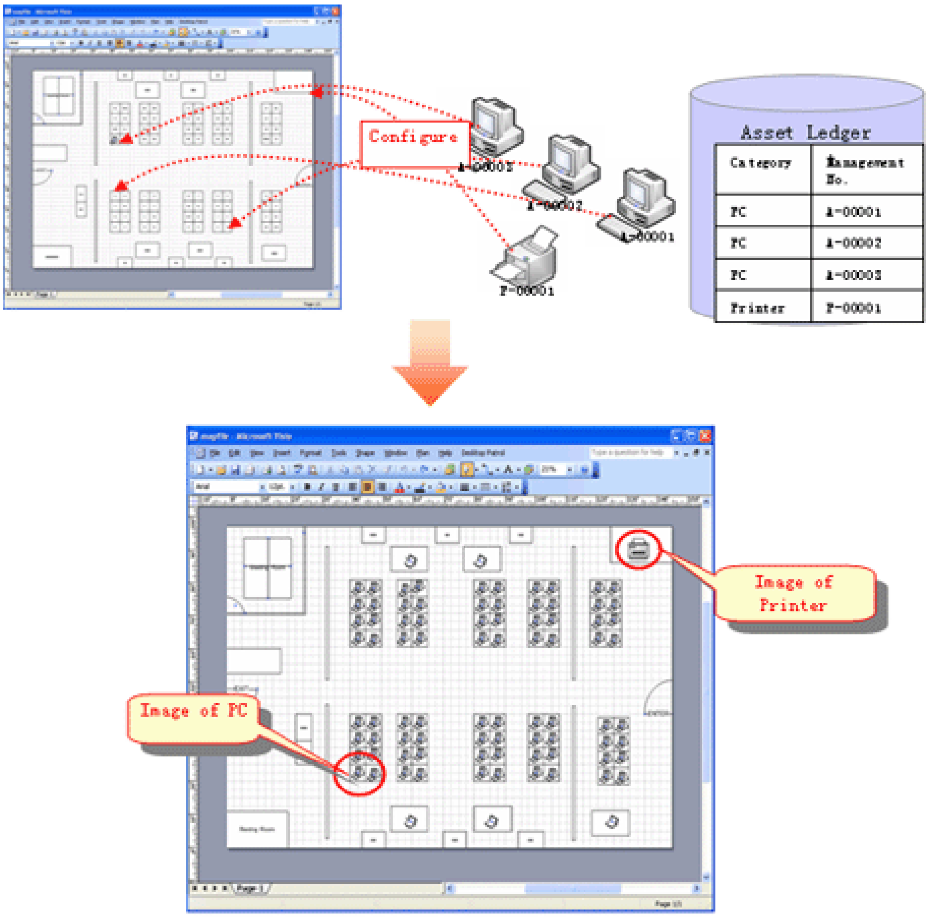

Asset management ledger
Asset information report (whole company)
Grasp asset operation status
Grasp contract status
Grasp stocktaking status
Grasp software license status
Grasp security strategy status
Grasp power saving strategy status
System administrator, section administrator

Device Management by Layout Diagram

For the layout diagram that shows the floor image, it can be managed after confirming the managed device in asset ledger.

In the mean time of confirming the configuration of device visually, the asset information of device can be viewed.

When performing the device management based on the layout diagram, Microsoft® Office Visio® is required.



Asset Ledger

Category	Management No.
PC	A-00001
PC	A-00002
PC	A-00003
Printer	P-00001

Map file

Support Virtual Desktop Environment

To use and audit the virtual desktop, support the CT, main menu, and management ledger functions in the following ways.

CT

To install the CT on the virtual desktop,

- Support the link clone environment.
- Support connecting the remote desktop to the terminal server.
- Determine the CT running in the virtual PC, and reflect the power saving and security auditing results.

Main Menu

To determine information about the virtual PC, add the following items:

- General PC list visible column(s) on the inventory information page
- Searched items that can be screened in the virtual environment when creating a policy group
- General PC list managed by the policy group
- Initial option “Domain Name” for starting the basic operation policy PC

Report Output Function

To determine information about the virtual PC, perform the following in the report:

- Set the auditing item “Hardware” in the security auditing report to “Not Auditing”.
- List the power saving status report to “Number of Unaudited PCs”.

Improvement of Usability

The improvements of following usability have been performed.

Customization of displayed items of PC list

The items displayed in [PC List] of the [PC Information] - [Inventory Information] of "Desktop Patrol Main Menu". The modification of displayed item can be set all at once in the system.

Tree view of software list

The software list of the following window of "Desktop Patrol Main Menu" will be displayed in tree view.

- [PC Information] - [Software Auditing] window

Page supporting list view

The page supports the list view of displayed items in each window of "Desktop Patrol Main Menu".

When there are many displayed items, the number of items displayed in one page can be narrowed down for display.

Integration to Web GUI of MC Window

The functions provided through Management Console before Systemwalker Desktop Patrol V13 has been integrated to Web GUI. The operation performed through MC window will no longer require window switch as before. Instead, everything can be operated through the Web window.

Display Operation Status and Usage Processing

As the Top window of the Main Menu, the "Status Window" that displays the operation status of Systemwalker Desktop Patrol in list has been added, based on which the following operations can be achieved.

- The overall status can be known in a short time.
- Since the status including Systemwalker Desktop Keeper will be displayed in the "Status Window" Top window in the system with Systemwalker Desktop Keeper V14.2.0 installed, the status can be known without switching the product window.
- According to the displayed results on the main menu status window, operations such as check and browse the faulty PC are extension to use processing is possible.

  The following items can be added:

  - Message Sending
  - Inventory Collection
  - Security Patch Installation
  - Security Settings Modification
  - Power Saving Settings Modification

Other Improved Functions

The following functions have been improved/enhanced.

Operation Log Collection

Systemwalker Desktop Patrol saves users' operations as logs in PCs which are running the CT, and adds a function for collecting such log files.

By confirming the operation log file, the following effects can be implemented.

- Forbid information disclosure
- Operation trace when a fault occurs in the PC

Improve Distribution Function

- Multiple files can be sent to different PCs through the distribution settings of the CS. Besides, the "File Distribution" function for confirming the distribution result in the CS is provided.

- Specify “Time Segment” in the “Distribute Software” function.
  Then, you can distribute software in the specified time segment.
- In order to distribute software more easily to a particular PC, apart from the existing distribution target, the PC group for distribution has been added.
  - PC group for distribution

    It is the group for distributing software. Any PC can be registered to the PC group for distribution.

    In addition, one PC can also be registered to multiple groups for distribution.
  - Policy group

    It is the group for performing operation setting of client. Even policy group, can be specified as the distribution target of software.
  - CS/DS

    It is the physical server, which is specified when it is expected to distribute software to PC under CS/DS only.

CT Operation Status Check Command

The command that can display the CT operation status in the window has been added.

Based on this, whether CT runs according to the settings of policy set in CT can be confirmed through CS and the window on correspondent CT/

Enhance Auditing Items of Security Settings

The auditing items of security settings have been added and modified.

- Settings that require complex password <Add>

  Whether the complex password has been specified can be audited.
- The auditing method of Guest account <Modify>

  As the auditing method of Guest account, it is allowed to check the enabling/disabling of account only without checking the password.
  In addition, the auditing result can be confirmed through the Main Menu and report.

Browse PC Information

The following operations can be performed in the system which is running Systemwalker Desktop Keeper V14.2.0.

- The Systemwalker Desktop Keeper log retrieval page can be invoked by one click on the PC information page of Systemwalker Desktop Patrol.

  Therefore, you can trace the operation that is performed on the faulty PC according to the operation logs managed by Systemwalker Desktop Keeper.
- You can also browse the inventory information on the log retrieval page of Systemwalker Desktop Keeper by clicking.

  Therefore, the security status of a PC whose files are exported through USB can be easily obtained.

Allowed Character Expanded for User ID

The underscore “_” can be used as a character for the user ID.

Improve Search Function

The function modifies from exact retrieval to fuzzy retrieval.

Improve Input Area for MAC Address

The MAC address input area modifies from an 8-bit unit to one input box.

Collect Inventory Collected through Other Products

When you run InvSend.exe to import inventory information based on Systemwalker Centric Manager or CSV, the Collection Date/Time will be updated.

Therefore, you can confirm the time when the inventory information is imported by viewing the Collection Date/Time.

1.4 System Structure

This section describes the structure of Systemwalker Desktop Patrol.

1.4.1 Components of Systemwalker Desktop Patrol

Systemwalker Desktop Patrol consists of the following components.

Systemwalker Desktop Patrol CS (Corporate Server)

Systemwalker Desktop Patrol CS defines the inventory information collection condition and software distribution condition as policies, and sends to servers of each PC.

According to databases of IT repository, personnel, and organizations, the component provides services such as security patches distribution, security auditing, and license management through the Web GUI. Usually one Systemwalker Desktop Patrol CS is installed in an enterprise.

Systemwalker Desktop Patrol AC (Asset Console)

Systemwalker Desktop Patrol AC is a console for administrators to export reports in terms of assets, security, and power saving.

Systemwalker Desktop Patrol DS (Domain Server)

Systemwalker Desktop Patrol DS is a server used for providing transferring/saving operation policy and inventory information, and distributing software.

This component is configured for scattering loads. It is effective when the client is remote and with low speed, or the distributed software is too large.

Systemwalker Desktop Patrol ADT (Auto Detection Terminal)

Systemwalker Desktop Patrol ADT is configured in each network segment, which is used for detecting devices (in the same network segment) that are connected to the internet. It also notifies the CS of the detected device information.

Systemwalker Desktop Patrol CT (Client Terminal)

Systemwalker Desktop Patrol CT is installed on the PC that manages assets by inventory collection. You can download software distribution and receive security patches through Systemwalker Desktop Patrol CT.

Besides, according to the administrator’s settings, a warning prompt appears when the power saving or security policy is violated.

Web GUI

Web GUI is a view for operating Systemwalker Desktop Patrol on the Web Browser through services provided by Systemwalker Desktop Patrol CS.

You can also set the policies for Systemwalker Desktop Patrol.

There are main menu and download menu on the Web GUI.

Live Help Expert

Live Help Expert is the software for operating Live Help Client remotely. If a fault occurs when a client user is operating on a PC, Live Help Expert can connect to the user’s PC and provide help.

For details, see the manual of Systemwalker Live Help.

Live Help Client

Live Help Client is the software that is operated remotely by Live Help Expert. It is installed between the client user’s PC and the server for remote operation. When the client cannot process according to the prompt message or does not know the operation methods of a program, it can seek help from Live Help Expert remotely.

For details, see the manual of Systemwalker Live Help.

1.4.2 Software Dictionary

What is Software Dictionary

To collect software information by using the inventory collection function of Systemwalker Desktop Patrol, you need to define the search condition of the software.

This definition is called “Software Dictionary” in Systemwalker Desktop Patrol.

Select “PC Information” - “Software Auditing” to confirm the collected software information.

The software dictionary supports the following:

- Support Center Definition

  Retrieval conditions of software that are distributed by E-mail through the Systemwalker Support Center.

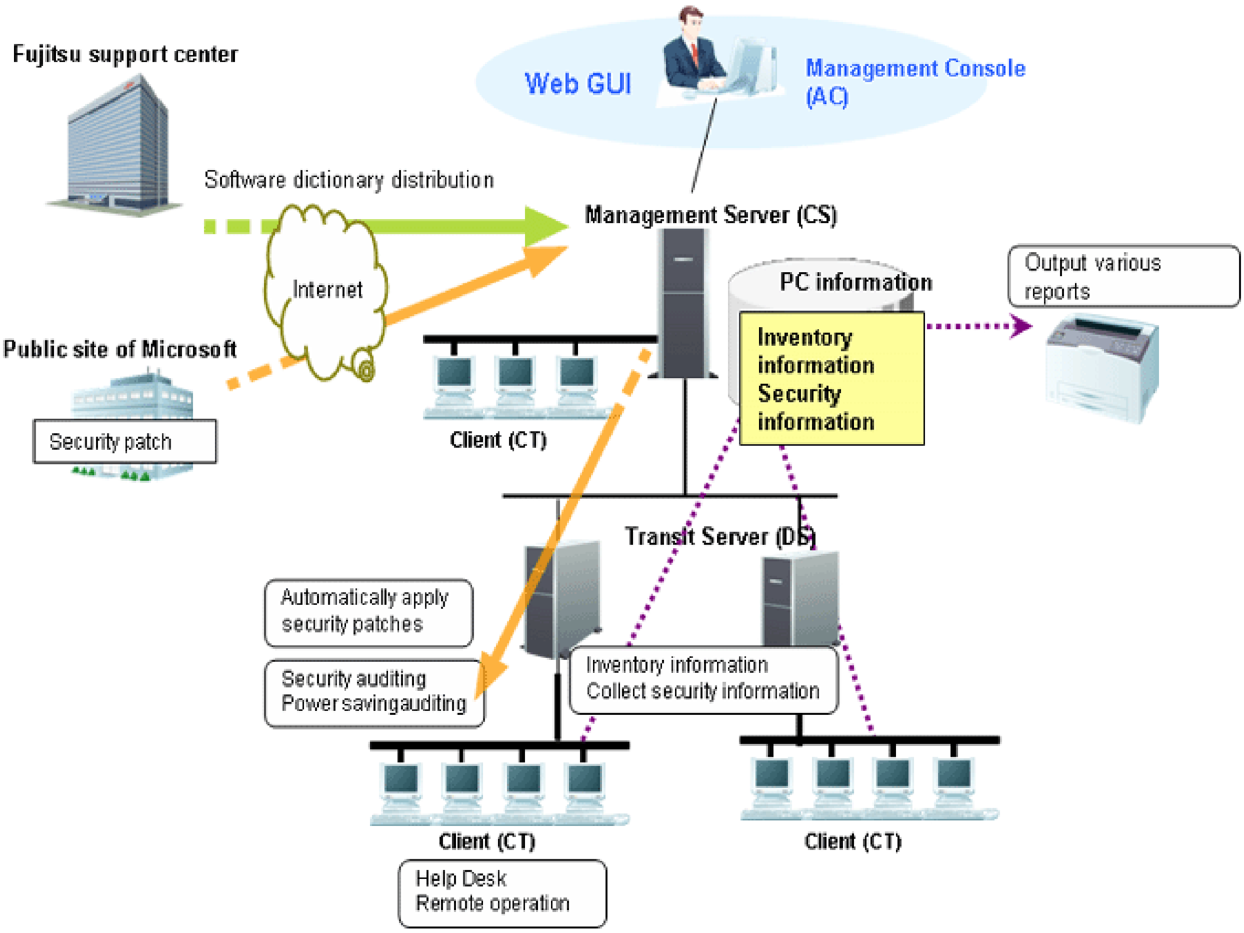
  Conditions for searching typical software, Microsoft security patches, and virus definition files of Anti-virus Software are supported. You can use the latest software dictionary to update the support center definition.

- User definition

  Conditions for searching independent software are supported.

1.4.3 System Structure

The following figure shows how to use the Systemwalker Desktop Patrol client (security auditing and inventory collection) and the troubleshooting.



Process of Applying Security Patches

1. Receive the software dictionary

   Receive and apply the software dictionary (used for detecting definition files of software and security patches) from manually download and apply.

2. Select management target software/security patches

   Select the software that is used as the management target.

   Besides, the software dictionary records security patch information that is automatically downloaded from Microsoft's public site. Select security patches that can be applied automatically.

3. Distribute/apply security patches

   Automatic download the selected security patches from the public site of Microsoft.

   Distribute and apply the downloaded security patches based on the operational configuration.

4. Collect inventory information

   Software installation status and hardware information selected in the software dictionary can be collected automatically.

   Besides, the application status of security patches can also be collected automatically.

5. Confirm

   The administrator confirms the software installation status and hardware information.

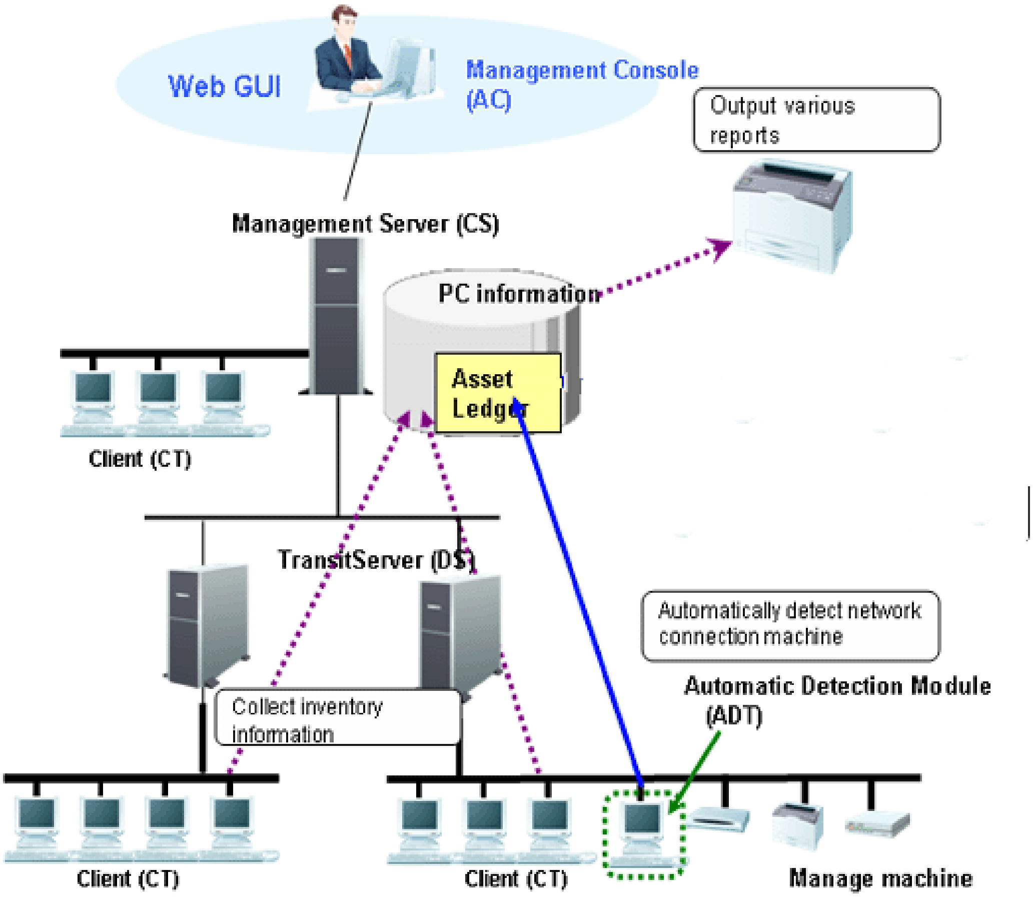
   The administrator can also determine whether the necessary security patches are applied.

Process of Remote Operation

1. Start the Live Help Client on the faulty PC.
2. The administrator uses the Live Help Expert function to connect to the client PC.

3. The administrator performs operations on the GUI of the client PC and rectifies faults.

The following figure shows the IT assets management through Systemwalker Desktop Patrol.



1. Register/ modify asset information

   Perform either of the following methods to register/modify the asset information:

   a. Register/ modify the inventory information

      Register/ modify the inventory information collected by Systemwalker Desktop Patrol manually or automatically as the asset information managed by management ledger.

   b. Register/ modify account

      Register/ modify the asset information managed by management ledger (the asset information used to be considered as the account).

   c. Register/ modify through device information auto-detected

      The device information auto-detected by the ADT is notified to the CS automatically. The unregistered device information can be registered on the unregistered device management page, or you can enter all the registered device names and register them uniformly.

   d. Register/ modify on the page

      Register and modify the asset information respectively through the main menu.

2. Confirm the asset information

   Perform either of the following methods to confirm the asset information:

   a. Through the page

      Confirm the device information, contract information, and checking status through the main menu.

3. Stocktaking Operation

   Perform either of the following methods to check the asset information:

   a. Collect the inventory information

      Check the asset information through the inventory information collected from the PC.

   b. Auto-Detect device information

      Check the asset information through the device information detected automatically by ADT.

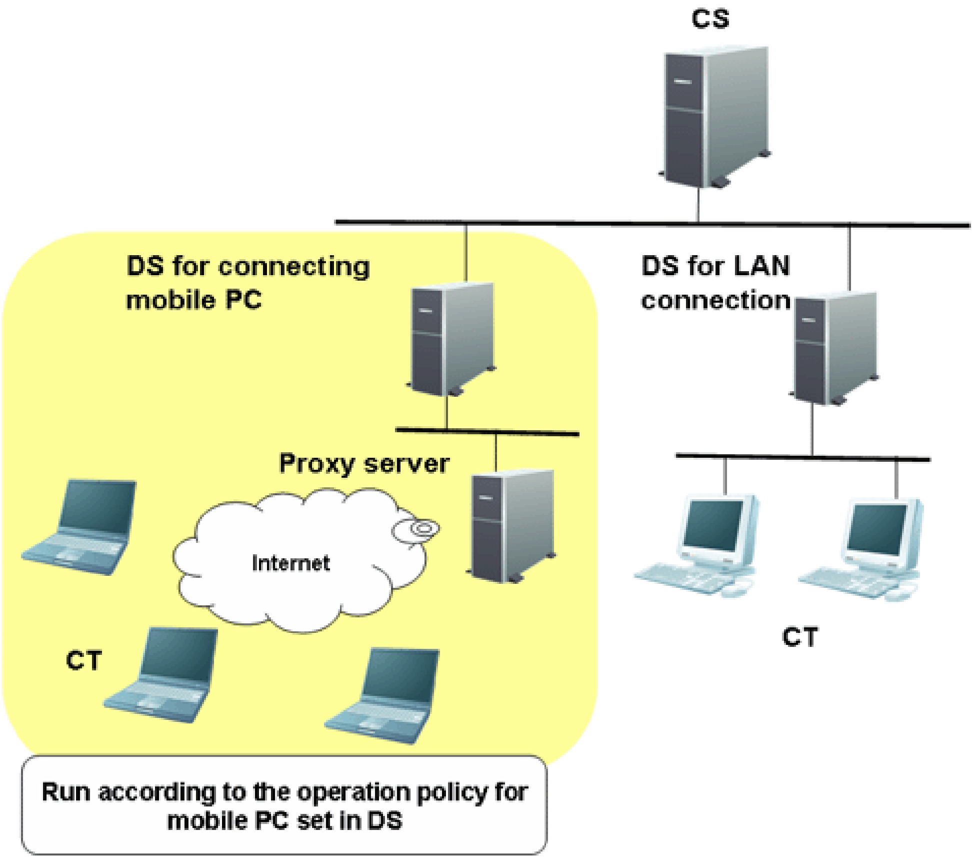
   c. Set on the page

      Set the stocktaking status (Checked/Not Checked) manually on the main menu.

4. Export reports

   Export results of asset running status, contract status, and checking status in a report according to the asset information managed by management ledger, so that you can know and audit the usage.

Use the Virtual Private Network (VPN) to access the internal network of the company from outside. The following figure shows the system structure for mobile operation.


CS
DS for connecting mobile PC
DS for LAN connection
Proxy server
Internet
CT
CT
Run according to the operation policy for mobile PC set in DS

Set the DS for connecting to the PC for mobile operation, and set the running policy that the PC uses on the DS. Then the PC connects to the DS and runs according to the preset policy.

Assets management based on Systemwalker Desktop Patrol can also be performed in the mobile operating PCs which are not always connecting to the Internet .

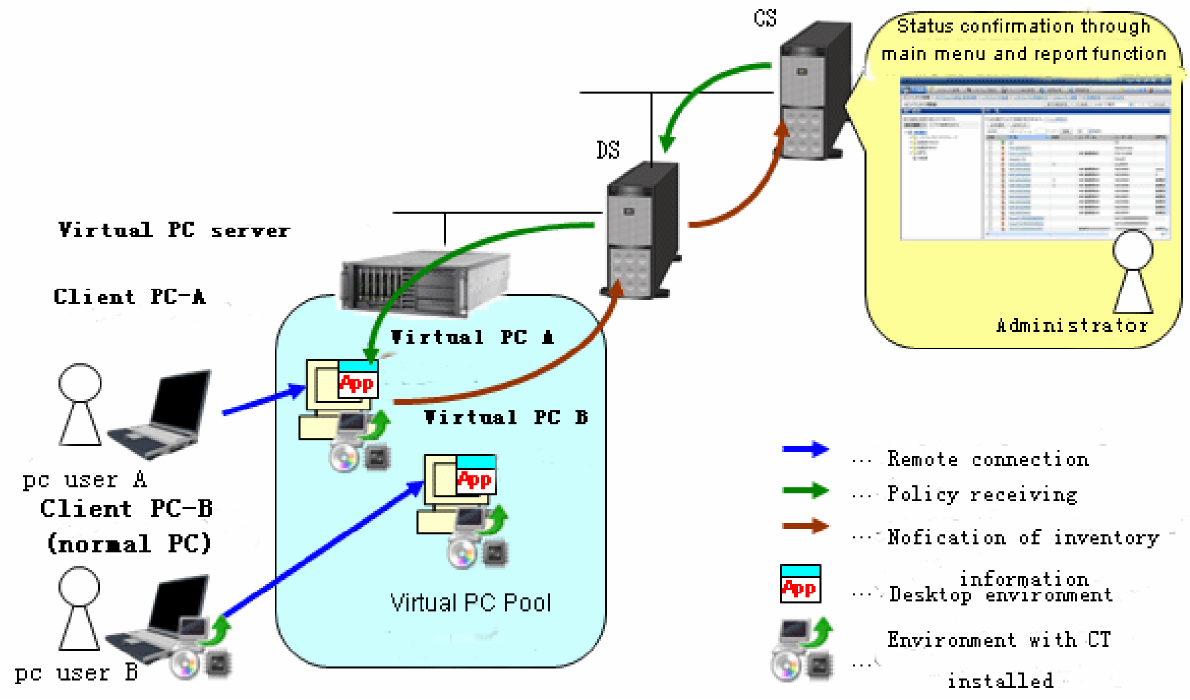
1.4.4 System Structure When CT is Installed in the Virtual Desktop Environment

When installing Systemwalker Desktop Patrol CT in the virtual desktop environment, the following situations may occur.

Using a Virtual PC Server

Install the CT on a virtual PC. Manage assets such as installing software or performing Windows security auditing. Determine information collected by the virtual PC through the main menu.

The processes of receiving policies from servers (CS and DS) and notifying the server of the inventory information are the same as those of a common CT.

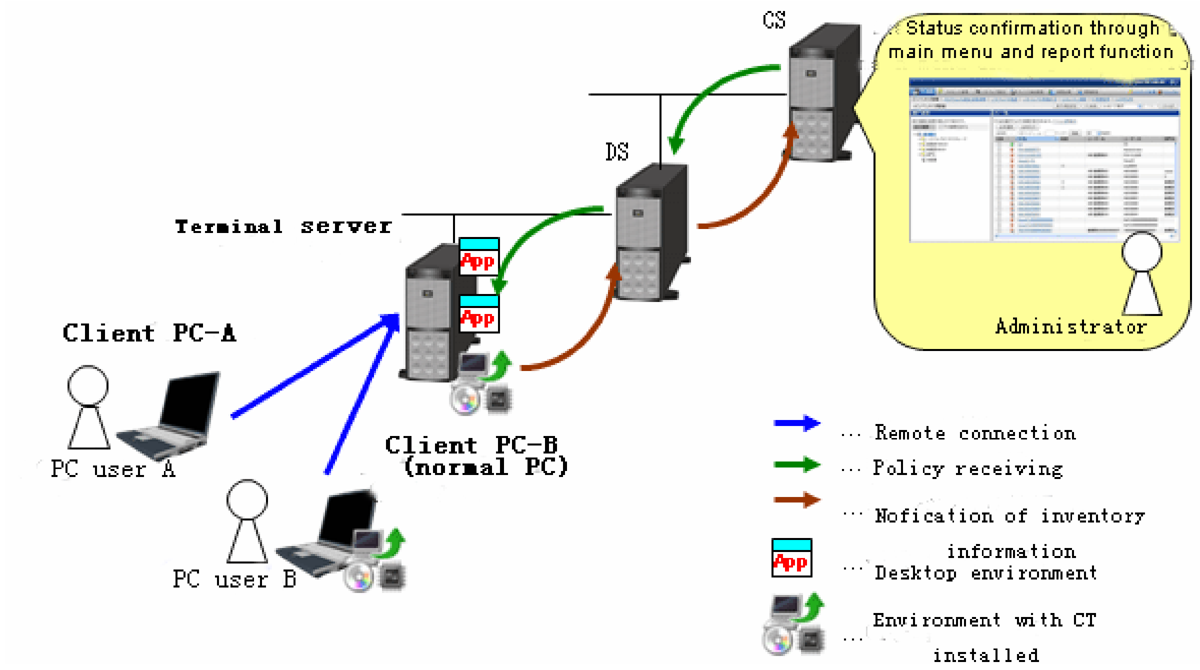


Virtual PC server: PC which is running VMware ESX, VMware vSphere, and Microsoft Hyper-V.
Client PC: Common notebook computer or desktop computer.
Virtual PC Pool: Set groups for virtual PCs.

Using a Terminal Server

Install CT for Windows of the terminal server. Manage assets such as installing software and performing Windows security auditing.

The processes of receiving policies from servers (CS and DS) and notifying the server of the inventory information are the same as those of a common CT.

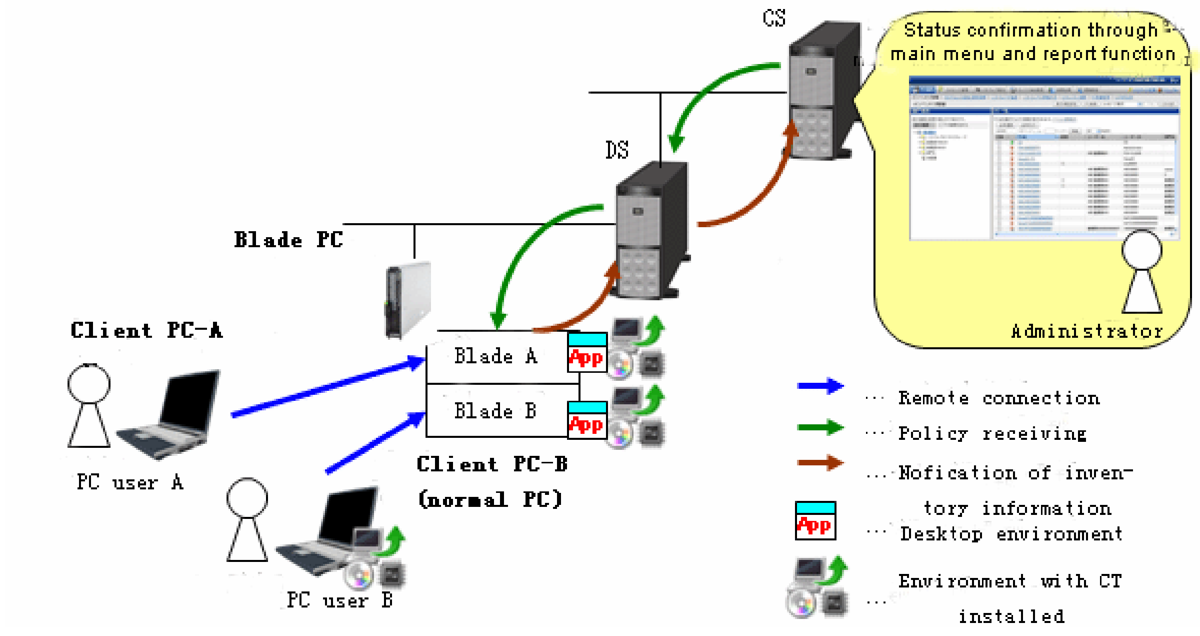

CS
Status confirmation through main menu and report function
Administrator
DS
Terminal server
App
App
Client PC-A
PC user A
Client PC-B (normal PC)
PC user B
… Remote connection
… Policy receiving
… Nofication of inventory information
App … Desktop environment
… Environment with CT installed

Terminal server: As a Windows server (Windows Server 2003 or Windows Server 2008), the environment for the terminal server or remote desktop session host is installed.
Client PC: Common notebook computer or desktop computer.

Using a Blade PC

Install CT in each blade Windows system of blade PCs. Manage assets such as installing software and performing Windows security auditing.

The processes of receiving policies from servers (CS and DS) and notifying the server of the inventory information are the same as those of a common CT.


CS
Status confirmation through main menu and report function
Administrator
DS
Blade PC
Blade A
Blade B
App
App
Client PC-A
PC user A
Client PC-B (normal PC)
PC user B
… Remote connection
… Policy receiving
… Nofication of inventory information
App … Desktop environment
… Environment with CT installed

Blade PC: PC whose special cabinet are mounted with multiple blades
Client PC: Common notebook computer or desktop computer.

1.4.5 Communications Security

Communications security of Systemwalker Desktop Patrol supports the following functions.

Proxy Server

A proxy server can be set.

SSL Communications

The SSL communications for encryption use can be performed between the following servers:

- Between “Systemwalker Desktop Patrol CS” and “Systemwalker Desktop Patrol DS”

  Information can be distributed after encrypted. Therefore, the security of network between “Systemwalker Desktop Patrol CS” and “Systemwalker Desktop Patrol DS” is enhanced.

Chapter 2 Systemwalker Desktop Patrol Functions

This chapter describes the functions of Systemwalker Desktop Patrol.

- PC Information Collection/Browse Function
- PC Auditing/Control Function
- License Management Function
- Security Patch Distribution/Application Function
- File Distribution Function
- Software Distribution Function
- Management Ledger Function
- Report Output Function
- Location Map Function
- Environment Setup Function
- Remote Operation Function
- Updater Function
- CT Prohibition Function

Also, please refer to *Systemwalker Desktop Patrol Operation Guide: for Administrators* for how to set and operate the functions, as well as the notices.

2.1 PC Information Collection/Browse Function

This section describes the PC information collection/browse function of Systemwalker Desktop Patrol.

In Systemwalker Desktop Patrol, the software and hardware information of PC is called Inventory information which can be collected from PCs. And this information can be managed in CS after registering in the database.

The assets management function of Systemwalker Desktop Patrol can flexibly meet various demands of enterprises.

In addition, the section describes the information collected through this function, together with the information display windows.

2.1.1 How to Collect

The following two modes can be used to collect the Inventory information.

- Agent mode
    - This method is not realized by the user and causes no burden.
    - It also can collect the information about software execution status.
- Command mode
    - Information can be collected via the external medium, e.g. floppy disk.
    - Information collection can be realized via the sending command of E-mail attachment (the command automatically operating from collection of Inventory information till E-mail sending).

Agent mode

Automatic collection of latest information and construction of PC information database can be realized through installation of CT in the PC.

According to the Client policy set in the main menu, CT collects Inventory information and sends it to the connected server. Inventory information collected by CTs will be finally transmitted to the highest-level CS and registered in the CS database.

Command mode

Command mode can be applied to collect Inventory information on such situations as network disconnection between PC and Master, and the slower network.

Command mode can be applied to collect Inventory information even if CT is not installed.

Command mode is classified as the following two types:

Inventory collection only: CTOffline.exe

After executing the command, collect Inventory information, and create the Inventory file (“User ID + PC Name”) in the present directory. Inventory information can be obtained via saving the created file to the specified directory of CS or DS.

Inventory collection + E-mail sending: CTMail.exe

Collect Inventory information and send the Inventory information file (“User ID + PC Name”) to CS or DS via the E-mail.

Collection items

Collection information is variable with different collection methods. Collectable information is shown in the following table.

Collect Information	How to Collect	
	Agent Mode	Command Mode
Basic Information (OS Information, Hardware Information)	○	○
Software Information	○	○
Anti-Virus Software	○	○
Add or Remove Programs	○	○
User Information	○	○
EXE Information	○	○
Registry Information	○	○
Unapplied Patch Information	○	○
Security Information: System Security Information User Security Information	○	○
Security Information: Desktop Keeper information	○	×
Power saving auditing information: Power saving setting value	○	○
Power saving auditing information: Power saving status	○	×
Software Operation Status	○	×
Files Collection	○	×
Simple operation logs	○	×

○: Collectable ×: Not collectable

2.1.2 Inventory Information

User ID and PC name can be added to Inventory information and collected together so as to quickly distinguish the sections of the collected information and the administrators of PCs by means of the Inventory Collection Function of Systemwalker Desktop Patrol. By this way, even though the section frequently changes or PC moves, the location of PC and section can be tracked.

The following information can be collected and browsed as Inventory information:

- Basic Info (OS Information, Hardware Information)
- Software Info
- Anti-Virus Software
- Add or Remove Programs
- User Info
- EXE Info
- Registry Info
- Unapplied Patch Info
- Contract Information
- Security Information
- Power Saving Information

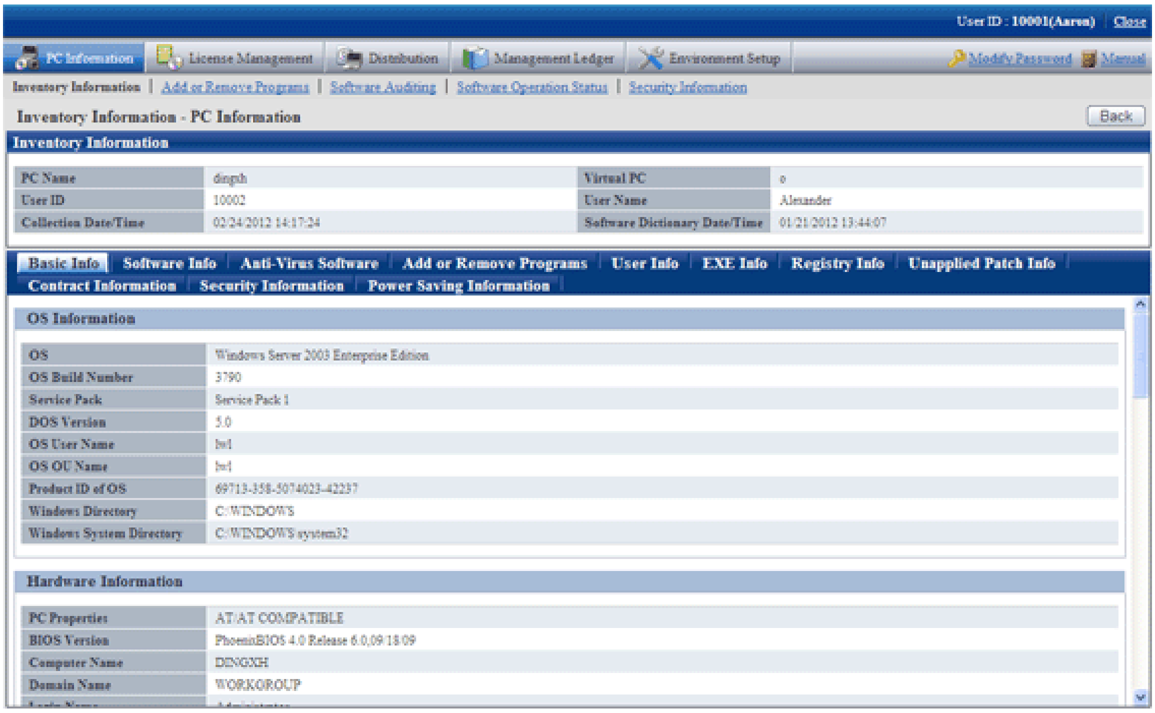
The information is mainly displayed in the “PC Information” - “Inventory Information” window of the main menu.

In addition, in the OS installed with Systemwalker Desktop Keeper V14.2.0, the above information of Systemwalker Desktop Patrol can be displayed by a click on the “Asset Information” link in the “Log Search” or “Log Details” window.

The display contents and pictures of information are shown below.

Basic Info (OS Information, Hardware Information)

Collect basic information of the PC (OS information, Hardware information).



Inventory Information - PC Information

Inventory Information

PC Name	dingxh	Virtual PC	0
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

OS Information

OS	Windows Server 2003 Enterprise Edition
OS Build Number	3790
Service Pack	Service Pack 1
DOS Version	5.0
OS User Name	lwl
OS OU Name	lwl
Product ID of OS	69713-358-5074023-42237
Windows Directory	C:\WINDOWS
Windows System Directory	C:\WINDOWS\system32

Hardware Information

PC Properties	AT/AT COMPATIBLE
BIOS Version	PhoenixBIOS 4.0 Release 6.0,09/18/09
Computer Name	DINGXH
Domain Name	WORKGROUP

As far as hardware information, collectable Inventory information may be variable with items that can be confirmed due to different OS (Operating System). Collectable hardware information is listed in the following table.

Class	Item Name	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
Hardware Information	PC Properties	○	○	○	○	○	○	○	○	○	
	BIOS Version	△	△	△	△	△	△	△	△	△	
	Computer Name	○	○	○	○	○	○	○	○	○	
	Domain Name	○	○	○	○	○	○	○	○	○	Obtain the group name if domain setup is not available.
	Login Name	○	○	○	○	○	○	○	○	○	
	CPU Name	○	○	○	○	○	○	○	○	○	
	CPU Clock Speed	△	△	△	△	△	△	△	△	△	To be obtained if CPU performance is higher than Pentium
	Number of CPU	○	○	○	○	○	○	○	○	○	
	CPU Details	○	○	○	○	○	○	○	○	○	
	Memory Size	○	○	○	○	○	○	○	○	○	In the PC installed with Vista (32 bit) SP1 above or Windows 7 (32 bit), if the physical memory exceeds 4G, the collected size of the memory will be different from that displayed in the “Control Panel” - “System” window.
	Swap File Size	○	○	○	○	○	○	○	○	○	

Class	Item Name	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
	Name of Keyboard Type	○	○	○	○	○	○	○	○	○	
	Installing Language	○	○	○	○	○	○	○	○	○	
	Mouse Type Name	○	○	○	○	○	○	○	○	○	
	Mouse Button Number	○	○	○	○	○	○	○	○	○	
	Manufacturer Name	△	△	△	△	△	△	△	△	△	
	Model Name	△	△	△	△	△	△	△	△	△	
	Serial Number	△	△	△	△	△	△	△	△	△	
	Primary Cache/ Secondary Cache	△	△	△	△	△	△	△	△	△	
OS Information	OS	○	○	○	○	○	○	○	○	○	
	OS Build Number	○	○	○	○	○	○	○	○	○	
	Service Pack	○	○	○	○	○	○	○	○	○	E.g. Displayed as “ServicePack X”. If the OS is Windows Server® 2003 R2, add “R2” to it. E.g. Service Pack 1, R2.
	DOS Version	○	○	×	○	×	○	×	○	×	
	OS User Name	○	○	△	△	△	△	△	△	△	If OS is Vista, Vista x64 Edition, or Windows 7, collect the user name originally created when installing the OS. If the OS is 2008, 2008 x64 Edition or 2008 R2, collect “Windows User”.
	OS OU Name	○	○	△	-	-	-	-	-	-	
	Prdocut ID of OS	○	○	○	○	○	○	○	○	○	
	Windows Directory	○	○	○	○	○	○	○	○	○	
	Windows System directory	○	○	○	○	○	○	○	○	○	
Displayer Information	Screen Resolution	○	○	○	○	○	○	○	○	○	
	Video Adapter	○	○	○	○	○	○	○	○	○	
	Video Memory Size	○	○	○	○	○	○	○	○	○	
	Resolution	○	○	○	○	○	○	○	○	○	

Class	Item Name	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
	Monitor (Note 2)	△	△	△	△	△	△	△	△	△	
	Screen Saver Name	○	○	○	○	○	○	○	○	○	
	Screen Refresh Rate	×	×	×	×	×	×	×	×	×	The information will be displayed if an old CT is installed in the OS earlier than Windows 2000.
Drive information (Note 2)	Drive Name	△	△	△	△	△	△	△	△	△	
	Drive Type	△	△	△	△	△	△	△	△	△	
	Drive Capacity	△	△	△	△	△	△	△	△	△	
	Drive Free Capacity	△	△	△	△	△	△	△	△	△	
	Volumel	△	△	△	△	△	△	△	△	△	
	File System Type	△	△	△	△	△	△	△	△	△	
CD-ROM information	Device Name	△	△	△	△	△	△	△	△	△	
Disk Inforamtion	Manufacturer Name	△	△	△	△	△	△	△	△	△	
	Model Name	△	△	△	△	△	△	△	△	△	
	Disk capacity	○	○	○	○	○	○	○	○	○	
	Disk IF	△	△	△	△	△	△	△	△	△	
	Description	○	○	○	○	○	○	○	○	○	
Memory Information	Device Locator	△	△	△	△	△	△	△	△	△	
	Size	△	△	△	△	△	△	△	△	△	
Network card information (Note 1)	Network Card	○	○	△	△	△	△	△	△	△	Multiple results can be obtained. To obtain the logical names when grouping the multiple network cards.
	MAC Address	○	○	○	○	○	○	○	○	○	Multiple results can be obtained.
TCP/IP Information	Host name	○	○	○	○	○	○	○	○	○	Multiple results can be obtained
	IP Address	○	○	○	○	○	○	○	○	○	
	Subnet Mask	○	○	○	○	○	○	○	○	○	
	Default Gateway	○	○	○	○	○	○	○	○	○	
	DHCP Server	○	○	○	○	○	○	○	○	○	
	DNS Server	○	○	△	△	△	△	△	△	△	
Network sharing	Network Path Name	△	△	△	△	△	△	△	△	△	

Class	Item Name	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
information (Note 2)	Network Service Supplier Name	△	△	△	△	△	△	△	△	△	
	Drive Letter	△	△	△	△	△	△	△	△	△	
Printer Information (Note 2)	Printer Name	△	△	△	△	△	△	△	△	△	
	Printer Type	△	△	△	△	△	△	△	△	△	

○: Collectable.

△: May be not collectable according to the type of OS and device.

×: Not collectable.

-: Uncollected or no corresponding information.

XP: Windows® XP

2003: Windows Server® 2003

2003 x64: Windows Server® 2003 x64 Edition

Vista: Windows Vista®

Vista 64bit: Windows Vista® x64 Edition

7: Windows® 7

7 64bit: Windows® 7 x64 Edition

2008: Windows Server® 2008

2008 64bit: Windows Server® 2008 x64 Edition

Note 1:

- During the application of DHCP, if IP address can not be distributed due to inexistence of DHCP server, it is required to automatically form network connection IP (Internet Protocol) via APIPA (Automatic Private IP Addressing). Then, the PC will automatically distribute and obtain private IP address within the IP address scope reserved by Microsoft Corporation from 169.254.0.1 and 169.254.255.254.
- When the spare TCP/IP address is set in Windows® XP, Windows Server® 2003, Windows Vista®, Windows® or Windows Server® 2008, the TCP/IP value distributed by the DHCP server can be obtained.
- If the DHCP server does not exist, please use the private IP address obtained automatically or the TCP/IP value set in user information. If DHCP is used, the DHCP server can be obtained.
- Network card information or TCP/IP information can not be obtained through Inventory collection under the following conditions. In addition, set NULL in IP address, or do not collect Inventory information.
  - Network card is not installed
  - Network card is disabled
  - Network cable is disconnected
  - IP address is not distributed in the DHCP environment.
  - IP address is not distributed in wireless LAN environment.
  - The network adapter has no effective IP address.

  If Inventory information has not been collected, please collect it by any of the following methods.

  1. Collect the Inventory information in command mode CT.
  2. Insert the network cable in the original network adapter for connection.
  3. Set the properties of adapter as “Network Adapter”, and apply VPN to PPP.

- Obtain IP addresses in ascending order. The finally obtained IP address shall be NULL.
- If DHCP is applied, DNS server information obtained from DHCP server can not be collected.

Note 2:

The following hardware information can not be collected when collecting Inventory information via agent mode, but it can be normally collected via command mode.

- Screen Saver

  The screen saver set by the user in “Display Properties” is not collectable, but the screen saver for the initial setting of OS which is displayed when logging in will be collected.

OS	Collected Screen Saver
Windows® XP	Windows XP
Windows Server® 2003	Windows Server 2003
Windows Vista®	Windows sign
Windows® 7	Windows sign
Windows Server® 2008	Windows sign

- Drive information

  Network drive belongs to dynamic information of the registered user unit; it can be collected in the CT executed by the login user in command mode. The information can not be browsed via the service (SYSTEM authority) agent mode.

  Drive information is collectable when the shared folder of the device in the domain to which the CT belongs is distributed to the network drive.

- Network sharing information

  Network sharing information is uncollected.

- Printer information

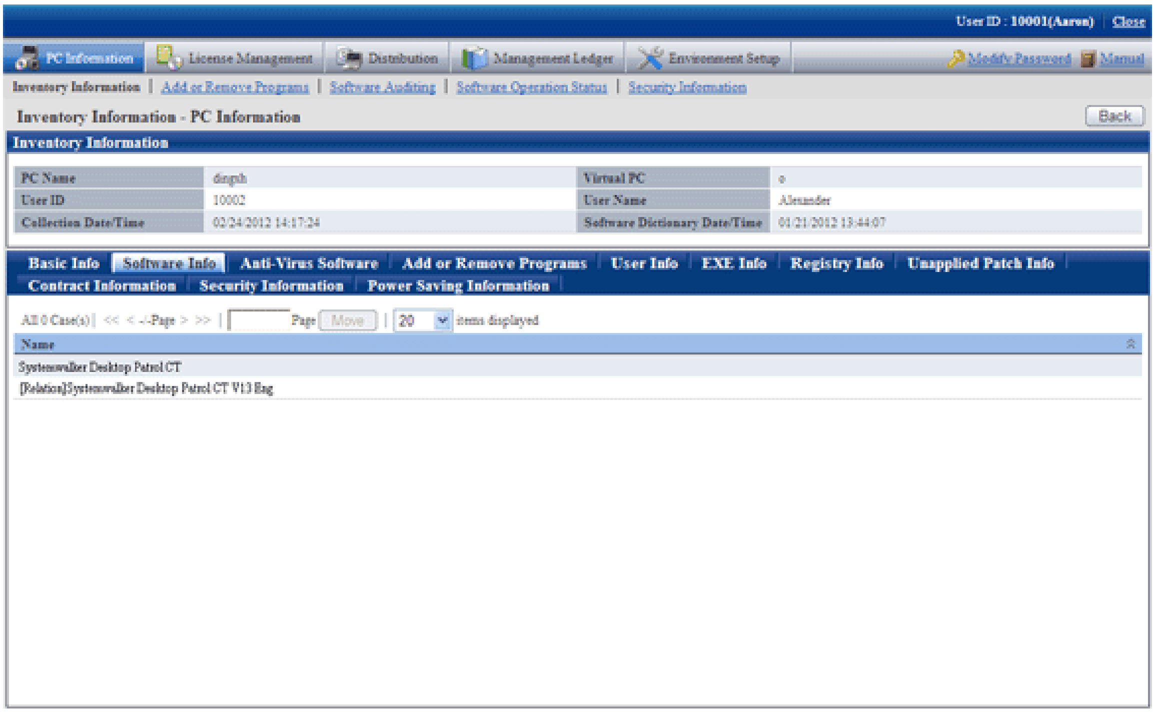
  Printer information can be collected through Inventory collection in command mode. Inventory collection is impossible in agent mode.

Software Info

Collect the installation software via the retrieval function of “Software Info” of Systemwalker Desktop Patrol.

Retrieval conditions are shown below:

- File retrieval
  - File (including directory) name retrieval
  - File date consistency and scope retrieval
  - Condition retrieval of file size (equal, more than, less than)
  - Condition retrieval of file version (equal, above)
- Registry retrieval
  - Retrieval according to the “Add or Delete Programs” information name
  - Retrieval according to any registry (Key Name, Value Name)


User ID : 10001(Aaron) | Close

PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual

Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information

Inventory Information - PC Information

Inventory Information

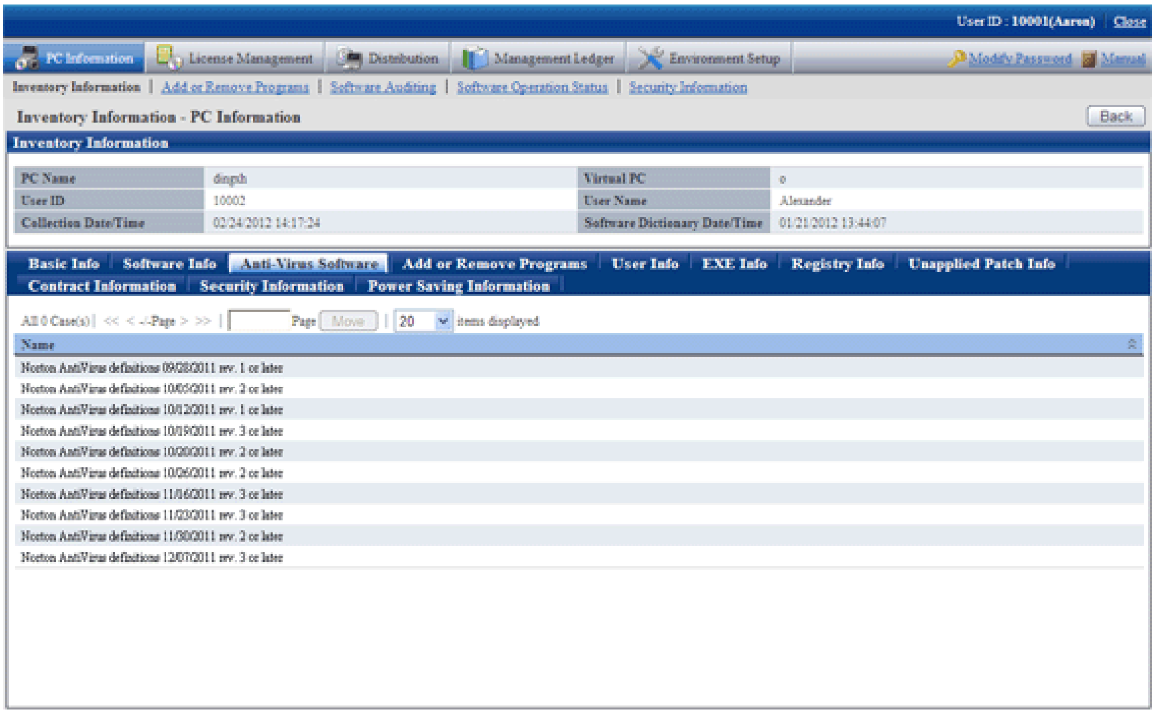
PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

Basic Info | Software Info | Anti-Virus Software | Add or Remove Programs | User Info | EXE Info | Registry Info | Unapplied Patch Info
Contract Information | Security Information | Power Saving Information
All 0 Case(s) | << < -/-Page > >> | Page Move | 20 items displayed

Name
Systemwalker Desktop Patrol CT
[Relation]Systemwalker Desktop Patrol CT V13 Eng

Anti-Virus Software

Collect the anti-virus software installed in the PC.


User ID : 10001(Aaron) | Close

PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual

Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information

Inventory Information - PC Information

Inventory Information

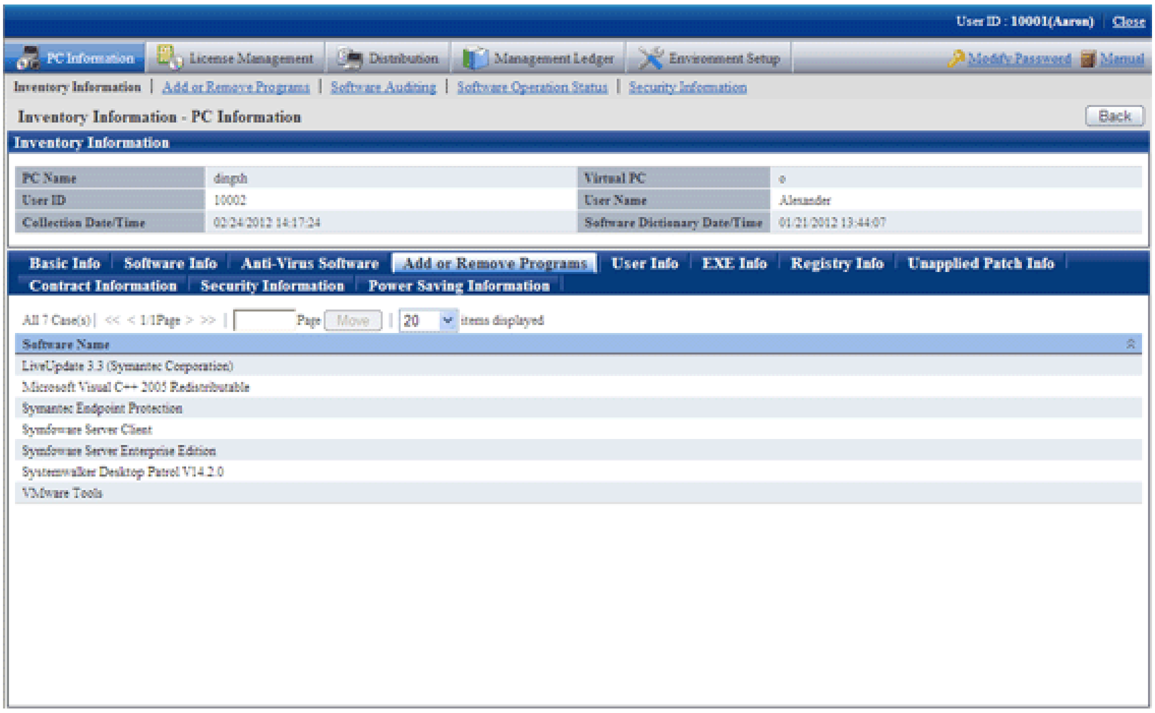
PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

Basic Info | Software Info | Anti-Virus Software | Add or Remove Programs | User Info | EXE Info | Registry Info | Unapplied Patch Info
Contract Information | Security Information | Power Saving Information
All 0 Case(s) | << < -/-Page > >> | Page Move | 20 items displayed

Name
Norton AntiVirus definitions 09/28/2011 rev. 1 or later
Norton AntiVirus definitions 10/05/2011 rev. 2 or later
Norton AntiVirus definitions 10/12/2011 rev. 1 or later
Norton AntiVirus definitions 10/19/2011 rev. 3 or later
Norton AntiVirus definitions 10/20/2011 rev. 2 or later
Norton AntiVirus definitions 10/26/2011 rev. 2 or later
Norton AntiVirus definitions 11/16/2011 rev. 3 or later
Norton AntiVirus definitions 11/23/2011 rev. 3 or later
Norton AntiVirus definitions 11/30/2011 rev. 2 or later
Norton AntiVirus definitions 12/07/2011 rev. 3 or later

Add or Remove Programs

Collect the program addition & deletion information of the PC.



Inventory Information - PC Information

Inventory Information

PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

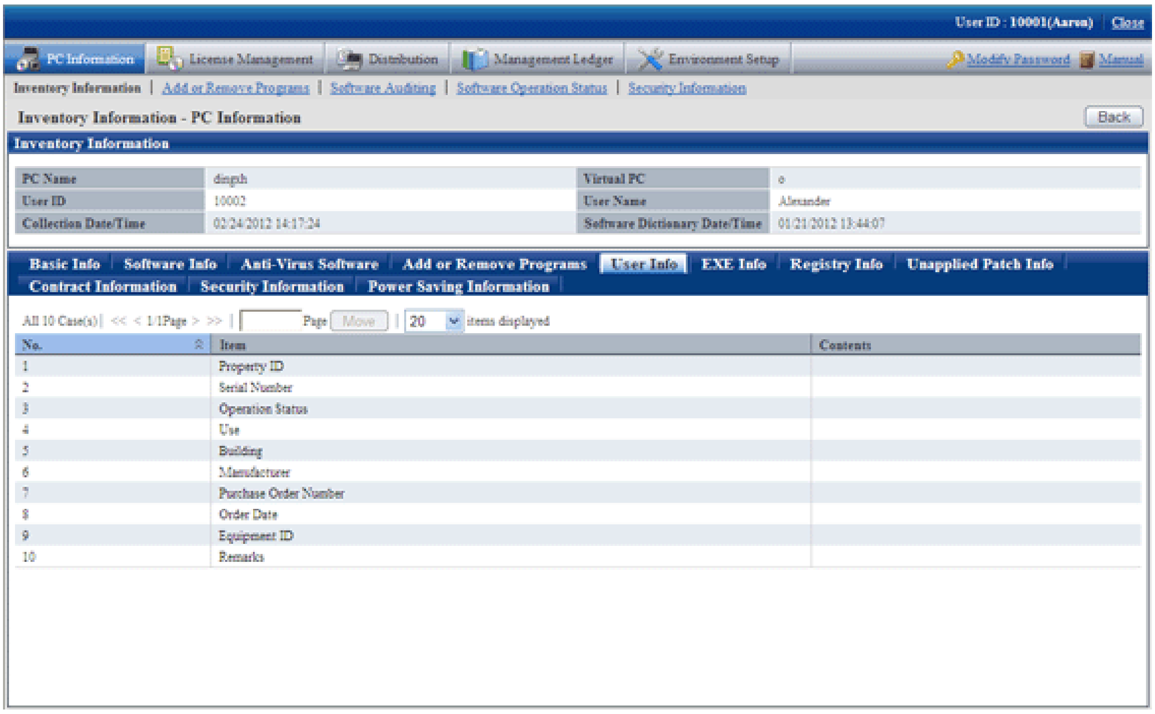
Software Name
LiveUpdate 3.3 (Symantec Corporation)
Microsoft Visual C++ 2005 Redistributable
Symantec Endpoint Protection
Symfoware Server Client
Symfoware Server Enterprise Edition
Systemwalker Desktop Patrol V14.2.0
VMware Tools

User Info

Consider any information set by the system administrator as “User Info” and collect it together with Inventory information.

Collect the user information entered by the PC user in the PC window.

10 cases of user information can be registered or changed at most.



Inventory Information - PC Information

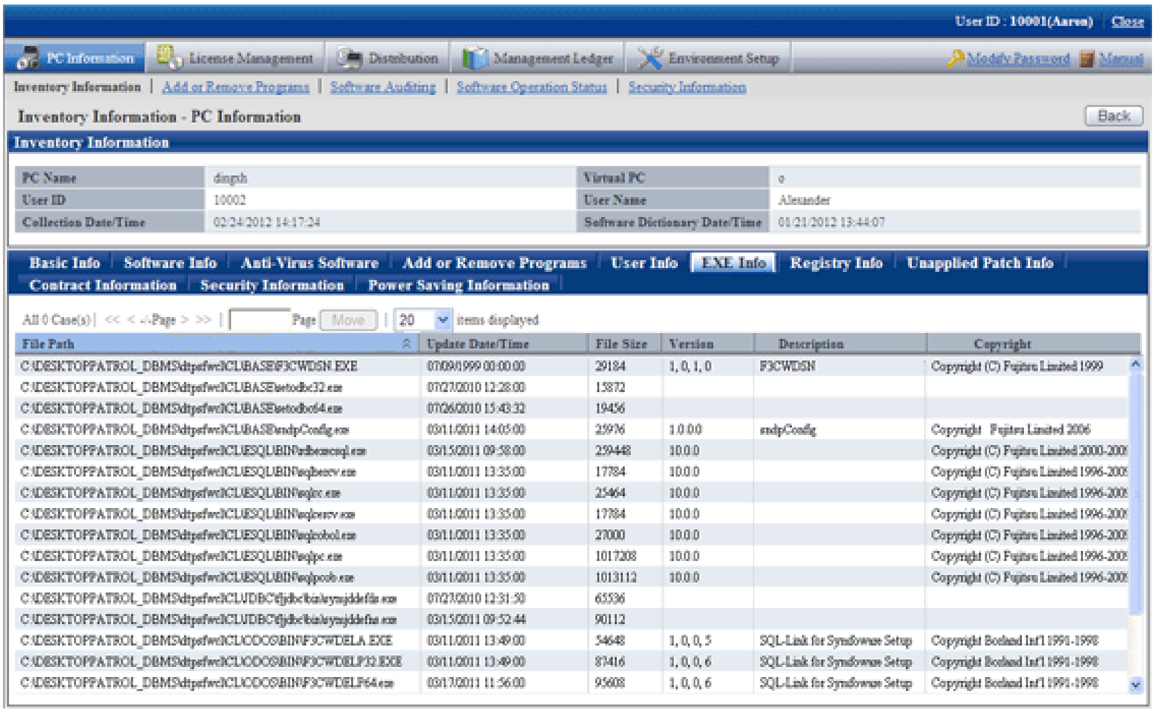
Inventory Information

PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

No.	Item	Contents
1	Property ID	
2	Serial Number	
3	Operation Status	
4	Use	
5	Building	
6	Manufacturer	
7	Purchase Order Number	
8	Order Date	
9	Equipement ID	
10	Remarks	

EXE Info

The user can collect the properties information of all execution files (files whose extension name is .exe) in the PC.



Inventory Information - PC Information

Inventory Information

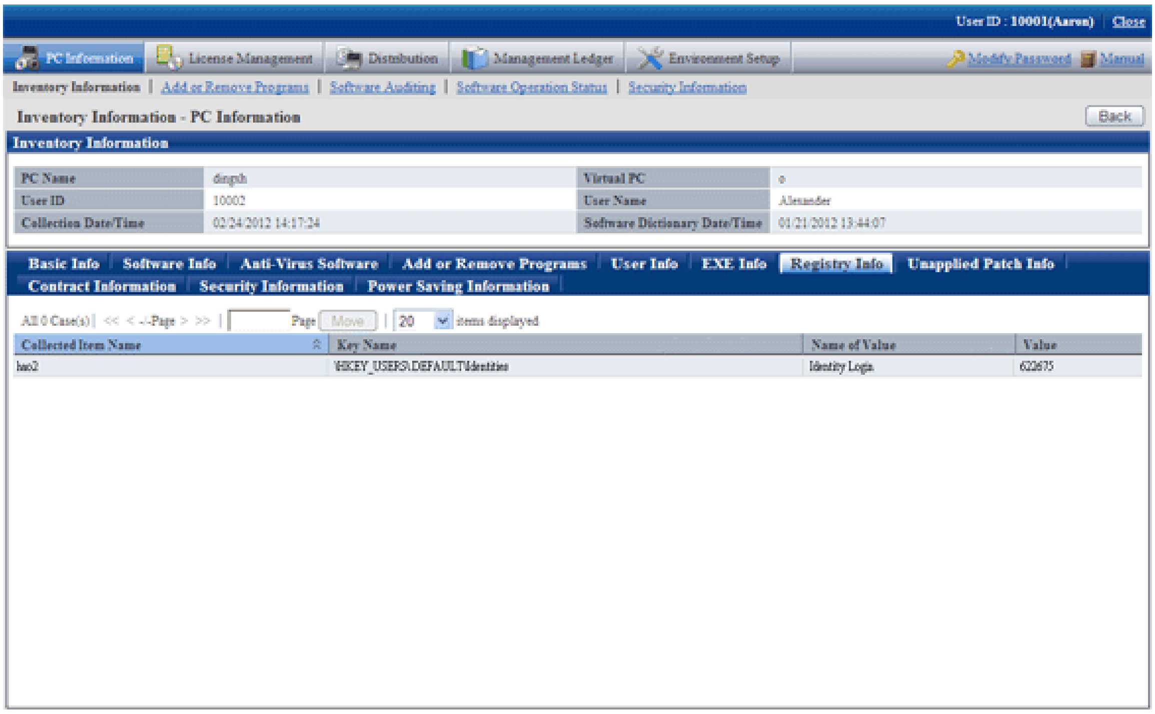
PC Name	dingzh	Virtual PC	○
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

File Path	Update Date/Time	File Size	Version	Description	Copyright
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\BASE\F3CWDSN.EXE	07/09/1999 00:00:00	29184	1, 0, 1, 0	F3CWDSN	Copyright (C) Fujitsu Limited 1999
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\BASE\setodbc32.exe	07/27/2010 12:28:00	15872			
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\BASE\setodbc64.exe	07/26/2010 15:43:32	19456			
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\BASE\sndpConfig.exe	03/11/2011 14:05:00	25976	1.0.0.0	sndpConfig	Copyright Fujitsu Limited 2006
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\rdbexecsql.exe	03/15/2011 09:58:00	259448	10.0.0		Copyright (C) Fujitsu Limited 2000-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlbserv.exe	03/11/2011 13:35:00	17784	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlcc.exe	03/11/2011 13:35:00	23464	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlcserv.exe	03/11/2011 13:35:00	17784	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlcobol.exe	03/11/2011 13:35:00	27000	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlpc.exe	03/11/2011 13:35:00	1017208	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ESQL\BIN\sqlpcob.exe	03/11/2011 13:35:00	1013112	10.0.0		Copyright (C) Fujitsu Limited 1996-200
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\JDBC\fjjdbc\bin\asymjddefile.exe	07/27/2010 12:31:50	65536			
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\JDBC\fjjdbc\bin\asymjddefna.exe	03/15/2011 09:52:44	90112			
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ODOS\BIN\F3CWDELA.EXE	03/11/2011 13:49:00	54648	1, 0, 0, 5	SQL-Link for Symfoware Setup	Copyright Borland Int'l 1991-1998
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ODOS\BIN\F3CWDELP32.EXE	03/11/2011 13:49:00	87416	1, 0, 0, 6	SQL-Link for Symfoware Setup	Copyright Borland Int'l 1991-1998
C:\DESKTOPPATROL_DBMS\dtpsfwcl\CL\ODOS\BIN\F3CWDELP64.exe	03/17/2011 11:56:00	95608	1, 0, 0, 6	SQL-Link for Symfoware Setup	Copyright Borland Int'l 1991-1998

Registry Info

The information in the registry of OS can be collected by the specified key name or value name.

The registry information is shown in the main menu as follows:



Inventory Information - PC Information

Inventory Information

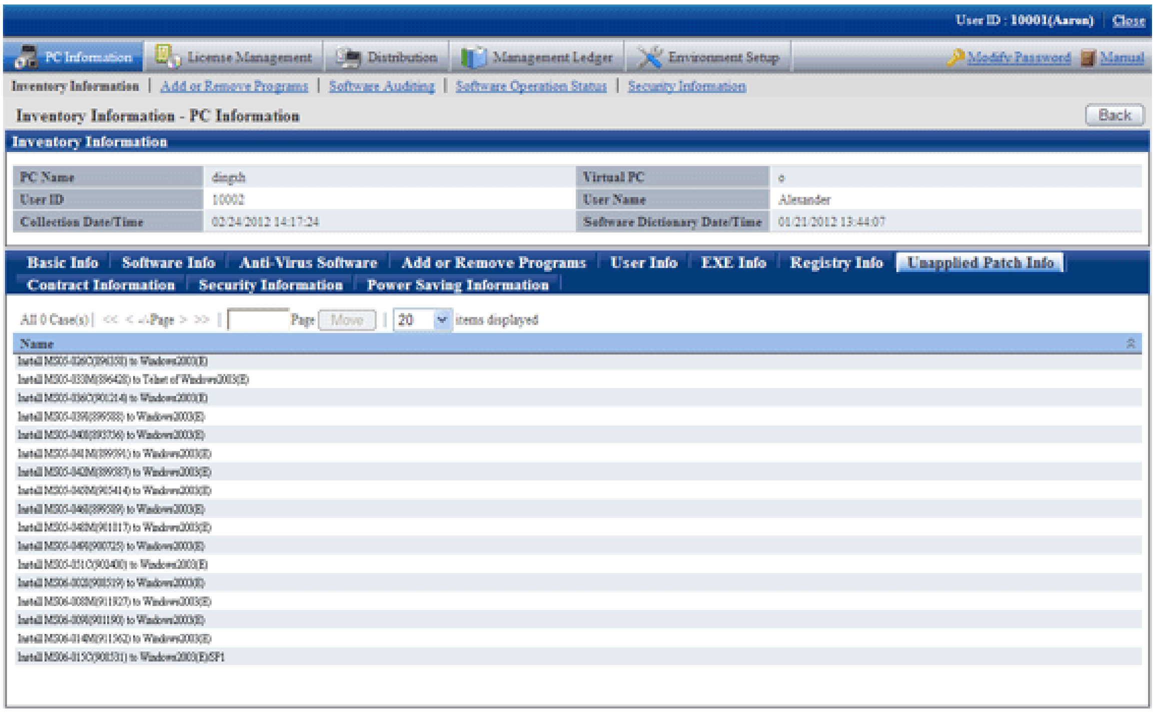
PC Name	dingzh	Virtual PC	○
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

Collected Item Name	Key Name	Name of Value	Value
hao2	\HKEY_USERS\.DEFAULT\Identities	Identity Login	622675

Unapplied Patch Info

The user can browse the information of automatic application patches unapplied to the CT

The information of unapplied patches is shown in the main menu as follows:



User ID : 10001(Aaron) | Close

Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information

Inventory Information - PC Information

Inventory Information

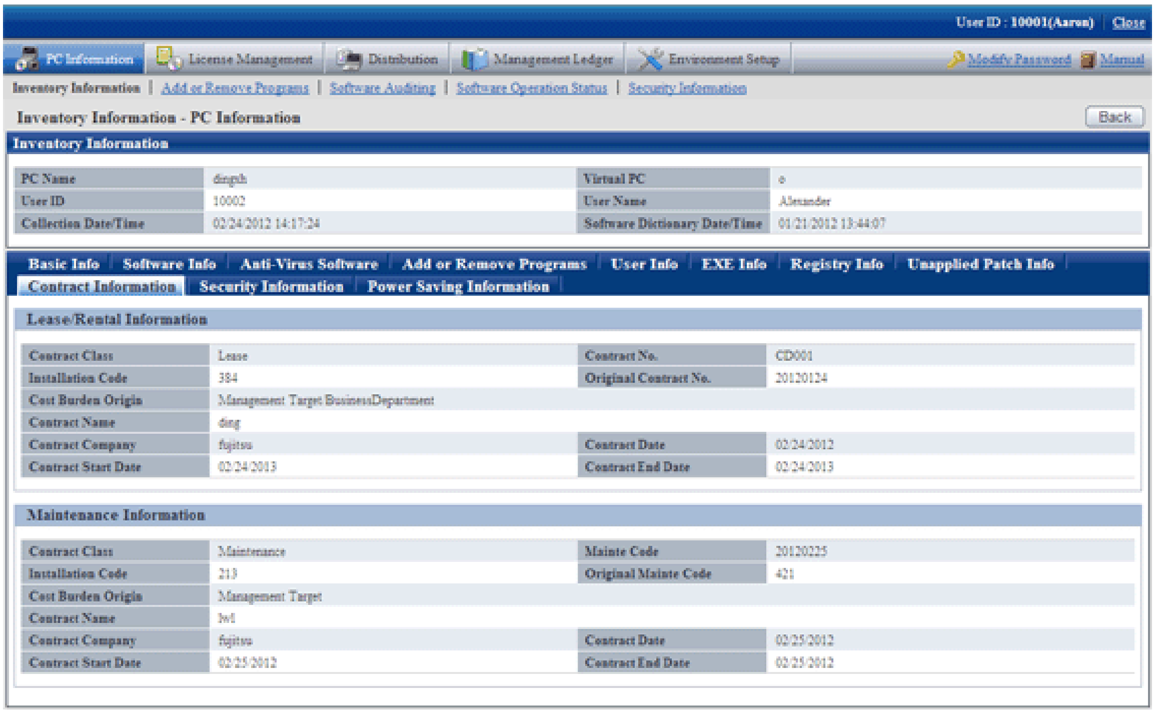
PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

All 0 Case(s) | << < -/-Page > >> | Page Move | 20 items displayed

Name
Install MS05-026C(896358) to Windows2003(E)
Install MS05-033M(896428) to Telnet of Windows2003(E)
Install MS05-036C(901214) to Windows2003(E)
Install MS05-039I(899588) to Windows2003(E)
Install MS05-040I(893756) to Windows2003(E)
Install MS05-041M(899591) to Windows2003(E)
Install MS05-042M(899587) to Windows2003(E)
Install MS05-043M(905414) to Windows2003(E)
Install MS05-046I(899589) to Windows2003(E)
Install MS05-048M(901017) to Windows2003(E)
Install MS05-049I(900725) to Windows2003(E)
Install MS05-051C(902400) to Windows2003(E)
Install MS06-002I(908519) to Windows2003(E)
Install MS06-008M(911927) to Windows2003(E)
Install MS06-009I(901190) to Windows2003(E)
Install MS06-014M(911562) to Windows2003(E)
Install MS06-015C(908531) to Windows2003(E)SP1

Contract Information

The user can browse the contract information of the PC (lease/rent/maintenance).



User ID : 10001(Aaron) | Close

Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information

Inventory Information - PC Information

Inventory Information

PC Name	dingzh	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

Lease/Rental Information

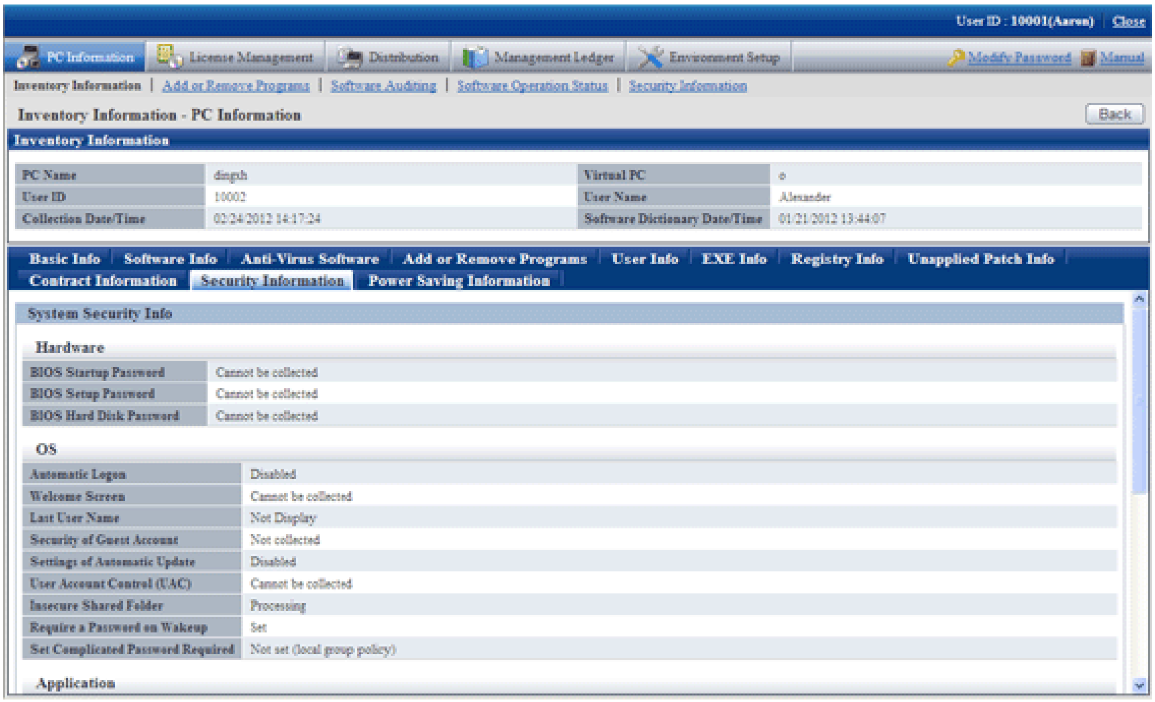
Contract Class	Lease	Contract No.	CD001
Installation Code	384	Original Contract No.	20120124
Cost Burden Origin	Management Target BusinessDepartment		
Contract Name	ding		
Contract Company	fujitsu	Contract Date	02/24/2012
Contract Start Date	02/24/2013	Contract End Date	02/24/2013

Maintenance Information

Contract Class	Maintenance	Mainte Code	20120225
Installation Code	213	Original Mainte Code	421
Cost Burden Origin	Management Target		
Contract Name	lwl		
Contract Company	fujitsu	Contract Date	02/25/2012
Contract Start Date	02/25/2012	Contract End Date	02/25/2012

Security Information

The user can browse the security information of the PC.



Inventory Information - PC Information

Inventory Information

PC Name	dmpth	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

System Security Info

Hardware

BIOS Startup Password	Cannot be collected
BIOS Setup Password	Cannot be collected
BIOS Hard Disk Password	Cannot be collected

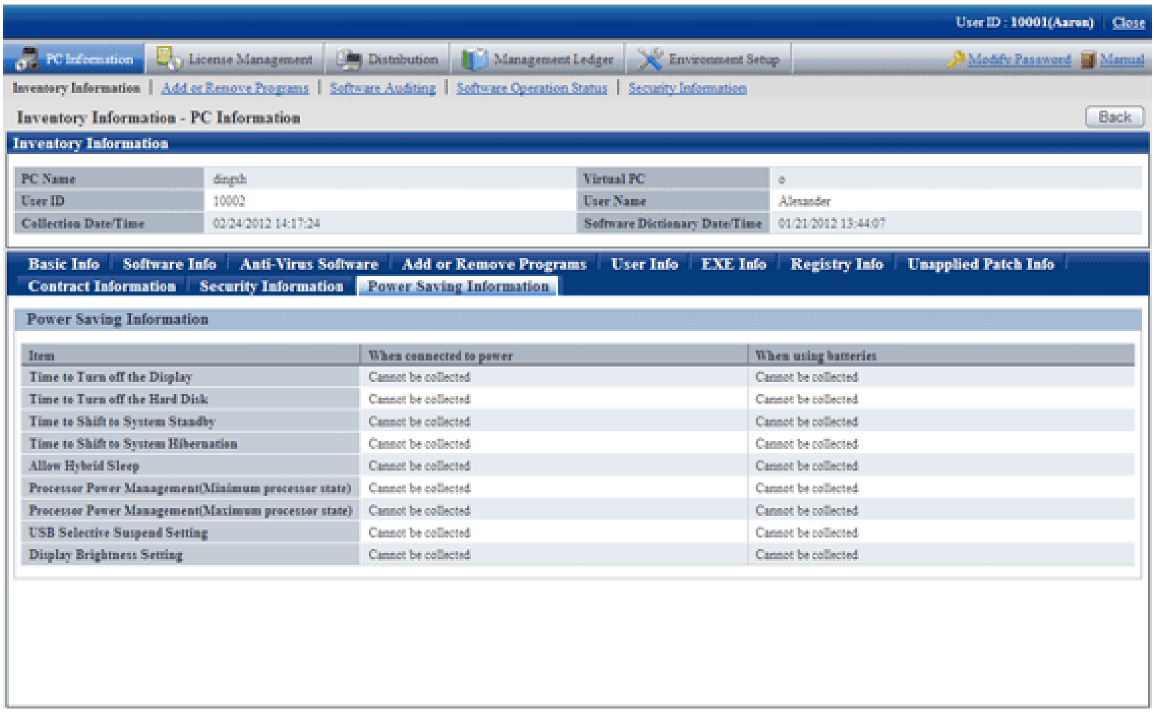
OS

Automatic Logon	Disabled
Welcome Screen	Cannot be collected
Last User Name	Not Display
Security of Guest Account	Not collected
Settings of Automatic Update	Disabled
User Account Control (UAC)	Cannot be collected
Insecure Shared Folder	Processing
Require a Password on Wakeup	Set
Set Complicated Password Required	Not set (local group policy)

Application

Power Saving Information

The user can browse the power saving information of the PC.



Inventory Information - PC Information

Inventory Information

PC Name	dmpth	Virtual PC	o
User ID	10002	User Name	Alexander
Collection Date/Time	02/24/2012 14:17:24	Software Dictionary Date/Time	01/21/2012 13:44:07

Power Saving Information

Item	When connected to power	When using batteries
Time to Turn off the Display	Cannot be collected	Cannot be collected
Time to Turn off the Hard Disk	Cannot be collected	Cannot be collected
Time to Shift to System Standby	Cannot be collected	Cannot be collected
Time to Shift to System Hibernation	Cannot be collected	Cannot be collected
Allow Hybrid Sleep	Cannot be collected	Cannot be collected
Processor Power Management(Minimum processor state)	Cannot be collected	Cannot be collected
Processor Power Management(Maximum processor state)	Cannot be collected	Cannot be collected
USB Selective Suspend Setting	Cannot be collected	Cannot be collected
Display Brightness Setting	Cannot be collected	Cannot be collected

Display of log retrieval window of Systemwalker Desktop Keeper

In the system installed with Systemwalker Desktop Keeper V14.2.0, the “Log Retrieval” window of Systemwalker Desktop Keeper can be displayed by a click on the “Log Management” link in the “PC Information” - “Inventory Information” window of main menu.

2.1.3 Program Addition & Deletion Information

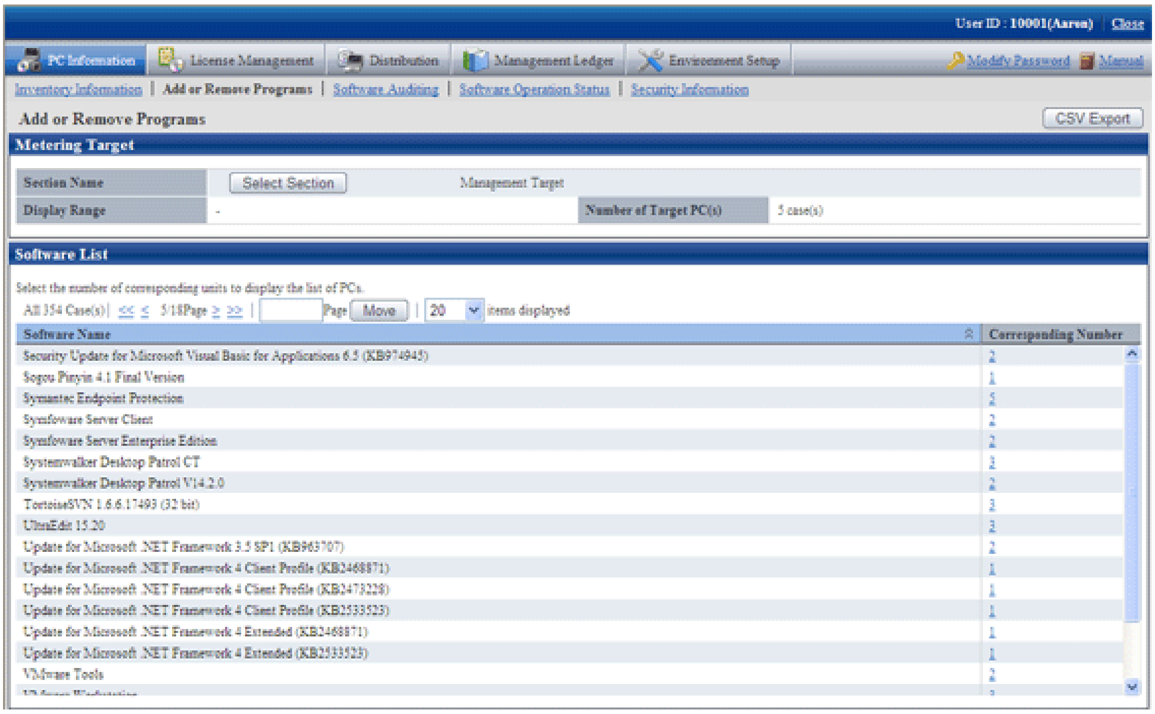
Automatically collect the software displayed in the “Add or Remove Programs” information.

The information will be used when performing license management on the applications set in the “Add or Delete Applications”, “Add or Delete Programs” or “Program and Function” after installation.

In addition, the update programs (Microsoft Office, etc) except OS update programs can not be collected.

The program information is displayed in the “PC Information” - “Add or Remove Programs” window of main menu.

The display picture is shown below:



User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information
CSV Export
Select Section
Move

Add or Remove Programs

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Target PC(s)	5 case(s)

Software List

Select the number of corresponding units to display the list of PCs.

All 354 Case(s) | << < 5/18Page > >> | Page Move | 20 items displayed

Software Name	Corresponding Number
Security Update for Microsoft Visual Basic for Applications 6.5 (KB974945)	2
Sogou Pinyin 4.1 Final Version	1
Symantec Endpoint Protection	5
Symfoware Server Client	2
Symfoware Server Enterprise Edition	2
Systemwalker Desktop Patrol CT	3
Systemwalker Desktop Patrol V14.2.0	2
TortoiseSVN 1.6.6.17493 (32 bit)	3
UltraEdit 15.20	3
Update for Microsoft .NET Framework 3.5 SP1 (KB963707)	2
Update for Microsoft .NET Framework 4 Client Profile (KB2468871)	1
Update for Microsoft .NET Framework 4 Client Profile (KB2473228)	1
Update for Microsoft .NET Framework 4 Client Profile (KB2533523)	1
Update for Microsoft .NET Framework 4 Extended (KB2468871)	1
Update for Microsoft .NET Framework 4 Extended (KB2533523)	1
VMware Tools	2
VMware Workstation	3

Note

If program information is not collected

If the version of Windows installed in the PC is earlier than 3.0, it is impossible to collect the applications installed by the user.

2.1.4 Software Auditing Information

Software installation status, as audited object, can be browsed.

The auditing information that can be viewed is listed below:

- Software installation status
- Installation status of anti-virus software
- Application status of security patches

The PC to which the security patches of Microsoft Corporation are not applied can be found.

The PC in which computer anti-virus software is not installed can be found.

The PC to which the latest virus definition file of computer anti-virus software is not applied can be found.

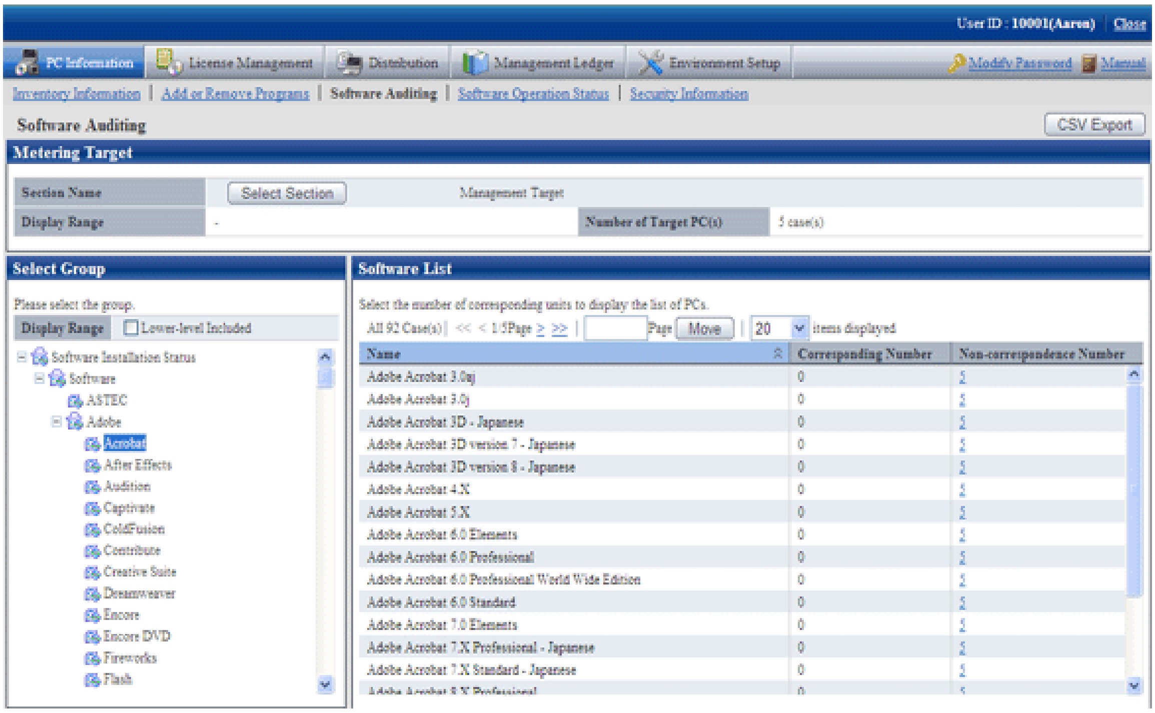
The administrator can find the PC in which potential computer virus and security breaches exist to improve the protective capability of the PC.

The information is displayed in the “PC Information” - “Software Auditing” window of main menu.

The display contents and pictures of different information are shown below:

Software installation status

The installation status of software managed by License and user defined software can be browsed.



Software Auditing

Metering Target

Section Name	Management Target		
Display Range	-	Number of Target PC(s)	5 case(s)

Select Group

Please select the group.

Display Range ☐ Lower-level Included

Software List

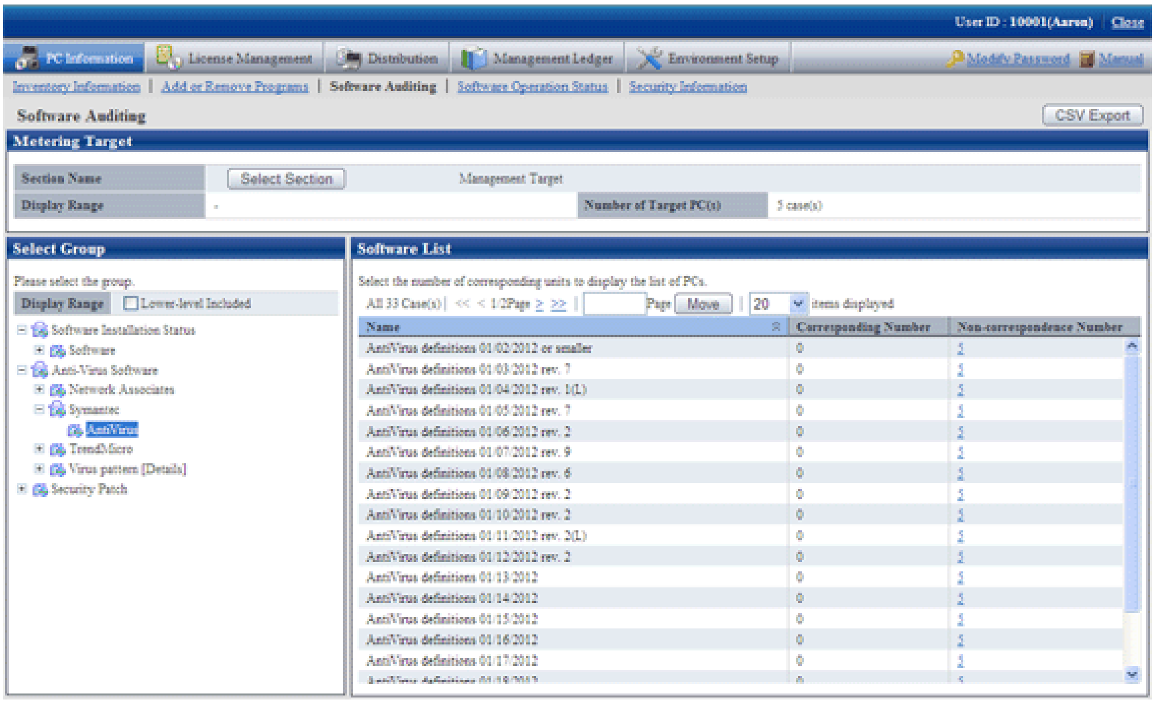
Select the number of corresponding units to display the list of PCs.

All 92 Case(s) | << < 1/5Page > >> | Page | 20 items displayed

Name	Corresponding Number	Non-correspondence Number
Adobe Acrobat 3.0aj	0	5
Adobe Acrobat 3.0j	0	5
Adobe Acrobat 3D - Japanese	0	5
Adobe Acrobat 3D version 7 - Japanese	0	5
Adobe Acrobat 3D version 8 - Japanese	0	5
Adobe Acrobat 4.X	0	5
Adobe Acrobat 5.X	0	5
Adobe Acrobat 6.0 Elements	0	5
Adobe Acrobat 6.0 Professional	0	5
Adobe Acrobat 6.0 Professional World Wide Edition	0	5
Adobe Acrobat 6.0 Standard	0	5
Adobe Acrobat 7.0 Elements	0	5
Adobe Acrobat 7.X Professional - Japanese	0	5
Adobe Acrobat 7.X Standard - Japanese	0	5
Adobe Acrobat 8.X Professional	0	5

Installation status of anti-virus software

The installation status of anti-virus software can be browsed.



Software Auditing

Metering Target

Section Name	Management Target		
Display Range	-	Number of Target PC(s)	5 case(s)

Select Group

Please select the group.

Display Range □ Lower-level Included

- ⊟ Software Installation Status
  - ⊞ Software
- ⊟ Anti-Virus Software
  - ⊞ Network Associates
  - ⊟ Symantec
    - AntiVirus
  - ⊞ TrendMicro
  - ⊞ Virus pattern [Details]
- ⊞ Security Patch

Software List

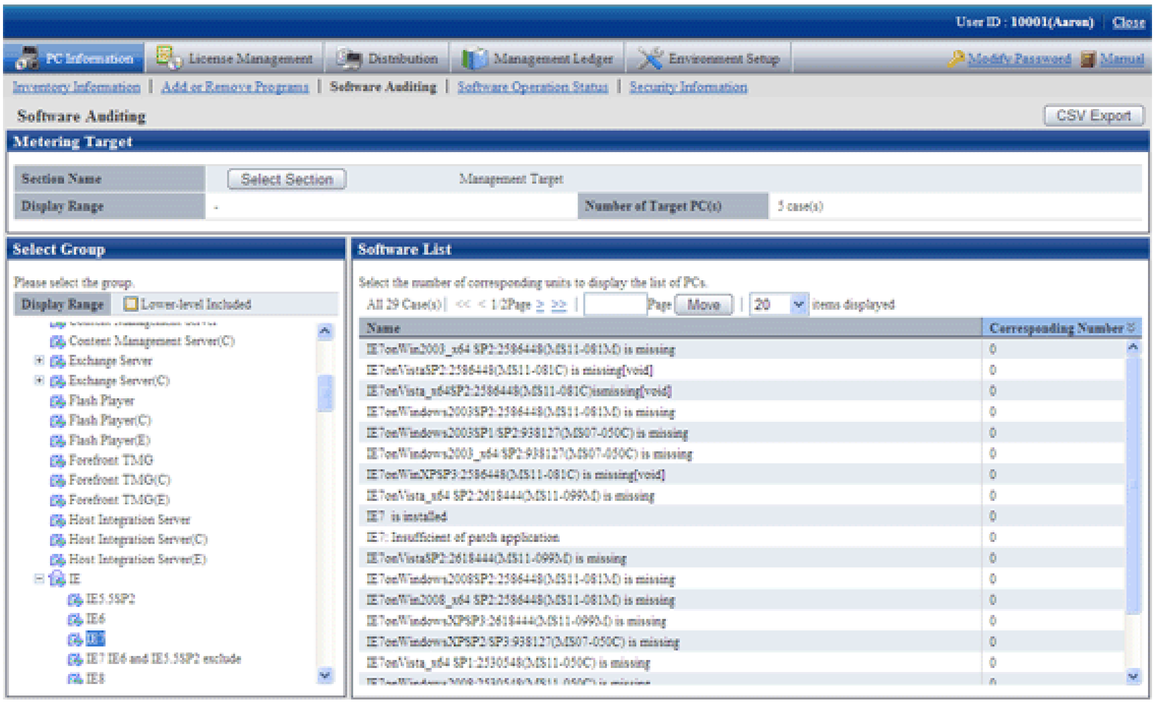
Select the number of corresponding units to display the list of PCs.

All 33 Case(s) | << < 1/2Page > >> | Page | 20 items displayed

Name	Corresponding Number	Non-correspondence Number
AntiVirus definitions 01/02/2012 or smaller	0	5
AntiVirus definitions 01/03/2012 rev. 7	0	5
AntiVirus definitions 01/04/2012 rev. 1(L)	0	5
AntiVirus definitions 01/05/2012 rev. 7	0	5
AntiVirus definitions 01/06/2012 rev. 2	0	5
AntiVirus definitions 01/07/2012 rev. 9	0	5
AntiVirus definitions 01/08/2012 rev. 6	0	5
AntiVirus definitions 01/09/2012 rev. 2	0	5
AntiVirus definitions 01/10/2012 rev. 2	0	5
AntiVirus definitions 01/11/2012 rev. 2(L)	0	5
AntiVirus definitions 01/12/2012 rev. 2	0	5
AntiVirus definitions 01/13/2012	0	5
AntiVirus definitions 01/14/2012	0	5
AntiVirus definitions 01/15/2012	0	5
AntiVirus definitions 01/16/2012	0	5
AntiVirus definitions 01/17/2012	0	5

Usage status of security patches

The usage status of security patches can be browsed.



Software Auditing

Metering Target

Section Name	Management Target		
Display Range	-	Number of Target PC(s)	5 case(s)

Select Group

Please select the group.

Display Range □ Lower-level Included

- Content Management Server(C)
- ⊞ Exchange Server
- ⊞ Exchange Server(C)
- Flash Player
- Flash Player(C)
- Flash Player(E)
- Forefront TMG
- Forefront TMG(C)
- Forefront TMG(E)
- Host Integration Server
- Host Integration Server(C)
- Host Integration Server(E)
- ⊟ IE
  - IE5.5SP2
  - IE6
  - IE7
  - IE7 IE6 and IE5.5SP2 exclude
  - IE8

Software List

Select the number of corresponding units to display the list of PCs.

All 29 Case(s) | << < 1/2Page > >> | Page | 20 items displayed

Name	Corresponding Number
IE7onWin2003_x64 SP2:2586448(MS11-081M) is missing	0
IE7onVistaSP2:2586448(MS11-081C) is missing[void]	0
IE7onVista_x64SP2:2586448(MS11-081C)ismissing[void]	0
IE7onWindows2003SP2:2586448(MS11-081M) is missing	0
IE7onWindows2003SP1/SP2:938127(MS07-050C) is missing	0
IE7onWindows2003_x64/SP2:938127(MS07-050C) is missing	0
IE7onWinXPSP3:2586448(MS11-081C) is missing[void]	0
IE7onVista_x64 SP2:2618444(MS11-099M) is missing	0
IE7 is installed	0
IE7: Insufficient of patch application	0
IE7onVistaSP2:2618444(MS11-099M) is missing	0
IE7onWindows2008SP2:2586448(MS11-081M) is missing	0
IE7onWin2008_x64 SP2:2586448(MS11-081M) is missing	0
IE7onWindowsXPSP3:2618444(MS11-099M) is missing	0
IE7onWindowsXPSP2/SP3:938127(MS07-050C) is missing	0
IE7onVista_x64 SP1:2530548(MS11-050C) is missing	0

2.1.5 Software Operation Status

Besides the information of installed software, the operation status of software can also be collected.

Software operation status relates to software information, so we can judge whether the software is the execution file for actual running in the “Software Operation Status” of “Software Dictionary” at first, and then browse by the easily understandable registered name in the “Software Dictionary”.

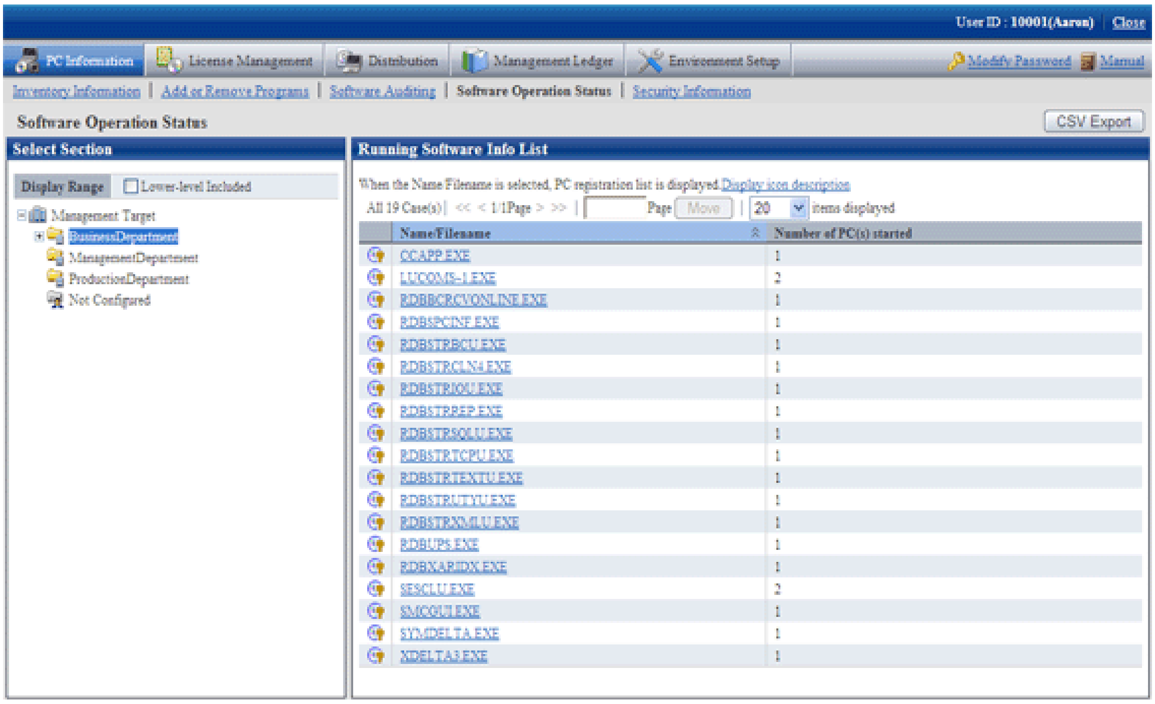
Effective utilization of assets can be realized through browsing the software operation status. For example, although license has been distributed and software has been installed, if software is not applied, dormant assets can be reduced by distributing the License to other users in need.

Software operation status is displayed as follows in the main menu:

Software operation status can not be collected in command mode.

Software operation status is displayed in the “PC Information” - “Software Operation Status” window of main menu.

Display contents and pictures of different information are shown below:



When the Name/Filename is selected, PC registration list is displayed. Display icon description

All 19 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Name/Filename	Number of PC(s) started
CCAPP.EXE	1
LUCOMS~1.EXE	2
RDBBCRCVONLINE.EXE	1
RDBSPCINF.EXE	1
RDBSTRBCU.EXE	1
RDBSTRCLN4.EXE	1
RDBSTRIOU.EXE	1
RDBSTRREP.EXE	1
RDBSTRSQLU.EXE	1
RDBSTRTCPU.EXE	1
RDBSTRTEXTU.EXE	1
RDBSTRUTYU.EXE	1
RDBSTRXMLU.EXE	1
RDBUPS.EXE	1
RDBXARIDX.EXE	1
SESCLU.EXE	2
SMCGUI.EXE	1
SYMDELTA.EXE	1
XDELTA3.EXE	1

Note

The following EXE files can not be obtained through collection of software operation status.

- .exe files installed when installing Windows (notepad.exe, iexplore.exe, wordpad.exe, etc)
- Process of Systemwalker Desktop Patrol on CS/DS/CT.

2.1.6 Security Information

The following security information functions can be provided.

The PCs having lower security setup level in automatic logon and screen saver can be found via these functions.

The administrator can find the PC in which potential computer virus and security breaches exist to improve the protective capability of the PC.

Security information is displayed in the “PC Information” - “Security Information” window of main menu.

The security information of the PC in which the Systemwalker Desktop Patrol with version earlier than V13.0.0 and the PC security information collected via CT in command mode can not be browsed.

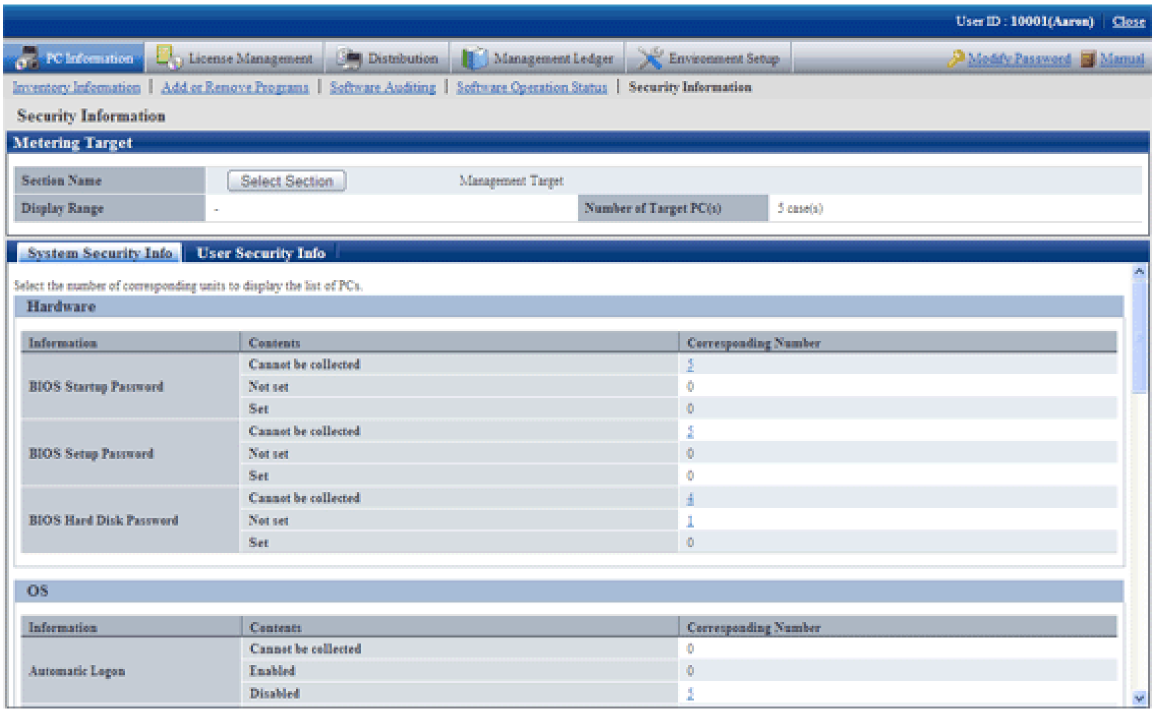
Collectable security information (system security information and user security information) and confirmable items may be variable with different OS (Operating System).

Note

User security information shall be collected during login, and it cannot be collected from the CT never logged on by the user after installation.

Collectable security information and display pictures are shown below:

System Security Information



Security Information

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Target PC(s)	5 case(s)

Select the number of corresponding units to display the list of PCs.

Hardware

Information	Contents	Corresponding Number
BIOS Startup Password	Cannot be collected	5
	Not set	0
	Set	0
BIOS Setup Password	Cannot be collected	5
	Not set	0
	Set	0
BIOS Hard Disk Password	Cannot be collected	4
	Not set	1
	Set	0

OS

Information	Contents	Corresponding Number
Automatic Logon	Cannot be collected	0
	Enabled	0
	Disabled	5

System security information collected from every OS is shown in the following table:

Class	Information	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
Hardware (Note 1)	BIOS Startup password	△	△	△	△	△	△	△	△	△	
	BIOS Setup Password	△	△	△	△	△	△	△	△	△	
	BIOS Hard Disk Password	△	△	△	△	△	△	△	△	△	
OS	Automatic Logon	○	○	○	○	○	○	○	○	○	
	Welcome Screen	○	-	-	○	○	○	○	○	○	In Windows Vista®, Windows® 7, Windows or Server® 2008, it must be set as

Class	Information	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Remarks
											“Displayed”.
	Last User Name	○	○	○	○	○	○	○	○	○	
	Security of Guest Account	○	○	○	○	○	○	○	○	○	
	Settings of Automatic Update	○	○	○	○	○	○	○	○	○	
	User Account Control (UAC)	-	-	-	○	○	○	○	○	○	
	Insecure Shared Folder	○	○	○	○	○	○	○	○	○	
	Require a Password on Wakeup	○	○	○	○	○	○	○	○	○	
	Set Complicated Password Required	○	○	○	○	○	○	○	○	○	
Application	Firewall	○	○	○	○	○	○	○	○	○	
	Real-time Scan Status of Anti-virus Software	○	○	○	○	○	○	○	○	○	
	Scheduled Scan Status of Anti-virus software	○	○	○	○	○	○	○	○	○	
	Scan Scope of Anti-virus Software	○	○	○	○	○	○	○	○	○	

○: Collectable.

△: May be not collectable according to the type of OS and device.

×: Not collectable.

-: Uncollected or no corresponding information.

XP: Windows® XP

2003: Windows Server® 2003

2003 x64: Windows Server® 2003 x64 Edition

Vista: Windows Vista®

Vista 64bit: Windows Vista® x64 Edition

7: Windows® 7

7 64bit: Windows® 7 x64 Edition

2008: Windows Server® 2008

2008 64bit: Windows Server® 2008 x64 Edition

Note 1:

Information collection may be impossible due to different types of devices. If information cannot be collected, it shall be set as “Not collectable”. Please confirm whether the command of the supported type of device (verifying tool of BIOS password setup status) is released on the Systemwalker technical information homepage in advance via this command.

The supported object products and auditable real-time inspection, firewall, timing scan and scan object range are shown below:

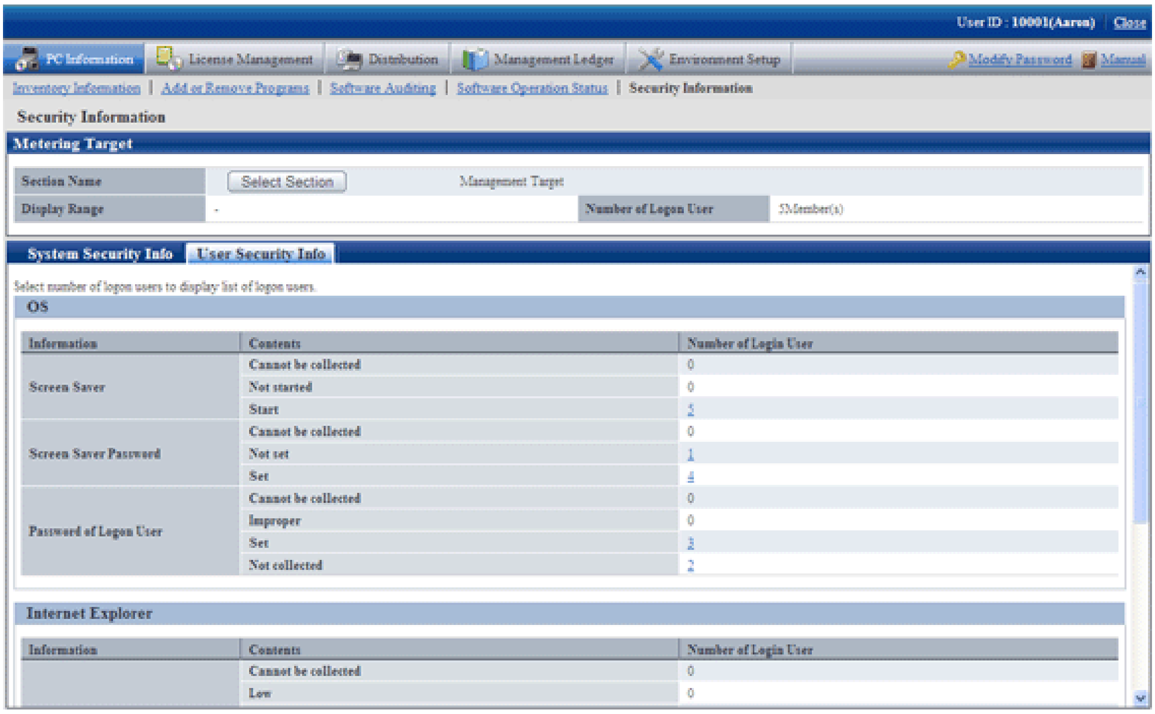
September, 2011

Manufacturer	Product Name	Version	Real-time Inspection	Firewall	Timing scan	Scan Object Range
Microsoft®	Windows® XP	SP2, SP3	-	○	-	-
	Windows Vista®	Without, SP1,SP2	-	○	-	-
	Windows® 7	Without, SP1	-	○	-	-
	Windows Server® 2003	SP1,SP2	-	○	-	-
	Windows Server® 2008	Without, SP1,SP2	-	○	-	-
TrendMicro	OfficeScan	Ver8.0, 10.0, 10.5	○	-	○	○
Symantec	Endpoint Protection	11.0	○	○	○	○
McAfee	VirusScan Enterprise	8.5i,8.7i,8.8	○	○	○	○

○: Auditable

-: Not audited or no corresponding function.

User Security Information



Security Information

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Logon User	5Member(s)

Select number of logon users to display list of logon users.

OS

Information	Contents	Number of Login User
Screen Saver	Cannot be collected	0
	Not started	0
	Start	5
Screen Saver Password	Cannot be collected	0
	Not set	1
	Set	4
Password of Logon User	Cannot be collected	0
	Improper	0
	Set	3
	Not collected	2

Internet Explorer

Information	Contents	Number of Login User
	Cannot be collected	0
	Low	0

System security information collected from every OS is shown in the following table:

Class	Information	XP	2003	2003 x64	Vista	Vista 64bit	7	7 64bit	2008	2008 64bit	Note
OS	Screen Saver	○	○	○	○	○	○	○	○	○	
	Screen Saver Password	○	○	○	○	○	○	○	○	○	
	Password of Logon User	○	○	○	○	○	○	○	○	○	
Internet Explorer	Internet Zone	○	○	○	○	○	○	○	○	○	
Application	Google Desktop [Search Across Computers]	○	○	○	○	○	○	○	○	○	

○: Collectable.

△: May be not collectable according to the type of OS and device.

×: Not collectable.

-: Uncollected or no corresponding information.

XP: Windows® XP

2003: Windows Server® 2003

2003 x64: Windows Server® 2003 x64 Edition

Vista: Windows Vista®

Vista 64bit: Windows Vista® x64 Edition

7: Windows® 7

7 64bit: Windows® 7 x64 Edition

2008: Windows Server® 2008

2008 64bit: Windows Server® 2008 x64 Edition

2.1.7 PC Operation Management

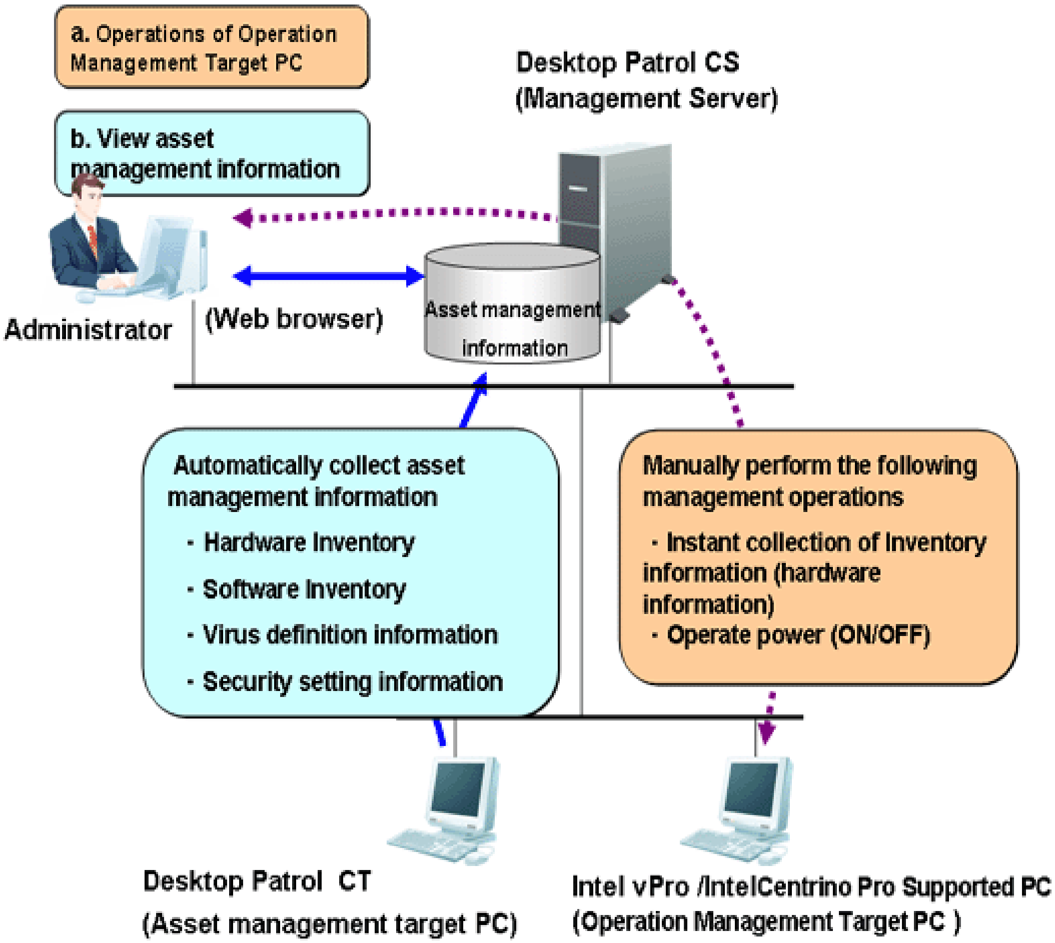
PC operation management function refers to the function to realize the remote control over the PC via Intel® AMT (CT, management, technology) in Intel® vPro™ and Intel® Centrino® Pro technology even though the PC is powered off.

PC operation management functions include:

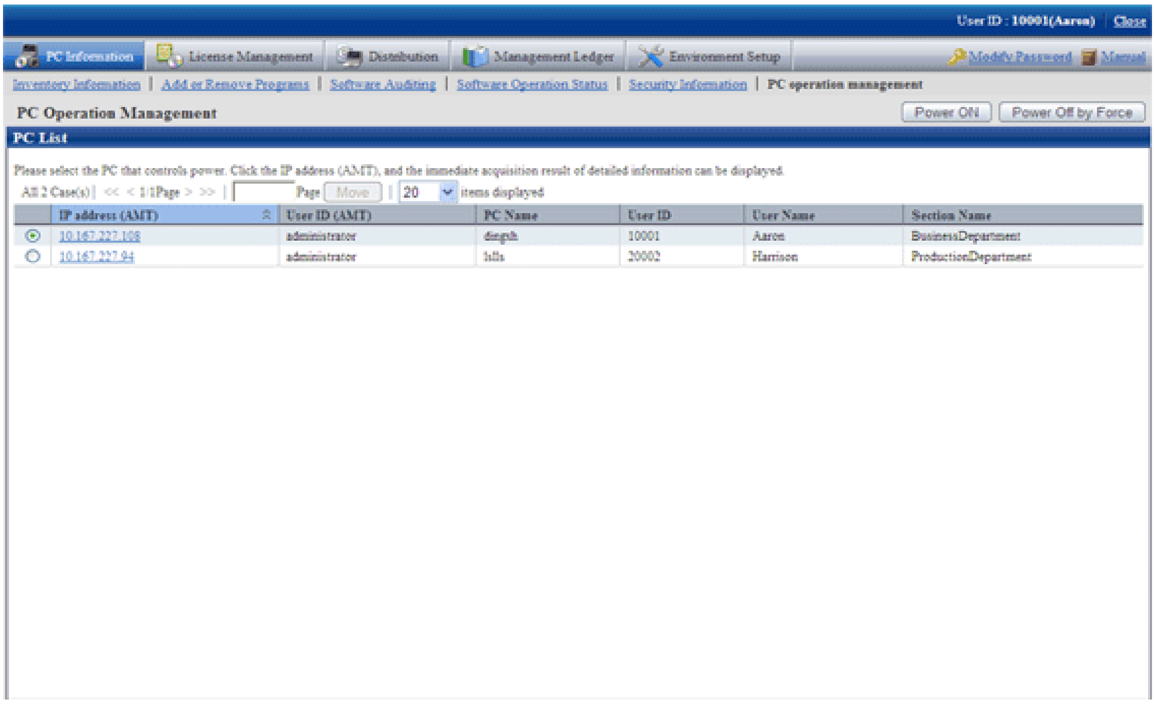
- Immediate collection of inventory information (hardware information) (Note)
- Operation on power supply (ON, OFF)

Note: The inventory collection via this function must need to use Intel® AMT; the acquired contents will be different from the inventory information browsed in the “PC Information” - “Inventory Information” window of main menu.

Overview of PC operation management function is summarily shown below:


a. Operations of Operation Management Target PC
b. View asset management information
Desktop Patrol CS
(Management Server)
Administrator
(Web browser)
Asset management information
Automatically collect asset management information
・Hardware Inventory
・Software Inventory
・Virus definition information
・Security setting information
Manually perform the following management operations
・Instant collection of Inventory information (hardware information)
・Operate power (ON/OFF)
Desktop Patrol CT
(Asset management target PC)
Intel vPro /IntelCentrino Pro Supported PC
(Operation Management Target PC)

PC operation management function displayed in the “PC” window of main menu.


User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Add or Remove Programs | Software Auditing | Software Operation Status | Security Information | PC operation management
Power ON
Power Off by Force

PC Operation Management

PC List

Please select the PC that controls power. Click the IP address (AMT), and the immediate acquisition result of detailed information can be displayed.

All 2 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

	IP address (AMT)	User ID (AMT)	PC Name	User ID	User Name	Section Name
●	10.167.227.108	administrator	dmpth	10001	Aaron	BusinessDepartment
○	10.167.227.94	administrator	hlls	20002	Harrison	ProductionDepartment

2.1.8 File Collection

This is the function that collected specified files.

For example, the status of PC in which a CT is installed can be confirmed through collecting log files of applications.

Collected files will be saved on CS.

The directory for saving the collected files can be modified through using the CustomPolicy command.

In addition, when using the collected file function after version upgrade, please confirm the setting value first.

For information on how to modify, please refer to “Command Reference” of Reference Manual.

2.1.9 Display of Usage Status and Application Processing

Display of Usage Status

The usage status of Systemwalker Desktop Patrol can be mastered in a short period via the “Status Window” window in the main menu homepage.

The following functions can be realized through displaying and browsing the statistic information in the “Status Window” window.

1. Easily master business status only through browsing the “Status Window” window.
2. Master the status of statistical items from multiple points of view to quickly judge the problems existing in service execution.

   Statistical items:

   - PC Not Collecting Inventory information
   - PC Not Applying Security Patches
   - PC Violating Security Policy
   - PC Violating Power Saving Policy
3. Display detailed information according to statistical items to easily screen out problems related to the items.

   Detailed Information:

   - Number of PC(s) in every section
   - Number of PC(s) for every item
4. Save the time for screening out corresponding PCs to quickly processing them because the PCs are displayed according to statistical items.
5. Because the step to log on Systemwalker Desktop Keeper is omitted in the system installed with Systemwalker Desktop Keeper and the status of Systemwalker Desktop Keeper (operation log result, etc) can also be displayed in the “Status Window” window, confirmation can be made in the “Status Window” window according to the point of view to every product.

Application processing

It is required to detect or view the problematic PCs according to the statistical items in the “Status Window” window to review assets management, automatically process PCs and draw attention of users.

The following application processing can be performed in the “Status Window” window:

1. Message sending
   - Send messages to the problematic PC to make the user of the PC aware of the problems in the application method.
   - Although the operation on the set diagnosis result window is allowed, the PC meeting the requirements of statistical items can be processed out of the set diagnosis result window, and the user can be informed of processing through sending a message.

- Messages can be sent via the Inventory information window which can be used when it is required to send a message to the user.

2. Inventory collection

   Collect Inventory information
   Collection can be performed before the Inventory collection task is assigned.

3. Inventory Delete

   Delete Inventory information
   All Inventory information not required for management of Systemwalker Desktop Patrol can be deleted.

4. Security Patch Installation

   Apply the security patches.
   This function shall be applied when the user has not applied security patches and not clear about how to use them during application of security patches.

5. Security Settings Modification

   Change security setup according to security policies.

   This function can be used in the following conditions.

   - When the system administrator and section administrator make the uniform processing during management on multiple PCs.

   - When the user makes processing through remote operation because he/she is not clear about how to change the security setup if the diagnosis is not used in the operation.

6. Power Saving Settings Modification

   Change power saving setup according to power saving policies.

   The user can use this function when he/she has not changed power saving setup and is not clear about how to change it.

2.1.10 Command of Inspection on CT Operation Status

It is a function to confirm operation status of CT in the window.

It is possible to confirm in the CS and the window of corresponding CT whether the CT operates according to the policy set in the CS, or how the CT operates and when it operates the next time, etc.

The function can be used in the following conditions.

- At the start

  When the administrator installs the new Systemwalker Desktop Patrol and changes system structure or application policy, it can be used to confirm whether the CT correctly operates according to the policies set in the CS.

- When faults occur

  During the application of Systemwalker Desktop Patrol, if the security patches are not applied to the CT, the user can confirm the operation status of CT and existing problems according to the output command.

2.1.11 Operation Log Collection

It is a function to save the user operation status as a log and collect this log file in the PC installed with a CT.

The following effects can be expected through confirming simple operation logs.

- Preventing information leakage

- Tracking operation when the PC has problems

The following information shall be saved to the simple operation log files. The actual operation of the user can be speculated according to these simple operation log files.

- Obtaining the window title displayed by the user
    - Name of execution program
    - Window title
    - Time of window activation
- Enabling the warning and stop messages caused by the specified files in “Control Execution File”
- Login/logout status of the user
- Startup time/Shutoff time of system

2.2 PC Auditing/Control Function

The PC can be audited according to the Power Saving Policy and Security Policy set by the administrator. If the PC violates the policies, a warning window will be displayed in the PC to remind the user of process.

In addition, the items violating the policies can be changed forcibly. (Note)

Note: Some items may not be changed forcibly.

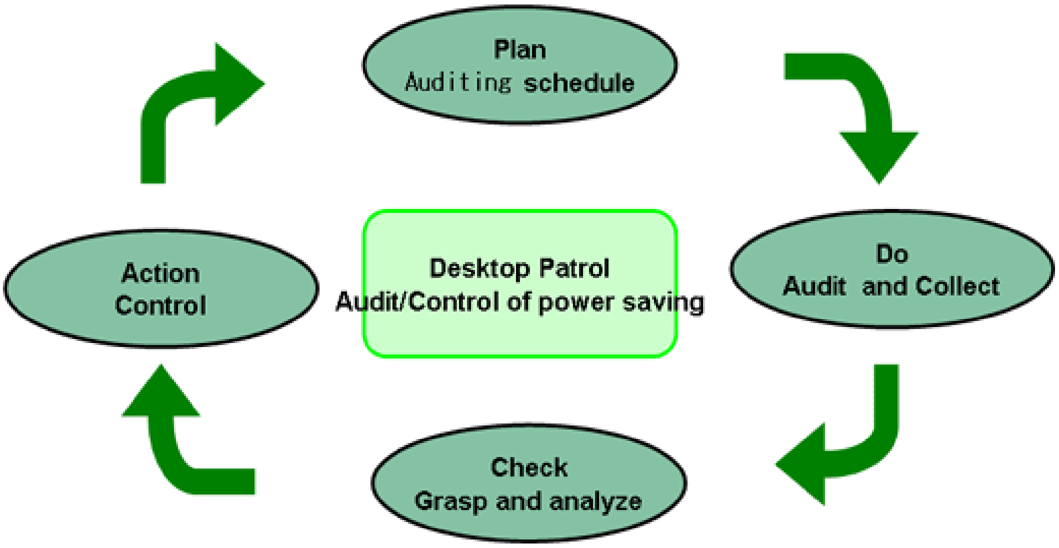
The following functions can be used for security auditing/control.

- Display a warning window or change the setup forcibly against the PC violating the policies
- Confirm the security and power saving control status according to the output reports.

2.2.1 Auditing Control of Power Saving Setup

Audit or control the power saving status of the PC according to the following procedure.

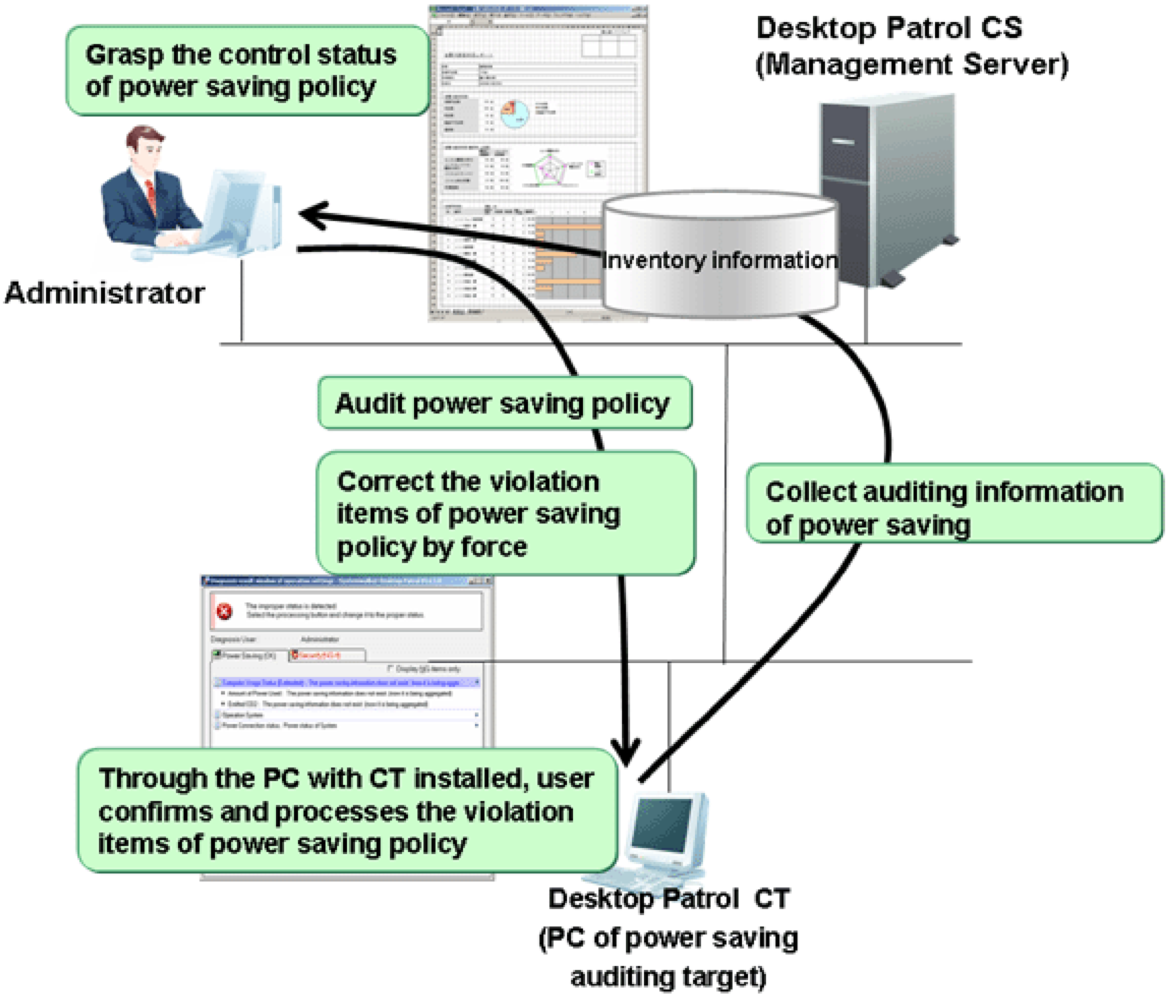
- Auditing plan: Execute power saving auditing plan of operating system.
- Audit and collect: Collect the information about power saving setup status of the PC.
- Master and analyze: Confirm and analyze the power saving setup status of the PC.
- Control: Control the PC needing treatment according to analysis results.



Power saving auditing and control status realized via Systemwalker Desktop Patrol during the PDCA period is summarily shown below:

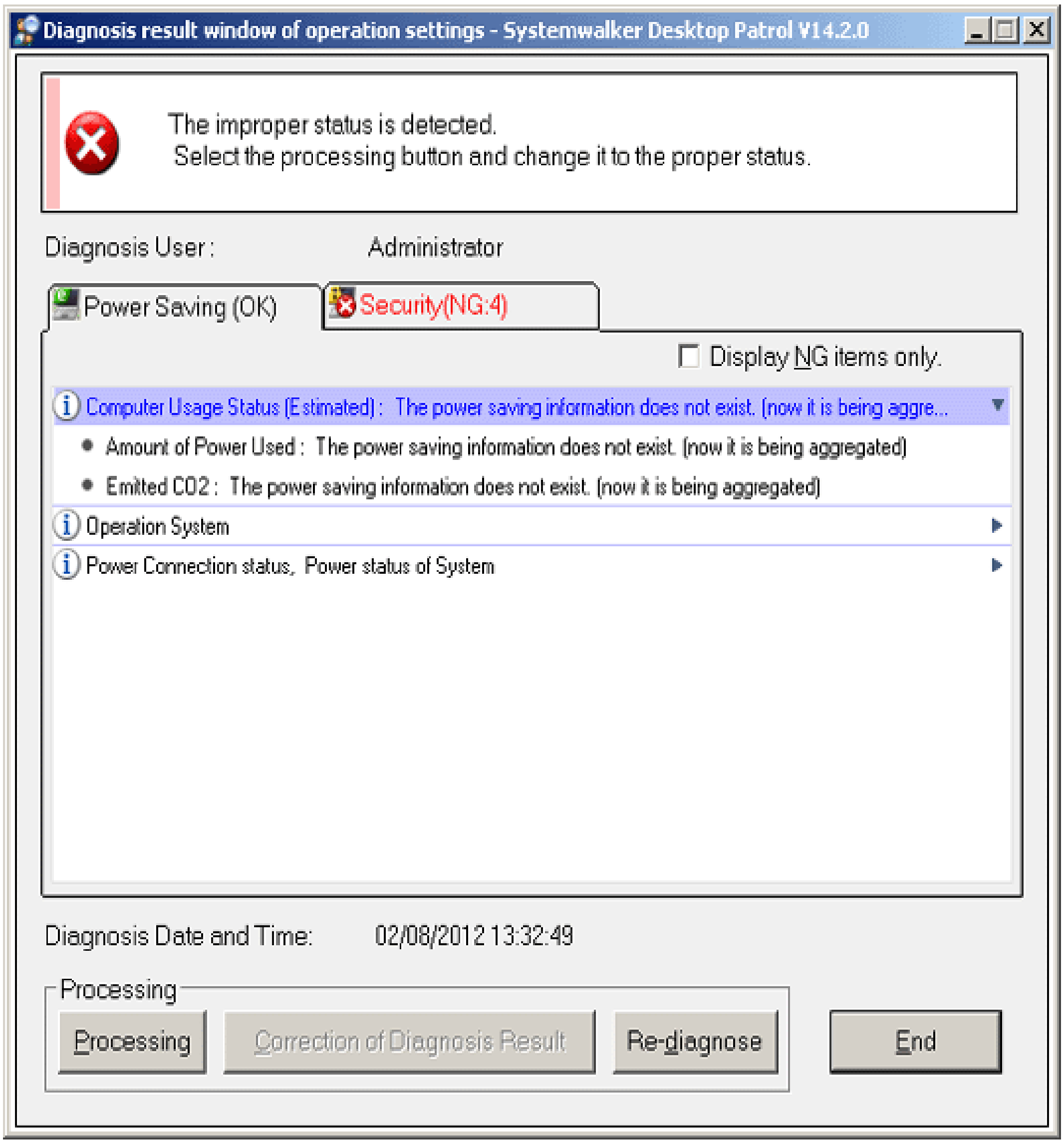
Power saving auditing and control status and power consumption can be confirmed according to the following reports.

- Power saving setup status report
- Power consumption auditing report



Grasp the control status of power saving policy
Desktop Patrol CS (Management Server)
Administrator
Inventory information
Audit power saving policy
Correct the violation items of power saving policy by force
Collect auditing information of power saving
Through the PC with CT installed, user confirms and processes the violation items of power saving policy
Desktop Patrol CT (PC of power saving auditing target)

The power saving setup diagnosis result window displayed in the CT is shown below.



Diagnosis result window of operation settings - Systemwalker Desktop Patrol V14.2.0

The improper status is detected.
Select the processing button and change it to the proper status.

Diagnosis User: Administrator

☐ Display NG items only.

Computer Usage Status (Estimated) : The power saving information does not exist. (now it is being aggre...

- Amount of Power Used : The power saving information does not exist. (now it is being aggregated)
- Emitted CO2 : The power saving information does not exist. (now it is being aggregated)

Operation System

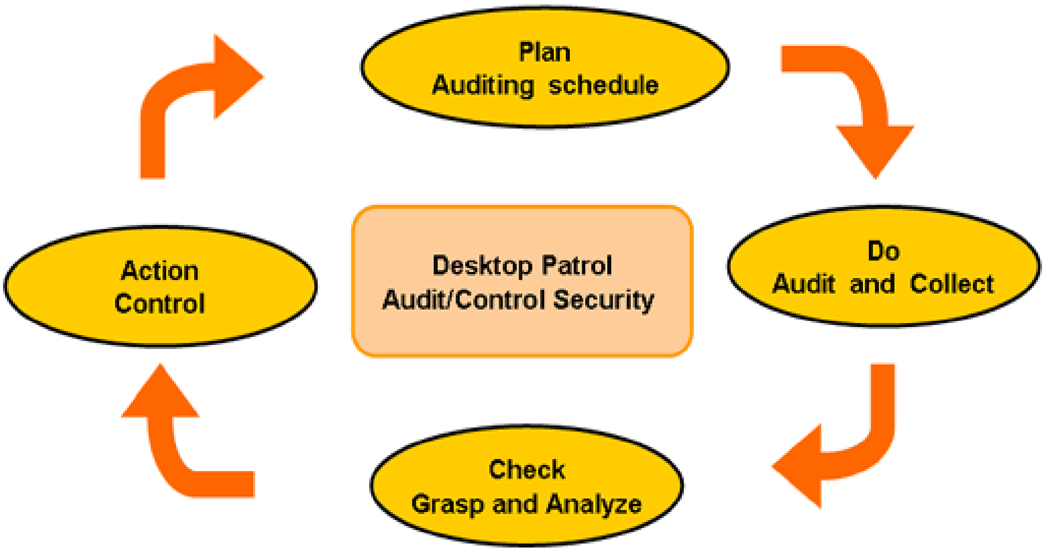
Power Connection status, Power status of System

Diagnosis Date and Time: 02/08/2012 13:32:49

2.2.2 Auditing/Control of Security Setup

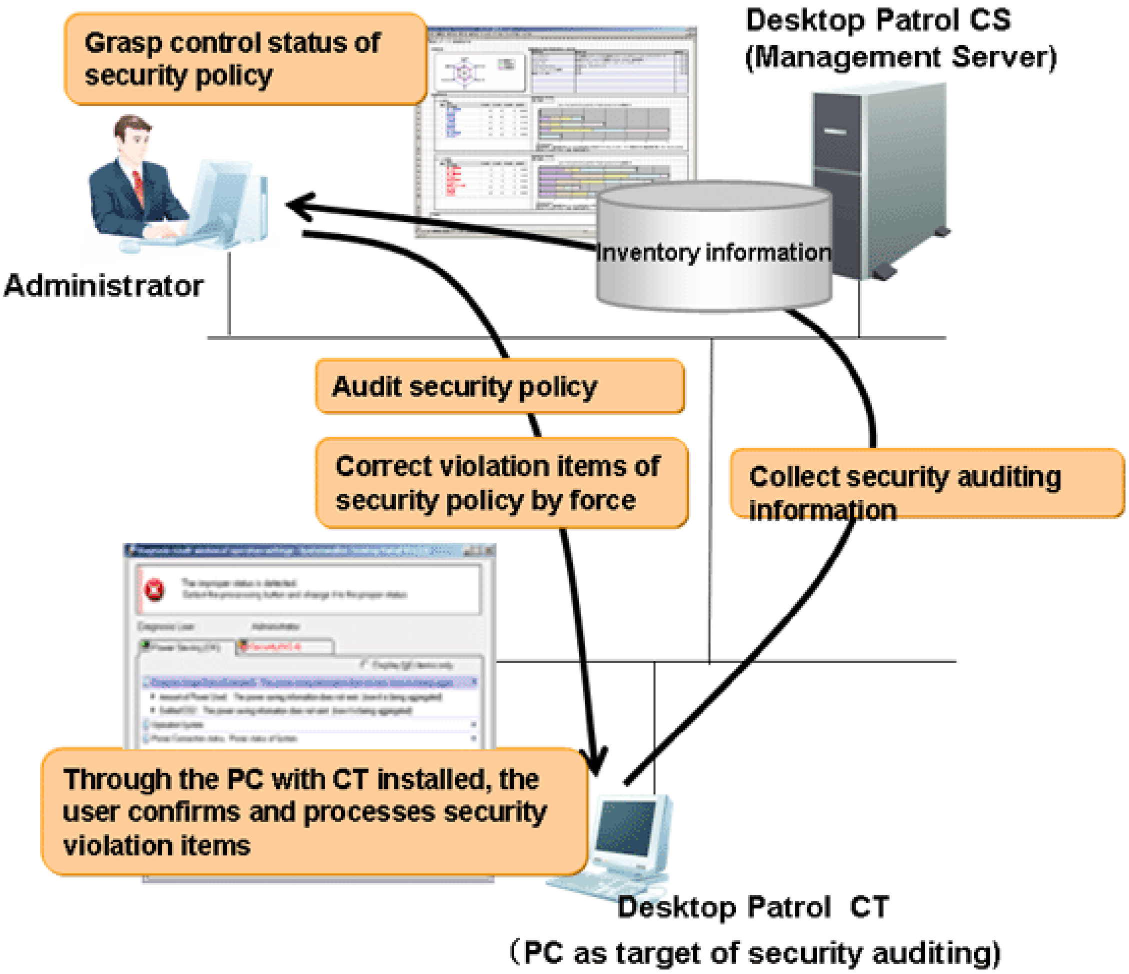
Audit or control the power saving status of the PC according to the following procedure.

- Auditing plan: Execute the security auditing plan of the operating system.
- Audit and collect: Collect the information about security setup status of the PC.
- Master and analyze: Confirm and analyze the security setup status of the PC.
- Control: Control the PC needing treatment according to analysis results.
-

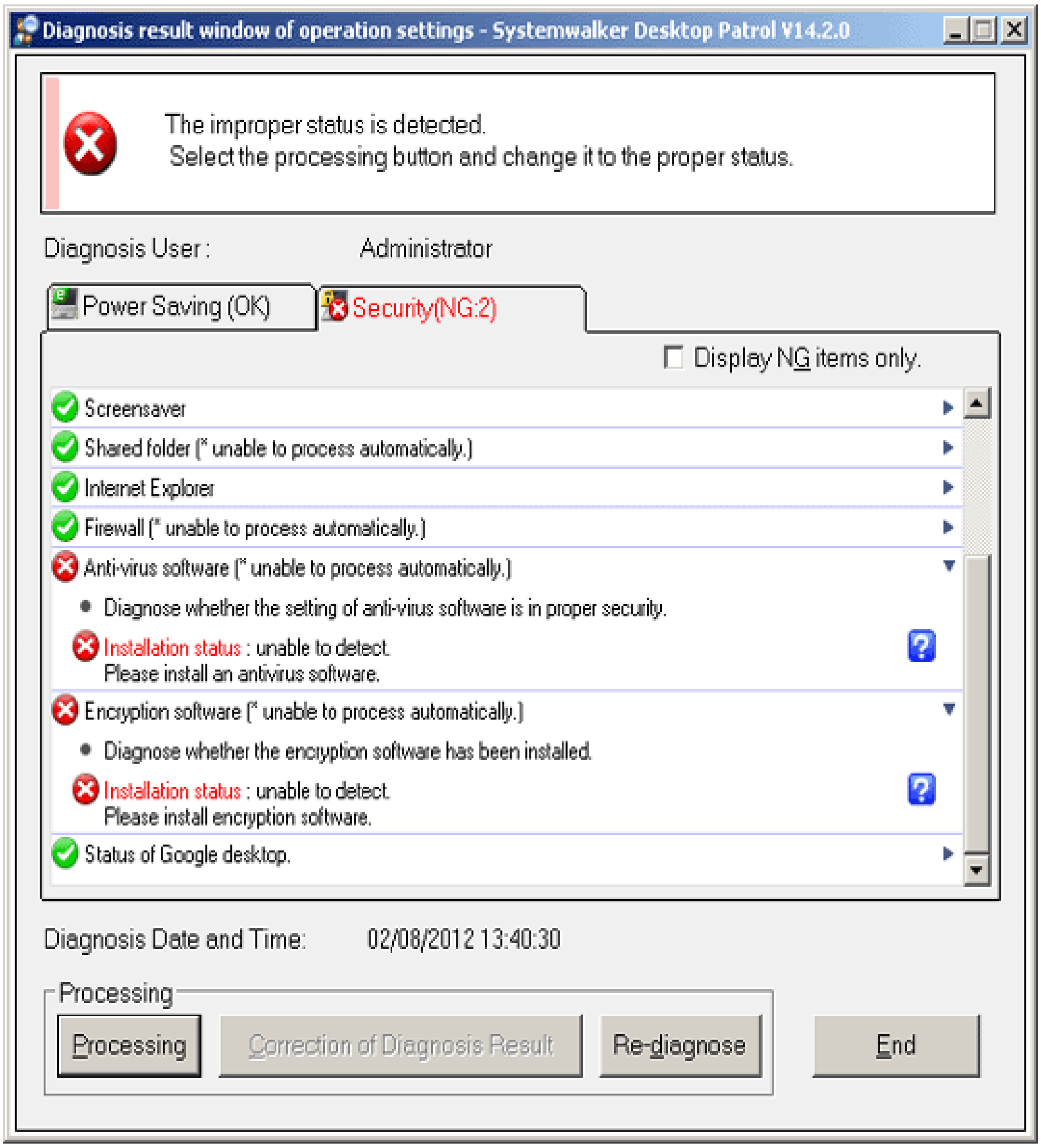


Security setup auditing and control status realized via Systemwalker Desktop Patrol during the PDCA period is summarily shown below:

The security policy control status can be confirmed according to the security auditing reports.


Grasp control status of security policy
Desktop Patrol CS
(Management Server)
Administrator
Inventory information
Audit security policy
Correct violation items of security policy by force
Collect security auditing information
Through the PC with CT installed, the user confirms and processes security violation items
Desktop Patrol CT
（PC as target of security auditing)

The security setup diagnosis result window displayed in the CT is shown below.



Diagnosis result window of operation settings - Systemwalker Desktop Patrol V14.2.0

The improper status is detected.
Select the processing button and change it to the proper status.

Diagnosis User : Administrator

Power Saving (OK)
Security(NG:2)

□ Display NG items only.

✓ Screensaver

✓ Shared folder (* unable to process automatically.)

✓ Internet Explorer

✓ Firewall (* unable to process automatically.)

✗ Anti-virus software (* unable to process automatically.)

- Diagnose whether the setting of anti-virus software is in proper security.

✗ Installation status : unable to detect.
Please install an antivirus software.

✗ Encryption software (* unable to process automatically.)

- Diagnose whether the encryption software has been installed.

✗ Installation status : unable to detect.
Please install encryption software.

✓ Status of Google desktop.

Diagnosis Date and Time: 02/08/2012 13:40:30

2.3 License Management Function

This section describes the License management function of Systemwalker Desktop Patrol.

2.3.1 License Management

In Systemwalker Desktop Patrol, License management is realized through distributing the License to each PC.

License management needs the following 3 prerequisites.

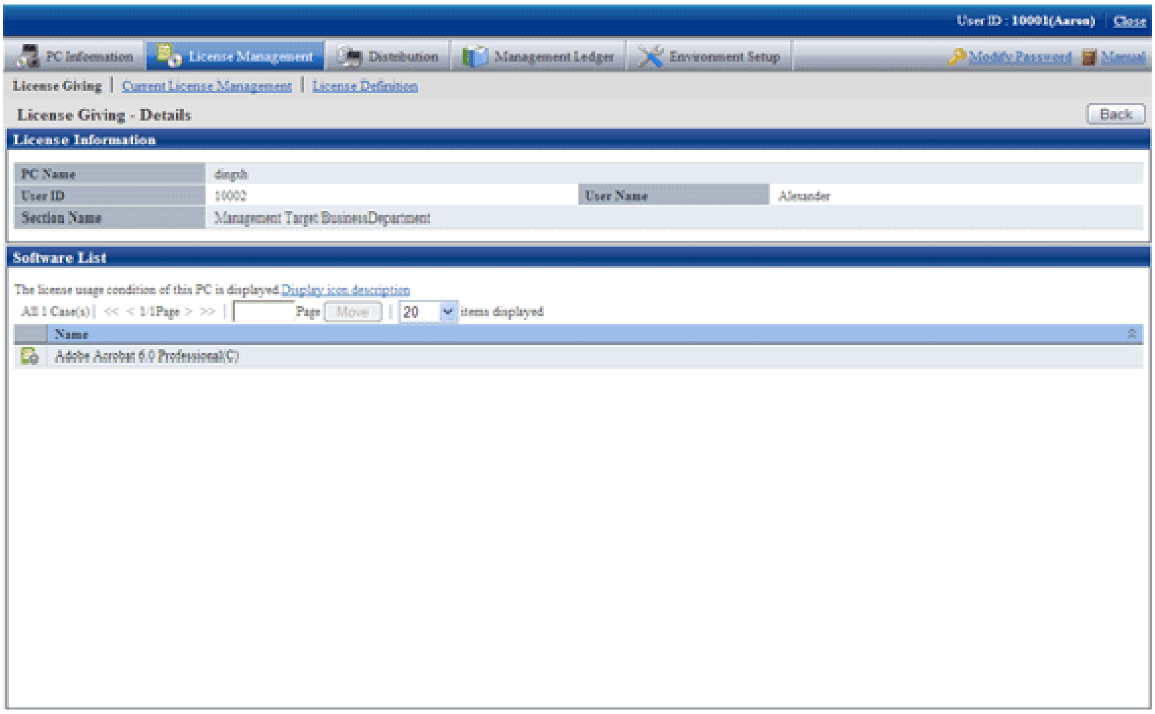
- “Software Dictionary” has been registered
- The relation between License and software (Dictionary Code) has been defined in the “License Management” - “License Definition” window of the main menu.
- The number of Licenses for each section has been set in the “License Management” - “Current License Management ” window of main menu.

Distribute the license to software used in the PC in the “License Management” - “License Allocation” window of the main menu to manage the number of Licenses can be realized.

Confirm the usage status of software to which licenses have been distributed in the “License Management” - “License Allocation” window of main menu.

If application of the software to which the License is not distributed is found through “Event Settings”, the user can notify the administration of a violation by E-mail or make a list of error logs in the event log.

After selecting the PC name in the “License Management” - “License Giving” window of main menu, the usage status of License will be displayed as below.



License Giving - Details

License Information

PC Name	dingsh		
User ID	10002	User Name	Alexander
Section Name	Management Target BusinessDepartment		

Software List

The license usage condition of this PC is displayed Display icon description

All 1 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

	Name
	Adobe Acrobat 6.0 Professional(C)

Creation function of User Asset Software Dictionary

It is required to add the user definition of software dictionary.

The creation function of user asset software dictionary, as a user definition function, can be simply defined according to the “Add or Remove Programs” information collected as Inventory information.

The installed software products in PCs can easily become License management objects via this function, so the user can master flexible application of IT assets and shortage of software license.

2.3.2 Control Execution File

The applications unnecessary during the work can be defined as “Control Execution File System” to detect the PCs on which these applications have been installed.

In addition, to prevent these applications being applied in CTs, a warning message can be sent to the user when starting them to prevent them from being enabled. But, execution of the command of displaying command execution window cannot be prohibited (Note).

Note: cmd. exe and .BAT files, etc.

2.4 File Distribution Function

This section describes the file distribution function of Systemwalker Desktop Patrol.

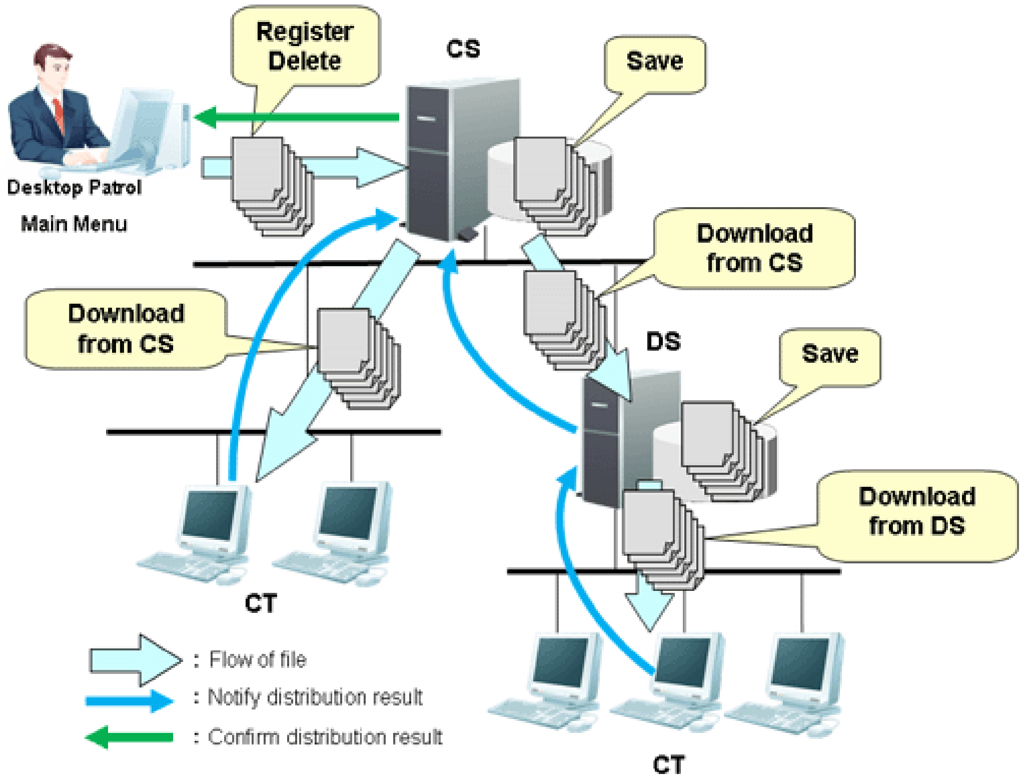
File distribution function is a function of distributing multiple files from CS to multiple CTs only through operation on the CS. In addition, the distribution result can be confirmed on the CS.

This function is recommended for simple file distribution to replace the folders of definition files and execution files.

If software installation is included in distribution, please use the “2.5 Software Distribution Function”. In addition, if it is required to apply security patches, please use “2.6 Security Patches Distribution /Application Function”

The file distribution function of Systemwalker Desktop Patrol consists of the following 3 parts.

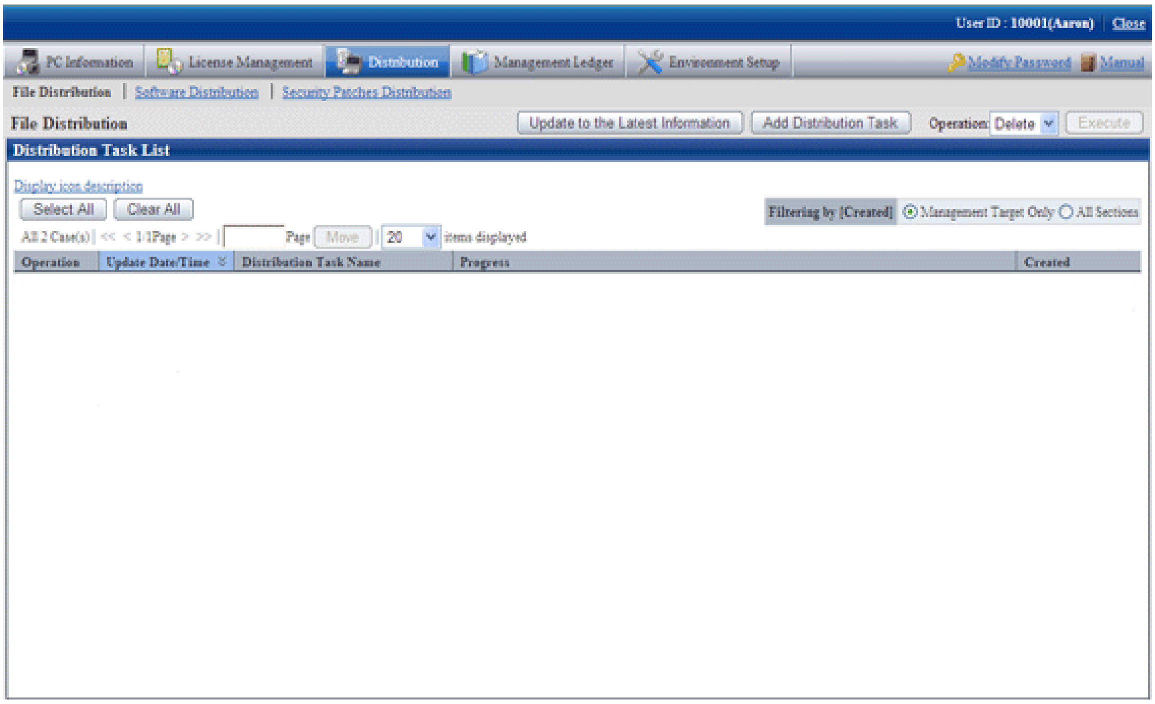
- Distribution Settings of file and distribution target
- File download
- Distribution result confirmation



2.4.1 File Distribution Settings & Distribution Target

The files to be distributed shall be set as distributed files and CT as distribution target.

Complete Distribution Settings in the initial screen of “Distribution” - “File Distribution” in the main menu of CS.

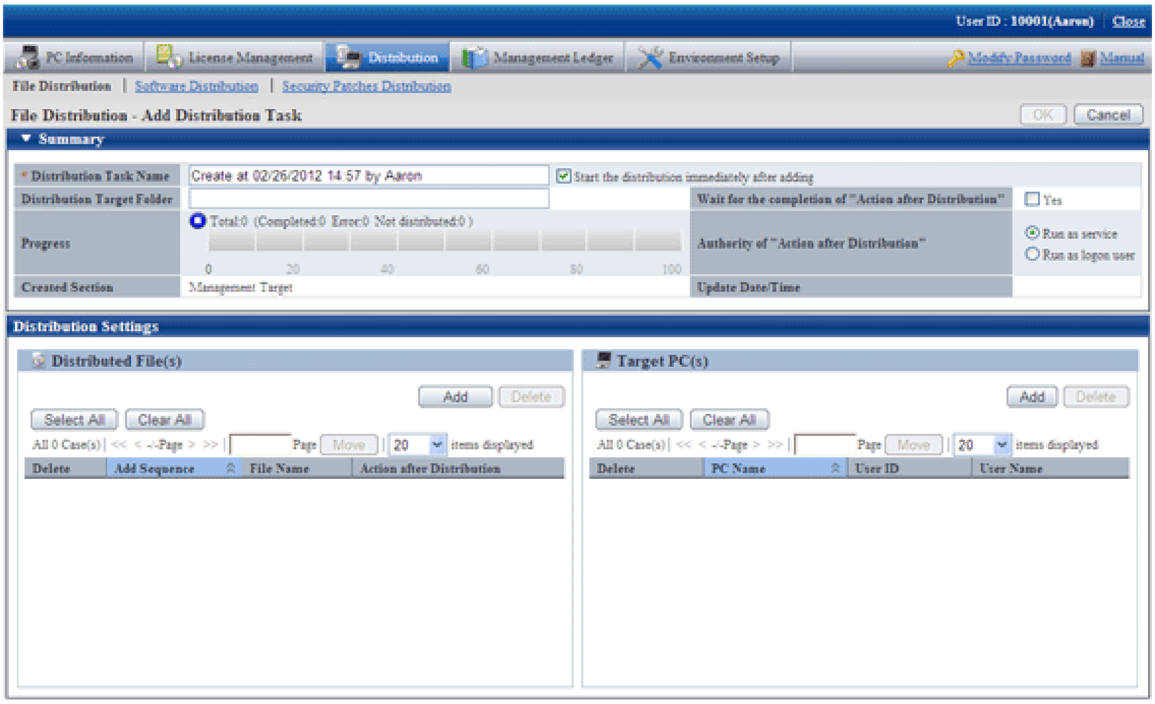


Filtering by [Created]: ● Management Target Only ○ All Sections

2.4.2 File Download

Distribute files according to the setup and download the distributed files.

Immediate distribution begins by a click on the “OK” button in the setup window after completing the setup in the main menu.

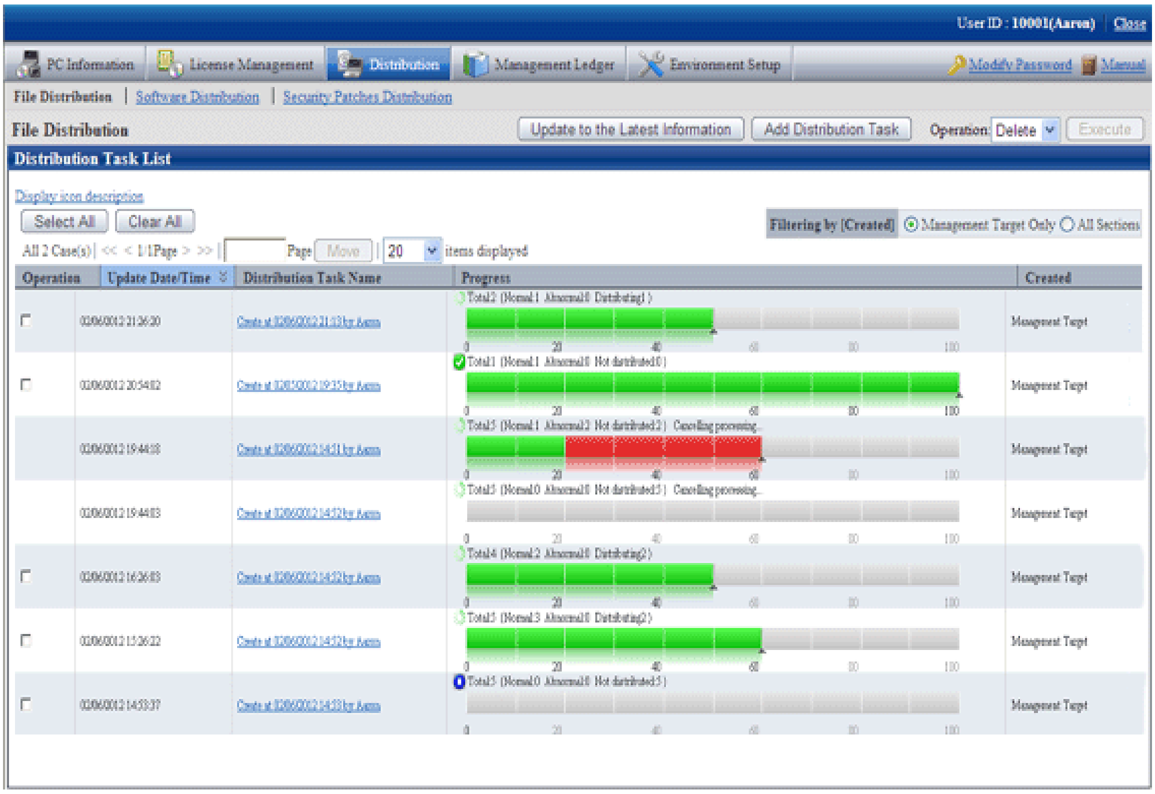


* Distribution Task Name	Create at 02/26/2012 14:57 by Aaron ☑ Start the distribution immediately after adding		
Distribution Target Folder		Wait for the completion of "Action after Distribution"	□ Yes
Progress	Total:0 (Completed:0 Error:0 Not distributed:0)	Authority of "Action after Distribution"	● Run as service ○ Run as logon user
Created Section	Management Target	Update Date/Time	

2.4.3 Distribution Result Confirmation

Distribution result can be confirmed in the initial screen of “File Distribution”.

If immediate distribution begins after completing Distribution Settings in the main menu, distribution result can be confirmed about 20 minutes later.


User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
File Distribution | Software Distribution | Security Patches Distribution
Update to the Latest Information
Add Distribution Task
Execute
Select All
Clear All
Display icon description
All 2 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

File Distribution

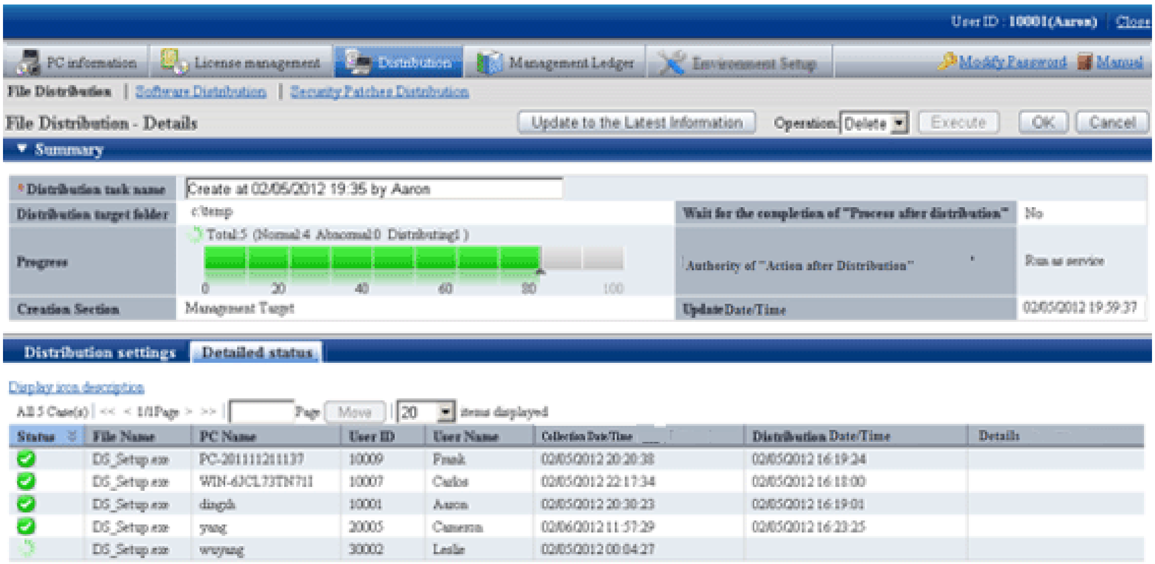
Operation: Delete

Distribution Task List

Filtering by [Created] ● Management Target Only ○ All Sections

Operation	Update Date/Time	Distribution Task Name	Progress	Created
☐	02/06/2012 21:26:30	Create at 02/06/2012 21:13 by Aaron	Total:2 (Normal:1 Abnormal:0 Distributing:1)	Management Target
☐	02/06/2012 20:54:02	Create at 02/05/2012 19:35 by Aaron	✓ Total:1 (Normal:1 Abnormal:0 Not distributed:0)	Management Target
	02/06/2012 19:44:18	Create at 02/06/2012 14:31 by Aaron	Total:5 (Normal:1 Abnormal:2 Not distributed:2) Cancelling processing...	Management Target
	02/06/2012 19:44:03	Create at 02/06/2012 14:32 by Aaron	Total:5 (Normal:0 Abnormal:0 Not distributed:5) Cancelling processing...	Management Target
☐	02/06/2012 16:26:03	Create at 02/06/2012 14:32 by Aaron	Total:4 (Normal:2 Abnormal:0 Distributing:2)	Management Target
☐	02/06/2012 15:26:22	Create at 02/06/2012 14:32 by Aaron	Total:5 (Normal:3 Abnormal:0 Distributing:2)	Management Target
☐	02/06/2012 14:53:37	Create at 02/06/2012 14:33 by Aaron	Total:5 (Normal:0 Abnormal:0 Not distributed:5)	Management Target

If it is desired to confirm the distribution result of every distribution task, click the link of the distribution task to confirm detailed information.


User ID : 10001(Aaron) | Close
PC information
License management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
File Distribution | Software Distribution | Security Patches Distribution
Update to the Latest Information
Execute
OK
Cancel
▼ Summary
Distribution settings
Detailed status
Display icon description
All 5 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

File Distribution - Details

Operation: Delete

* Distribution task name	Create at 02/05/2012 19:35 by Aaron		
Distribution target folder	c:\temp	Wait for the completion of "Process after distribution"	No
Progress	Total:5 (Normal:4 Abnormal:0 Distributing:1)	Authority of "Action after Distribution"	Run as service
Creation Section	Management Target	Update Date/Time	02/05/2012 19:59:37

Status	File Name	PC Name	User ID	User Name	Collection Date/Time	Distribution Date/Time	Details
✓	DS_Setup.exe	PC-201111211137	10009	Frank	02/05/2012 20:20:38	02/05/2012 16:19:24	
✓	DS_Setup.exe	WIN-6JCL73TN711	10007	Carlos	02/05/2012 22:17:34	02/05/2012 16:18:00	
✓	DS_Setup.exe	dingzh	10001	Aaron	02/05/2012 20:30:23	02/05/2012 16:19:01	
✓	DS_Setup.exe	yang	20005	Cameron	02/06/2012 11:57:29	02/05/2012 16:23:25	
	DS_Setup.exe	wuyang	30002	Leslie	02/05/2012 00:04:27		

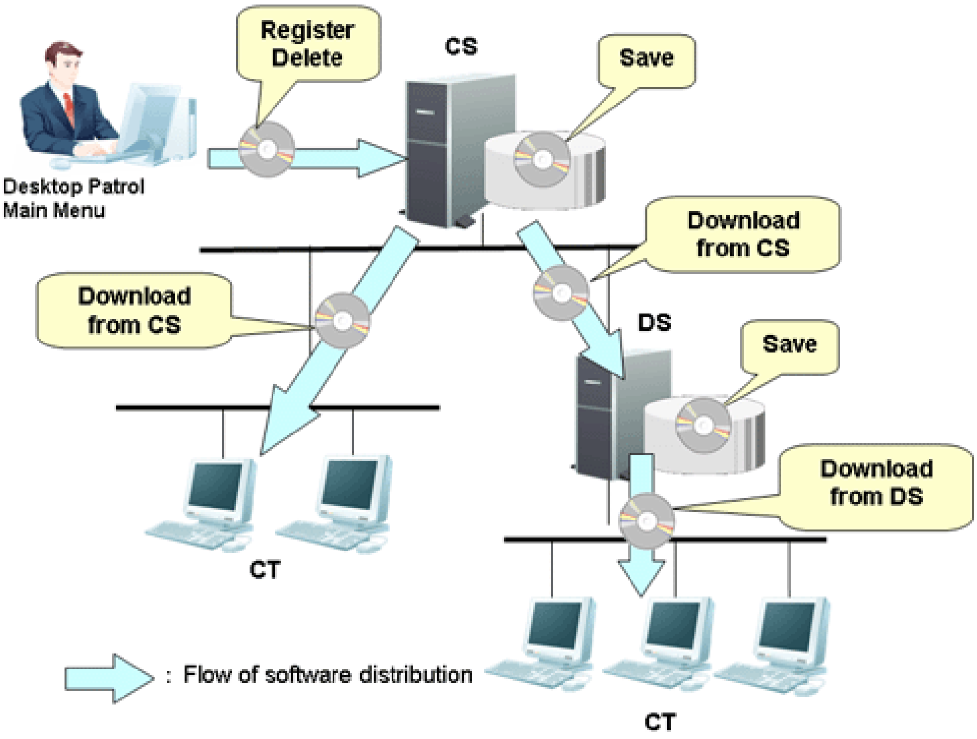
2.5 Software Distribution Function

Software distribution function is a function to manage the object data distributed from the file unit to the software unit in the upstream server and download distribution targets by the specified server or PC from the upstream server.

Software distribution function of Systemwalker Desktop Patrol consists of the following parts.

- Management on Software Distribution
- Setup of software distribution target
- Download of Software Distribution

Both files and software can be distributed via the software distribution function of Systemwalker Desktop Patrol.

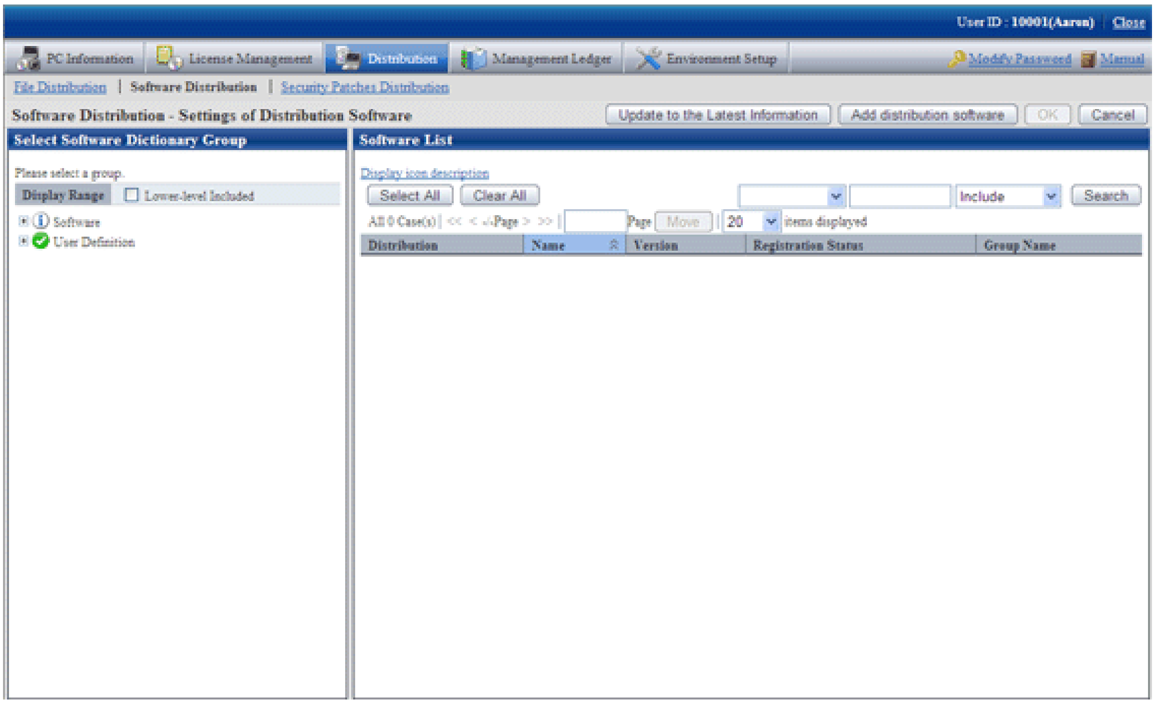


2.5.1 Management on Software Distribution

Management on Software Distribution includes:

- Registering, updating or deleting Software Distribution
- Creating the group of Software Distribution

Manage the Software Distribution in the “Software Distribution” - “Settings of Distribution Software” window of the main menu.



Software Distribution

In Systemwalker Desktop Patrol, both files and software can be registered as Software Distribution.

The user can set the name, version, valid period and size of Software Distribution.

The PC can only browse and download the Software Distribution during the specified period in the “Valid Period” of them.

The Software Distribution downloaded to the server and CT can be assigned to the execution files (post-download execution files) of automatic application (installation). It is required to set the service authority for the software which requires administrator authority for execution.

Software Group for Distribution

To realize the classified management on Software Distribution, a Software Distribution group can be created and a distribution target server can be distributed to the group.

The “Distribution Target Server” set for the software group for distribution can assign the Software Distribution in this group to the specified server. The server assigned as distribution target downloads Software Distribution from the upstream server and CT can download Software Distribution from the upstream server.

2.5.2 Setup of Software Distribution Target

The following items can be set as software distribution targets.

- CS

  Physical server, set as the distribution target when it is only desired to distribute software to the subordinate PCs of the CS.

- DS

  Physical server, set as the distribution target when it is only desired to distribute software to the subordinate PCs of the DS.

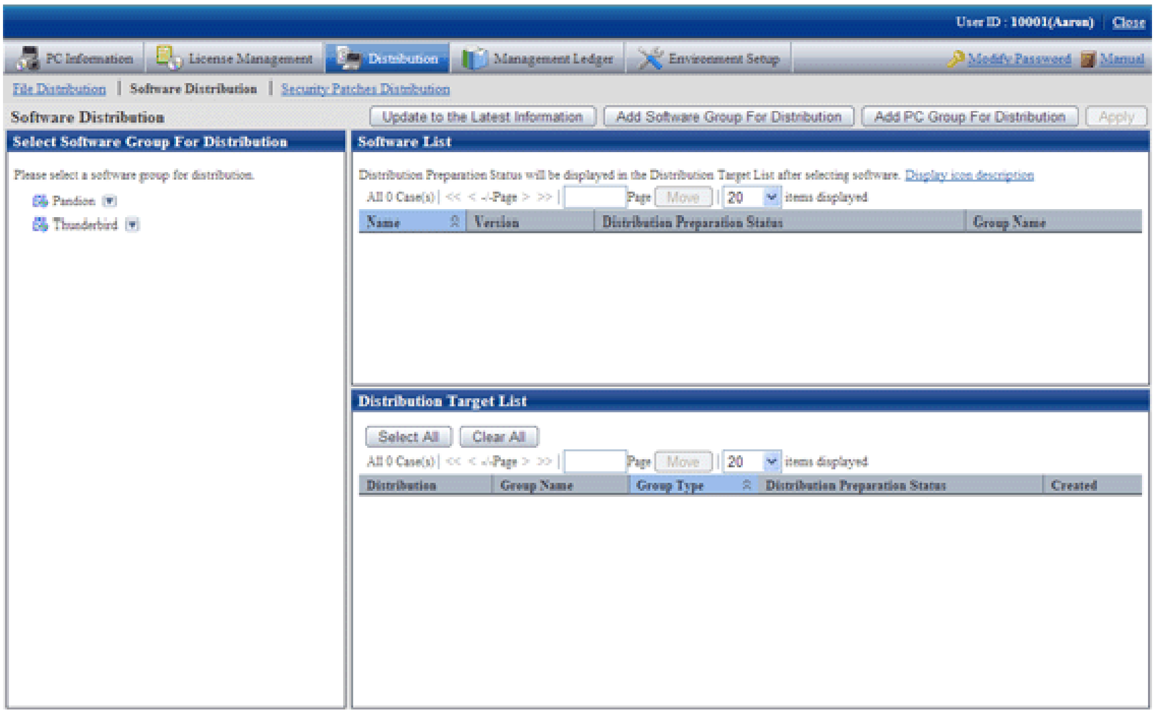
- Policy group

  Set as the distribution target when set as the distribution target when it is only desired to distribute software to the PCs registered with policy group.

- Software distribution PC group

  Set as the distribution target when set as the distribution target when it is only desired to distribute software to the PCs registered with the software distribution PC group.

Set the distribution targets in the “Software Distribution” - “Settings of Distribution Software” window of main menu.



Software Distribution

Select Software Group For Distribution

Please select a software group for distribution.

Software List

Distribution Preparation Status will be displayed in the Distribution Target List after selecting software.

All 0 Case(s) | << < -/-Page > >> | Page | 20 items displayed

Name	Version	Distribution Preparation Status	Group Name

Distribution Target List

All 0 Case(s) | << < -/-Page > >> | Page | 20 items displayed

Distribution	Group Name	Group Type	Distribution Preparation Status	Created

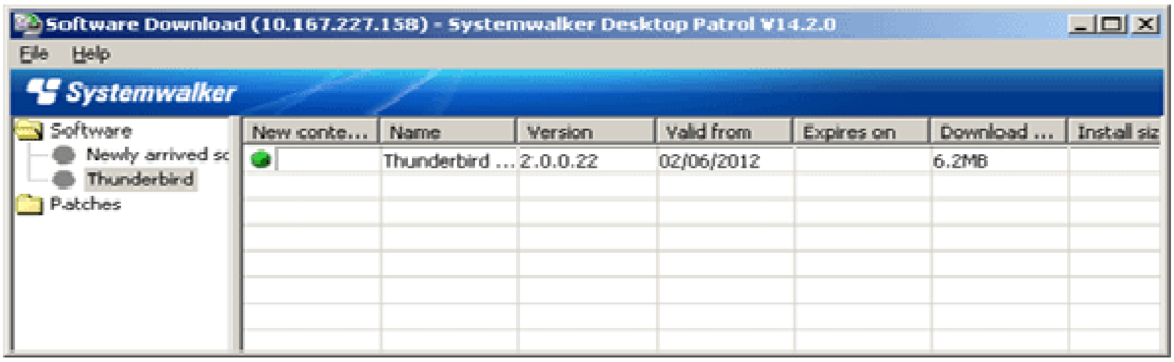
2.5.3 Download of Software Distribution

Download of Software Distribution is a function to download Software Distribution from the upstream server to the CT.

Manual download operation in the CT needs to enable the “Software Download” window.

Download Software Distribution to CT

Download of Software Distribution to CTs needs to enable “Software Download”, or is executed upon the receipt of the messages about new software.


Software Download (10.167.227.158) - Systemwalker Desktop Patrol V14.2.0
File
Help
Systemwalker
Software
Newly arrived sc
Thunderbird
Patches

New conte...	Name	Version	Valid from	Expires on	Download ...	Install siz
●	Thunderbird ...	2.0.0.22	02/06/2012		6.2MB	

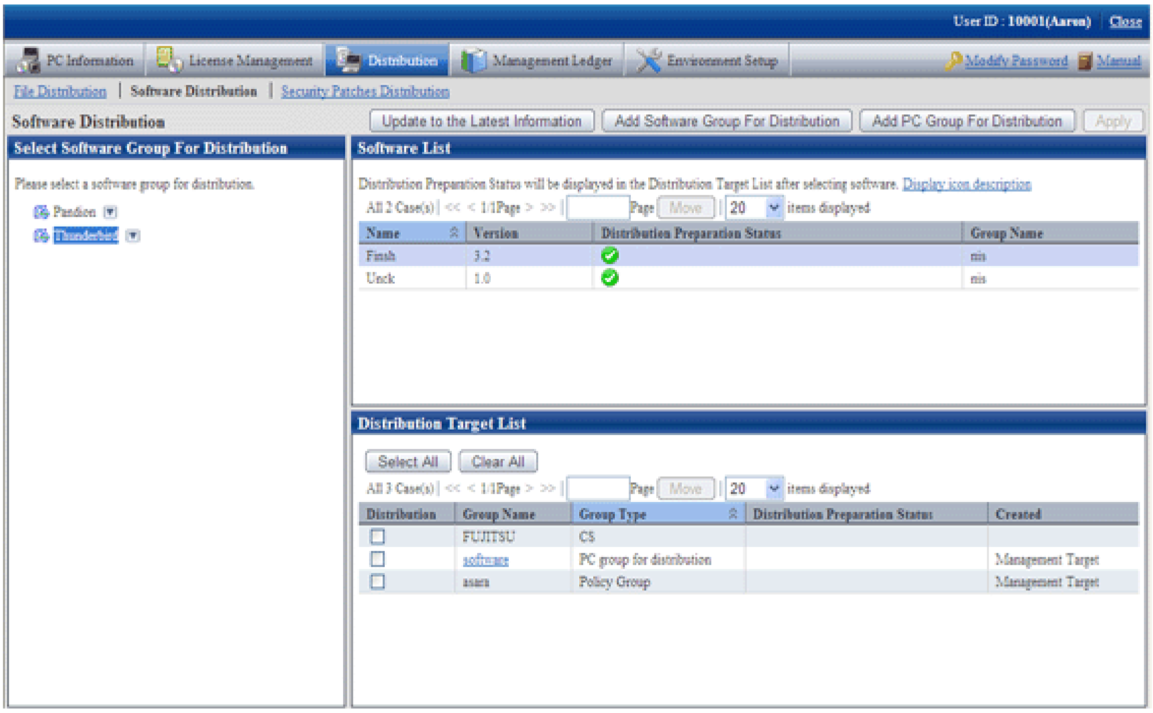
Refer to “Systemwalker Desktop Patrol Operation Guide: for Clients” for how to download Software Distribution to CTs.

Download Software Distribution to DS

DS can download Software Distribution from the upstream server periodically according to the download task scheme set in DS policy which can be set in the main menu.

Download confirmation function

The distribution status of every Software Distribution, the status and progress of distribution target server specified during registration of Software Distribution can be confirmed in the main menu.



Please select a software group for distribution.

Distribution Preparation Status will be displayed in the Distribution Target List after selecting software.

All 2 Case(s) | << < 1/1Page > >> |

Name	Version	Distribution Preparation Status	Group Name
Finsh	3.2	✓	mis
Unck	1.0	✓	mis

All 3 Case(s) | << < 1/1Page > >> |

Distribution	Group Name	Group Type	Distribution Preparation Status	Created
□	FUJITSU	CS		
□	software	PC group for distribution		Management Target
□	asara	Policy Group		Management Target

2.6 Security Patches Distribution /Application Function

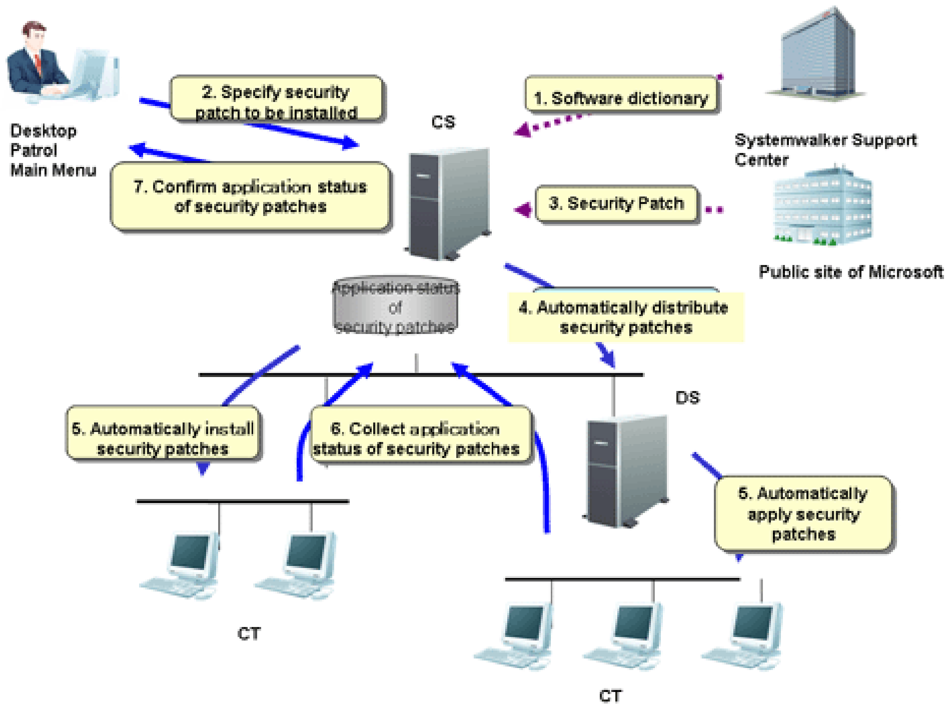
This section describes the security patches distribution and application function of Systemwalker Desktop Patrol.

2.6.1 Automatic Application of Security Patches

Systemwalker Desktop Patrol can automatically distribute the security patches provided by Microsoft Corporation from the upstream server to the CTs for application.

Systemwalker Desktop Patrol can download the security patches provided by Microsoft Corporation from “Microsoft Public Server” and automatically register them to the CS. Therefore, it can automatically complete all operations from acquisition of security patches to installation of them in the CTs.

By means of the function of automatic application of security patch, the complicated update operation is not necessary for the CT user to ensure security. In addition, this function can prevent security patches omission.


Desktop Patrol Main Menu
2. Specify security patch to be installed
7. Confirm application status of security patches
CS
1. Software dictionary
Systemwalker Support Center
3. Security Patch
Public site of Microsoft
Application status of security patches
4. Automatically distribute security patches
DS
5. Automatically install security patches
6. Collect application status of security patches
5. Automatically apply security patches
CT
CT

1. Systemwalker Support Center can distribute a ”Software Dictionary” defined in Inventory information by E-Mail. When apply a ”Software Dictionary”, please use the AtoolETPGT.exe(Software Dictionary Apply) command.
2. The security patches as application objects shall be specified by the CS administrator.
3. Download the security patches provided by Microsoft Corporation from “Microsoft Public Server” and automatically register them to the CS.
4. Security patches can be automatically distributed from the CS to DS, if DS is applied.
5. Security patches can be automatically applied from the CS or DS of the upstream server to CTs.
6. The application status of security patches in CTs can be collected and sent to CS or DS.
7. CS administrator confirms the application status of security patches.

Automatic application of security patches mentioned in 2-6 is performed via Systemwalker Desktop Patrol.

2.6.2 Manual Application of Security Patch

Security patches can be applied immediately when the high emergency security patches are released, or the user desires to apply the security patches at any time during movement.

After the security patches have been registered with the upstream server, select “Start” - “Programs” - “Systemwalker Desktop Patrol CT” - “Patch Application” to detect and apply the patches desired to be applied in the PC.

2.6.3 Selection of Security Patches Applied to Specific PC

The user can define the security patches to be applied to each policy group if he/she wants to select security patches and apply them to the specific PC.

In addition, extra patches shall be applied to the PC, if any patch application problem happens to it after the specific security patches have been applied.

The following setups shall be applied to the selected security patches.

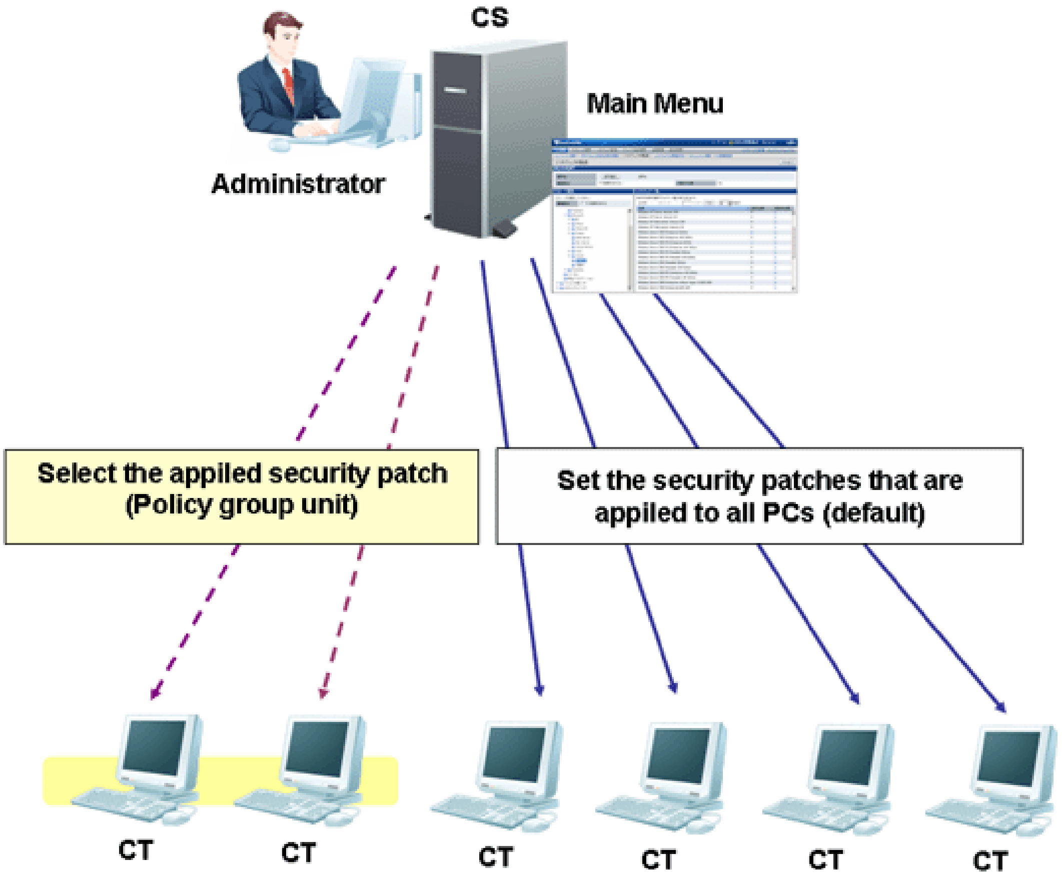
- Select security patches for specific PCs

- Do not apply the security patches provided later to specific PCs

The above setups can be combined.

Application drawing

The below drawing is to show how to select the security patches and apply them to specific PCs:


CS
Main Menu
Administrator
Select the appiled security patch
(Policy group unit)
Set the security patches that are
appiled to all PCs (default)
CT
CT
CT
CT
CT
CT

For the CTs out of the policy group, settings of security patches from the “Software Distribution” - “Settings of Distribution Software” window of the main menu and apply them to the CTs.

When selecting security patches for specific PCs, it is required to cancel the selected unapplied security patches from the “Environment Setup” - “Policy Group Management” - “Customize Various Policies” tab of main menu.

Therefore, the user can select security patches and apply them to the PCs belonging to the policy group.

2.7 Management Ledger Function

This section describes the management ledger function of Systemwalker Desktop Patrol.

2.7.1 Device Management

For the management target devices, the following operations can be carried out by means of the “Confirmation and Operating Device (PC and Device) Assets Status” function.

- Confirm device information according to section, type or location

- Register, change or delete device information
- Save the device account of device information

The information will be displayed in the “Device Management Ledger” - “Device Management” window of “Desktop Patrol Main Menu”.

The display information and picture are shown below:

Confirm device information by section, type or location

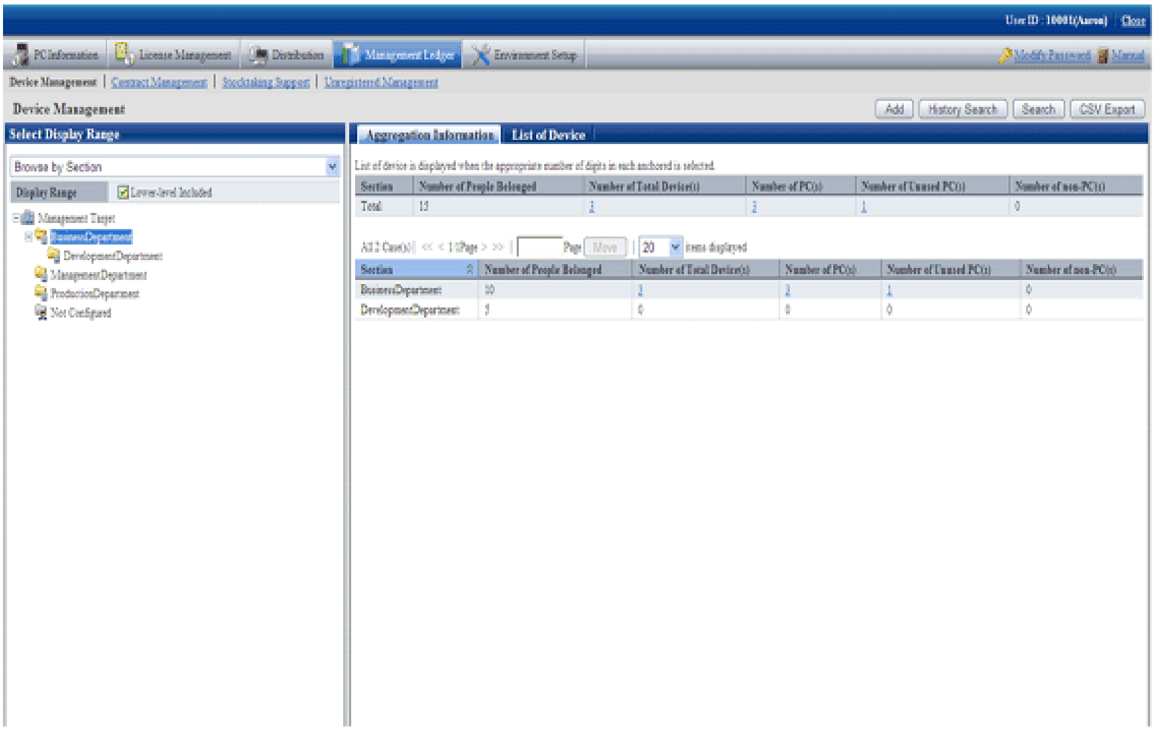
Display the information of devices meeting the requirements of user operation.

The user can easily search device information and display search results serving the purpose.

Aggregation Information

Display the whole quantity of management object devices and Number of PC(s) by section, type or location.

For example, aggregation information is displayed as follows by section:



List of device is displayed when the appropriate number of digits in each anchored is selected.

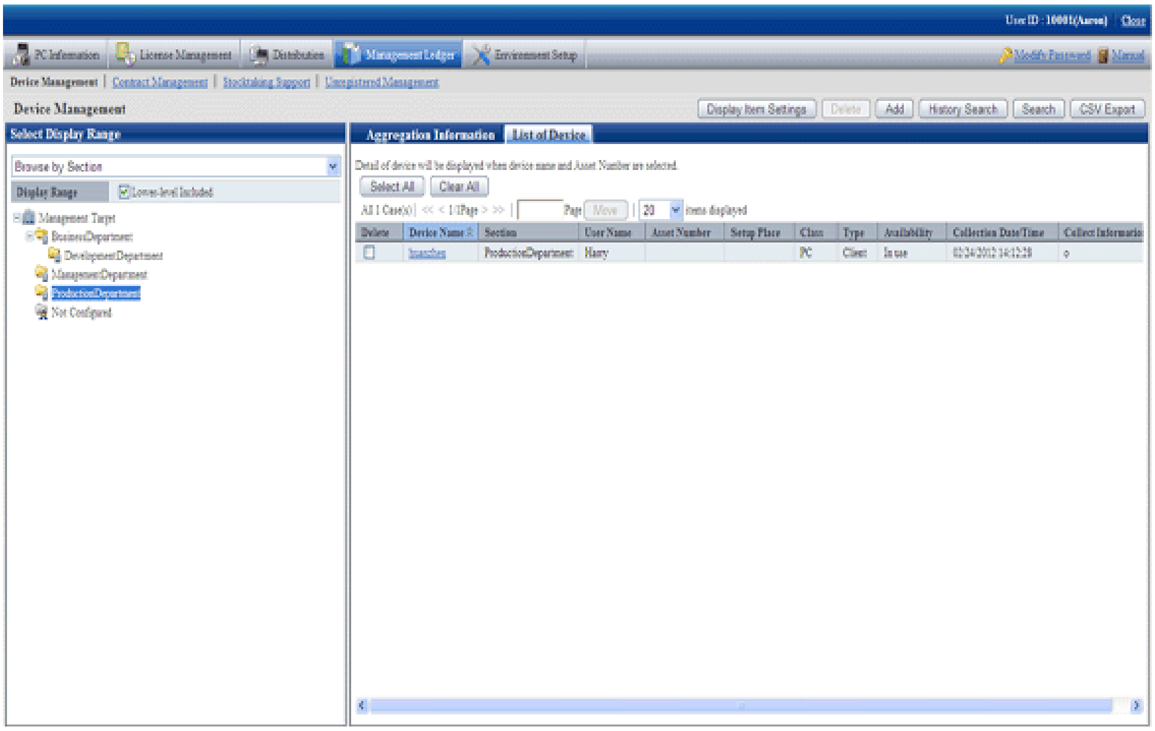
Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Unused PC(s)	Number of non-PC(s)
Total	15	2	2	1	0

Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Unused PC(s)	Number of non-PC(s)
BusinessDepartment	10	2	2	1	0
DevelopmentDepartment	5	0	0	0	0

List of Device

Display the management target devices by section, type or location.

For example, the device list is displayed as follows by section:



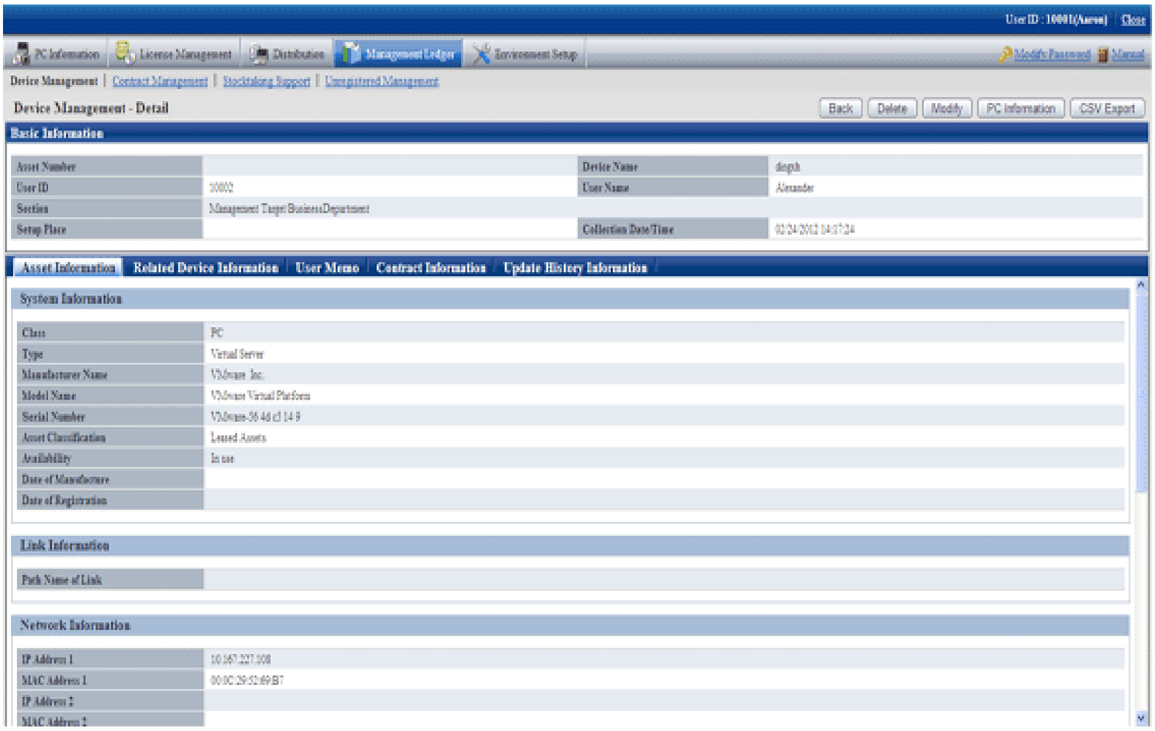
Detail of device will be displayed when device name and Asset Number are selected.

Delete	Device Name	Section	User Name	Asset Number	Setup Place	Class	Type	Availability	Collection Date/Time	Collect Informatio
□	[illegible]	ProductionDepartment	Harry			PC	Client	In use	02/24/2012 14:12:28	o

Details

Display the detailed information of the management object devices. Detailed information includes device information (Setup Place,/ Manufacturer Name,Main-body Information), user information, contract information and hardware information, etc.

Detailed information is shown below:



Asset Number		Device Name	[illegible]
User ID	10002	User Name	Alexander
Section	Management Target BusinessDepartment		
Setup Place		Collection Date/Time	02/24/2012 14:17:24

System Information

Class	PC
Type	Virtual Server
Manufacturer Name	VMware, Inc.
Model Name	VMware Virtual Platform
Serial Number	VMware-56 4d c1 14 9
Asset Classification	Leased Assets
Availability	In use
Date of Manufacture	
Date of Registration	

Link Information

Path Name of Link	

Network Information

IP Address 1	10.167.227.108
MAC Address 1	00:0C:29:52:69:B7
IP Address 2	
MAC Address 2	

Register, change or delete device information

Register, change or delete device information by device.

The administrator can both confirm the current device information and change device data.

In addition, device information of register, change and deletion results will be saved as historical information.

Note

The section administrator cannot delete the device information of other sections

The section administrator can only delete the information of the devices in his/her section or the subordinate section.

If a device relates to the one under the management of administrator and belongs to another section, the information about this device cannot be deleted.

In this case, the npte “The device belongs to another section and is undeletable” will be displayed in the above mentioned window.

Save device account of device information

Save device information (aggregation information, device list and device details) to CSV files respectively.

The saved data can be used in other documents, or linked with information of other systems, or used for data comparison.

In addition, in the device information display window, the device information can be output to CSV files used as asset information registration or change files. The device information can be uniformly changed through editing and uniformly registering these output files by means of the asset information registration or change function.

Change history of Device Information

Device setup and the device status prior to removal, transfer, inventory verification, return or discard shall be changed as historical information for management so as to make sure the previous usage ssatus of the device.

Application method

The methods to use the change history function of device information are shown below:

- After a large scale of organizational or personnel change, the system administrator wants to confirm whether any omission or error occurs during device removal.

  Display the device list removed in a specific period to confirm whether the devices have been correctly removed from the previous Setup Place.

- The system administrator wants to make sure the number of new PCs and their sections.

  Display the device list newly added in a specific period to confirm which sections they are installed in.

- The section administrator wants to make sure where the unknown devices newly added in his/her section come during inventory verification.

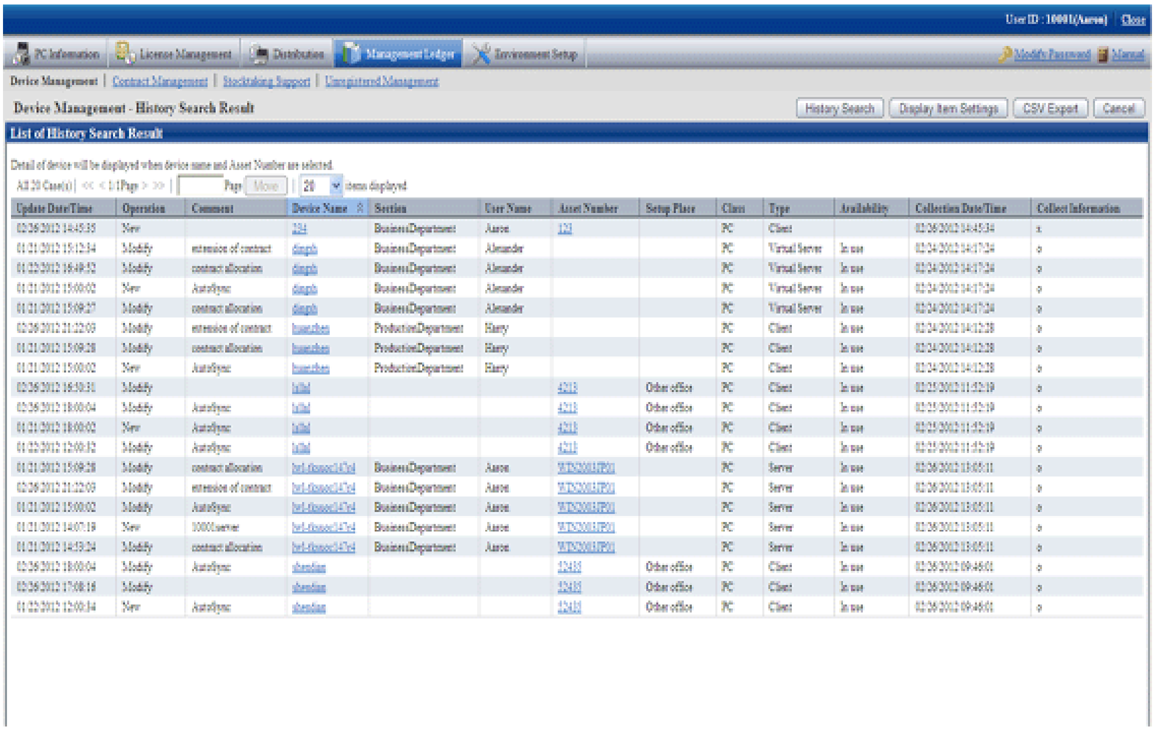
  According to the device Asset Number of new device, search the device history information to confirm the previous user and Setup Place of the device.

- During change of device information, if the administrator wants to change the device information incorrectly changed to the previous state.

  Confirm the information prior to change according to the change history of the object device and change it to the previous state.

“History Search Result” window

Confirm the update history in the “History Search Result” window.



Device Management - History Search Result

List of History Search Result

Detail of device will be displayed when device name and Asset Number are selected.

All 20 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Update Date/Time	Operation	Comment	Device Name	Section	User Name	Asset Number	Setup Place	Class	Type	Availability	Collection Date/Time	Collect Information
02/26/2012 14:45:35	New		124	BusinessDepartment	Aaron	123		PC	Client		02/26/2012 14:45:34	x
01/21/2012 15:12:34	Modify	extension of contract	dingzh	BusinessDepartment	Alexander			PC	Virtual Server	In use	02/24/2012 14:17:24	o
01/22/2012 16:49:52	Modify	contract allocation	dingzh	BusinessDepartment	Alexander			PC	Virtual Server	In use	02/24/2012 14:17:24	o
01/21/2012 15:00:02	New	AutoSync	dingzh	BusinessDepartment	Alexander			PC	Virtual Server	In use	02/24/2012 14:17:24	o
01/21/2012 15:09:27	Modify	contract allocation	dingzh	BusinessDepartment	Alexander			PC	Virtual Server	In use	02/24/2012 14:17:24	o
02/26/2012 21:22:09	Modify	extension of contract	huanzhen	ProductionDepartment	Harry			PC	Client	In use	02/24/2012 14:12:28	o
01/21/2012 15:09:28	Modify	contract allocation	huanzhen	ProductionDepartment	Harry			PC	Client	In use	02/24/2012 14:12:28	o
01/21/2012 15:00:02	New	AutoSync	huanzhen	ProductionDepartment	Harry			PC	Client	In use	02/24/2012 14:12:28	o
02/26/2012 16:50:31	Modify		taihd			4213	Other office	PC	Client	In use	02/25/2012 11:52:19	o
02/26/2012 18:00:04	Modify	AutoSync	taihd			4213	Other office	PC	Client	In use	02/25/2012 11:52:19	o
01/21/2012 18:00:02	New	AutoSync	taihd			4213	Other office	PC	Client	In use	02/25/2012 11:52:19	o
01/22/2012 12:00:12	Modify	AutoSync	taihd			4213	Other office	PC	Client	In use	02/25/2012 11:52:19	o
01/21/2012 15:09:28	Modify	contract allocation	hrl-tlosoc147e4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
02/26/2012 21:22:09	Modify	extension of contract	hrl-tlosoc147e4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
01/21/2012 15:00:02	Modify	AutoSync	hrl-tlosoc147e4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
01/21/2012 14:07:19	New	10001server	hrl-tlosoc147e4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
01/21/2012 14:53:24	Modify	contract allocation	hrl-tlosoc147e4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
02/26/2012 18:00:04	Modify	AutoSync	shendian			12435	Other office	PC	Client	In use	02/26/2012 09:46:01	o
02/26/2012 17:08:16	Modify		shendian			12435	Other office	PC	Client	In use	02/26/2012 09:46:01	o
01/22/2012 12:00:34	New	AutoSync	shendian			12435	Other office	PC	Client	In use	02/26/2012 09:46:01	o

2.7.2 Contract Management

The following operations can be carried out on the management target devices by means of the contract information management function.

- Confirm contract information by section or type
- Register, change or delete contract information
- Distribute contract information
- Save the device account of contract information
- Remind of contract term
- Contract extension

Confirm contract information by section or type

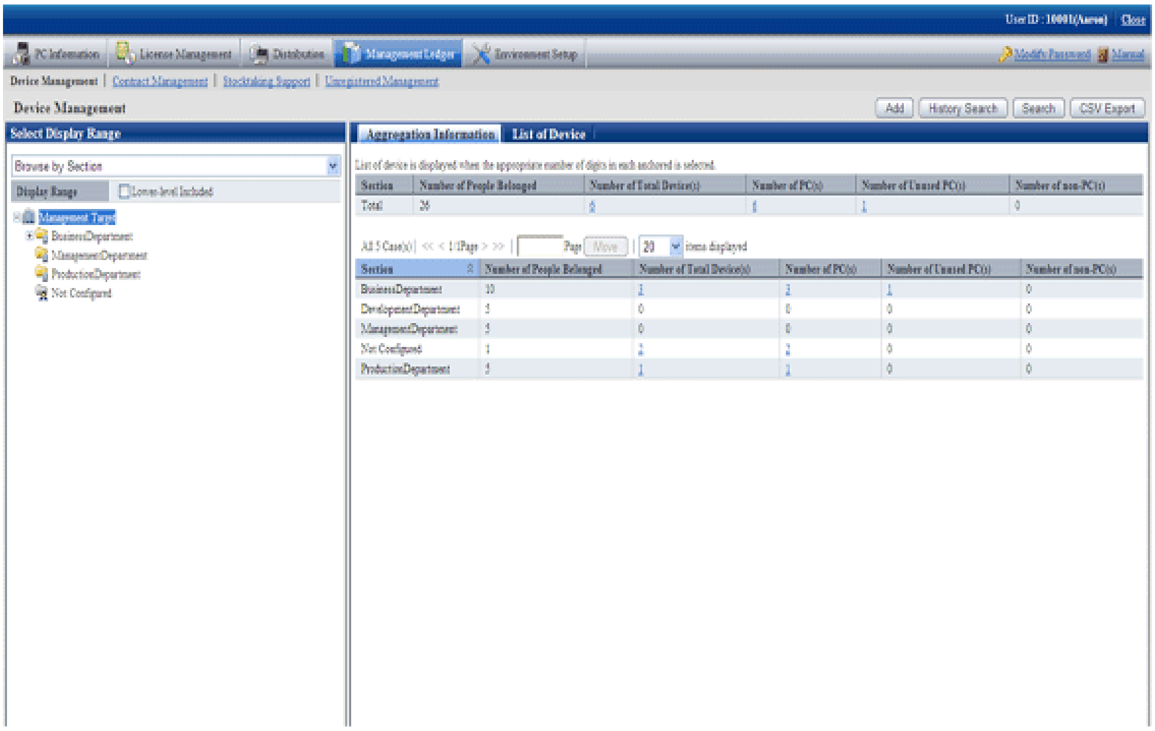
Display contract information meeting the requirements of user operation.

The user can easily search contract information to display the search results serving the purpose.

Aggregation Information

Display the contract quantity of management object devices and the number of contract device by section or class.

For example, the aggregation information is displayed by section as below:



List of device is displayed when the appropriate number of digits in each anchored is selected.

Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Unused PC(s)	Number of non-PC(s)
Total	26	6	6	1	0

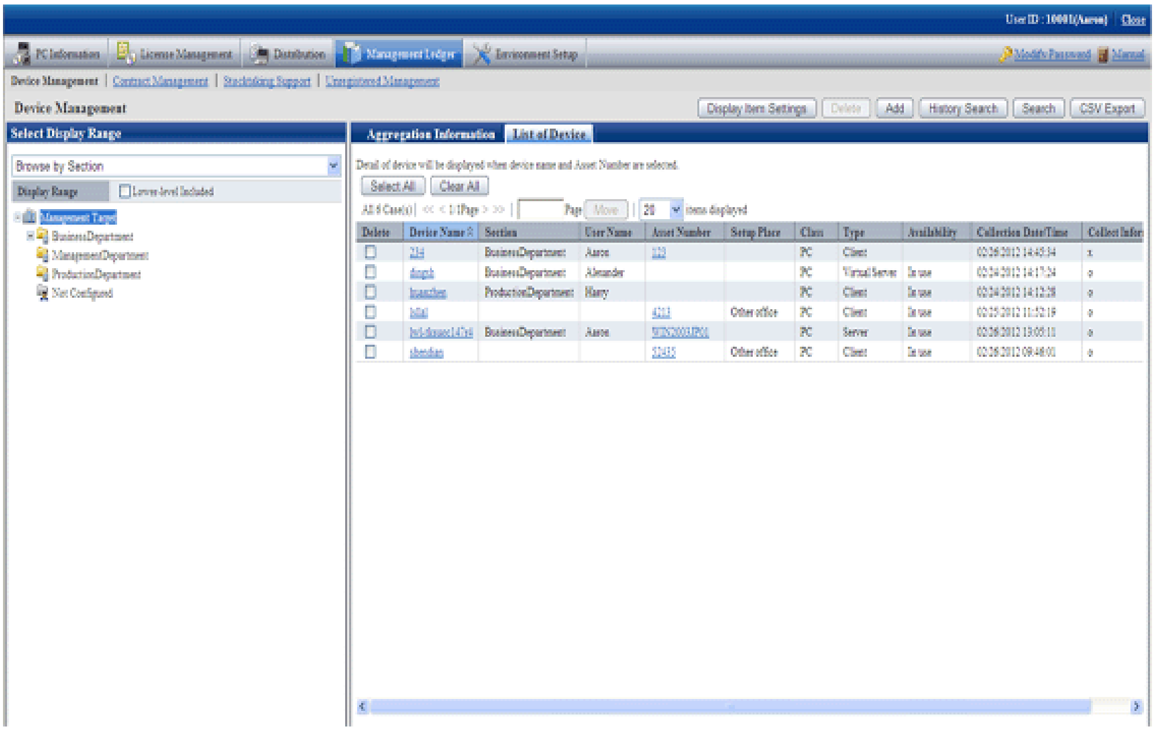
All 5 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Unused PC(s)	Number of non-PC(s)
BusinessDepartment	10	3	3	1	0
DevelopmentDepartment	5	0	0	0	0
ManagementDepartment	5	0	0	0	0
Not Configured	1	2	2	0	0
ProductionDepartment	5	1	1	0	0

List of Contract

Display the contract information of management target devices and the number of contract device by section or class.

For example, the contract list is displayed by section as below:



Detail of device will be displayed when device name and Asset Number are selected.

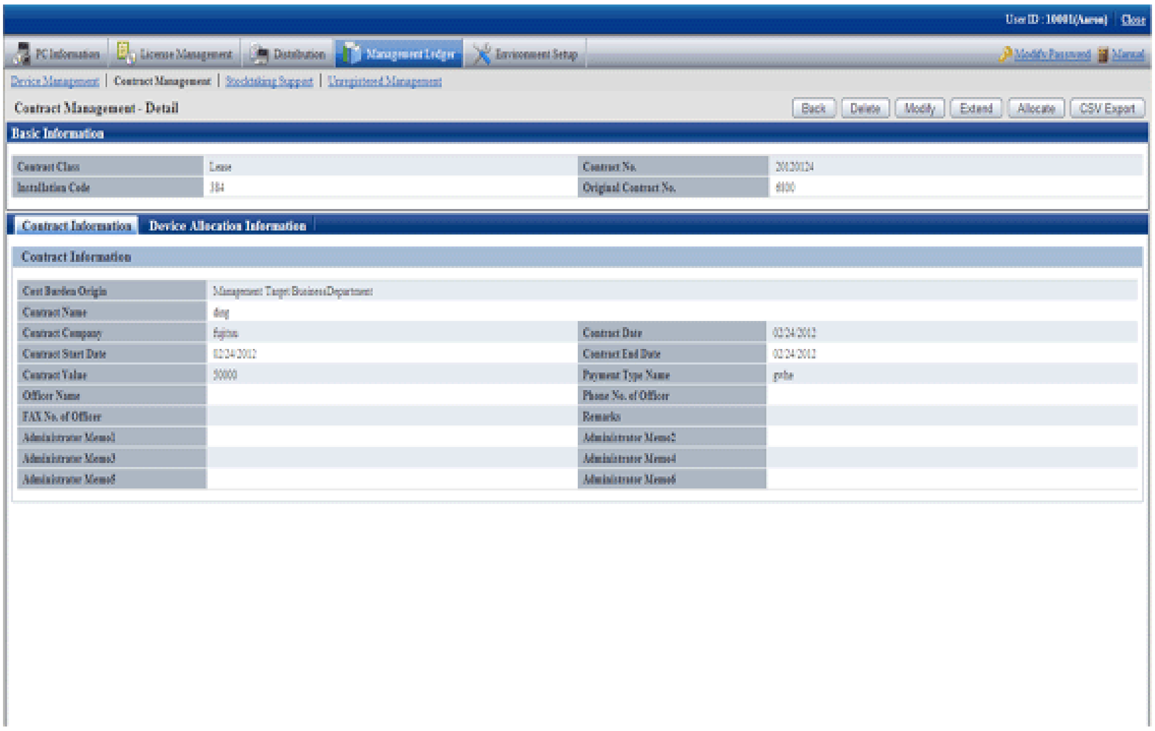
All 6 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Delete	Device Name	Section	User Name	Asset Number	Setup Place	Class	Type	Availability	Collection Date/Time	Collect Infor
□	234	BusinessDepartment	Aaron	123		PC	Client		02/26/2012 14:45:34	x
□	dongsh	BusinessDepartment	Alexander			PC	Virtual Server	In use	02/24/2012 14:17:24	o
□	huanzhen	ProductionDepartment	Harry			PC	Client	In use	02/24/2012 14:12:28	o
□	bilal			4213	Other office	PC	Client	In use	02/25/2012 11:52:19	o
□	bvl-dongsh14?4	BusinessDepartment	Aaron	WIN2003JP01		PC	Server	In use	02/26/2012 13:05:11	o
□	shenhan			32435	Other office	PC	Client	In use	02/26/2012 09:46:01	o

Contract Management - Detail

The contract information of selected management target devices includes contract company, contract term, and detailed information of contract amount and contract device list.

Detailed information is shown below:



Contract Management - Detail

Basic Information

Contract Class	Lease	Contract No.	20120124
Installation Code	384	Original Contract No.	6100

Contract Information

Cost Burden Origin	Management Target BusinessDepartment		
Contract Name	dng		
Contract Company	fujitsu	Contract Date	02/24/2012
Contract Start Date	02/24/2012	Contract End Date	02/24/2012
Contract Value	50000	Payment Type Name	gzhe
Officer Name		Phone No. of Officer	
FAX No. of Officer		Remarks	
Administrator Memo1		Administrator Memo2	
Administrator Memo3		Administrator Memo4	
Administrator Memo5		Administrator Memo6	

Register, change, or delete contract information

Register, change or delete information of every contract one after another.

The administrator can both confirm the current contract information and change contract data.

- Register or change contract information
- Delete contract information

Distribute contract information

Distribute the device information according to each contract unit.

It is required to combine contract information with device information in order to manage contract information. Device information can be smoothly and correctly distributed through filtering and searching the devices contained in the contract information.

Enter the filtering condition in the “Filter Distributed Devices” window to search the device information. Select the devices to be distributed from the searched device list to distribute device information.

Save device account of contract information

Save contract information (aggregation information, contract list, details of contract) as CSV files respectively.

The saved data can be used in other documents, or linked with information of other systems, or used for data comparison.

In addition, in the contract information display window, the contract information can be output to CSV files/ change files used as asset information registration. The contract information can be uniformly changed through editing and uniformly registering these output files by means of the asset information registration/change function.

Remind of contract term

When the lease/rent/maintenance contract term draws near or at the contract end date, the system administrator is notified of contract information by E-mail.

If it is necessary to extend the device lease/rent/maintenance contract term, it is required to adjust the device application policy to extend contract company or to sign a new contract and go through the formalities of contract extension with the signing company before the contract expires. However, if the contract term (e.g. lease contract) is as long as 4 years, the system administrator shall often take the trouble to audit the terms of different contracts.

Therefore, the contract management workload of the system administrator can be reduced through automatically reminding him/her by E-mail before the contract end date or at the expiration date of the contract.

Contract extension

Extend the contract according to the contract information (lease/rent/maintenance) management by Systemwalker Desktop Patrol.

After the contract is extended, it is required to create the information of extended contract and the device information distributed to the original contract will be transferred into the information of extended contract.

In addition, the information of extended contract also contains “Original Contact No”, which can be confirmed in the contract list window to confirm which contract is renewed.

2.7.3 Stocktaking Support

The following operations can be carried out via the function of supporting inventory verification of management target devices.

- Confirm inventory verification status by section, type or location
- Change inventory verification state
- Inventory verification Operational Configuration
- Save device account of inventory verification status
- Correction of Place

Confirm inventory verification status by section, type or locating

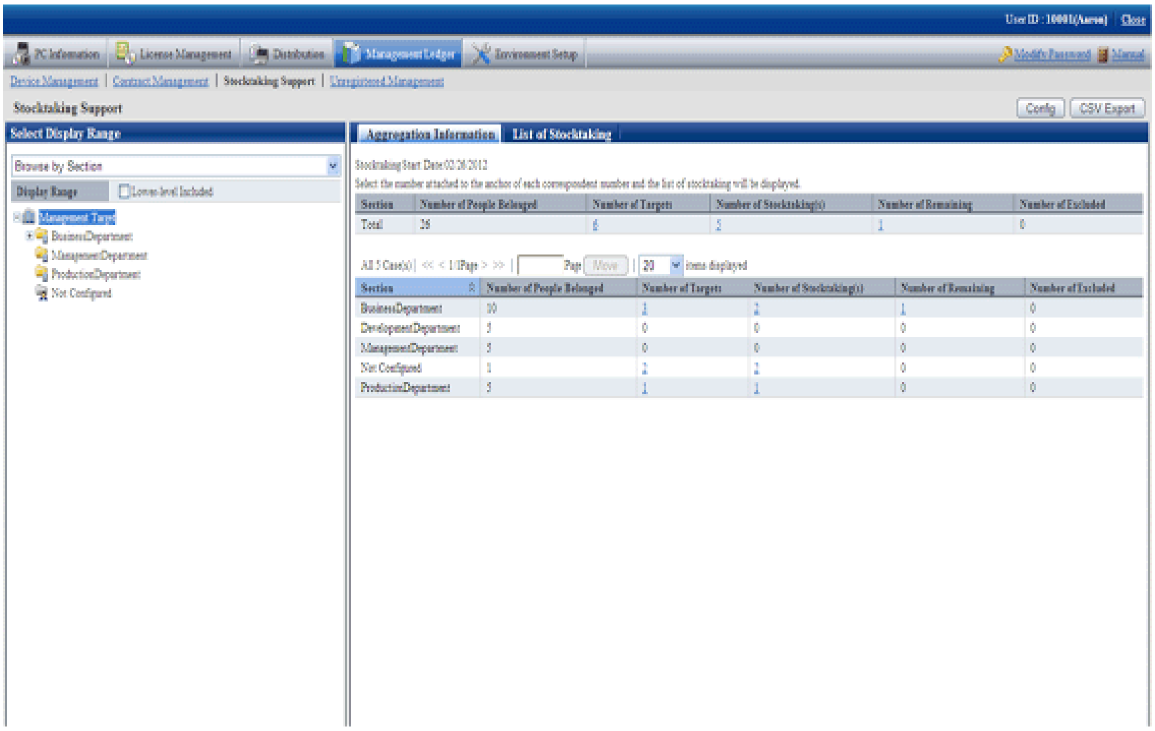
Display inventory verification status meeting the requirements of user operation.

The user can easily search inventory verification status to display the search results serving the purpose.

Aggregation Information

Display the quantity of inventory verification objects and inventory verification status by section, type or location.

For example, aggregation information is displayed by section as below:



Stocktaking Start Date:02/26/2012

Select the number attached to the anchor of each correspondent number and the list of stocktaking will be displayed.

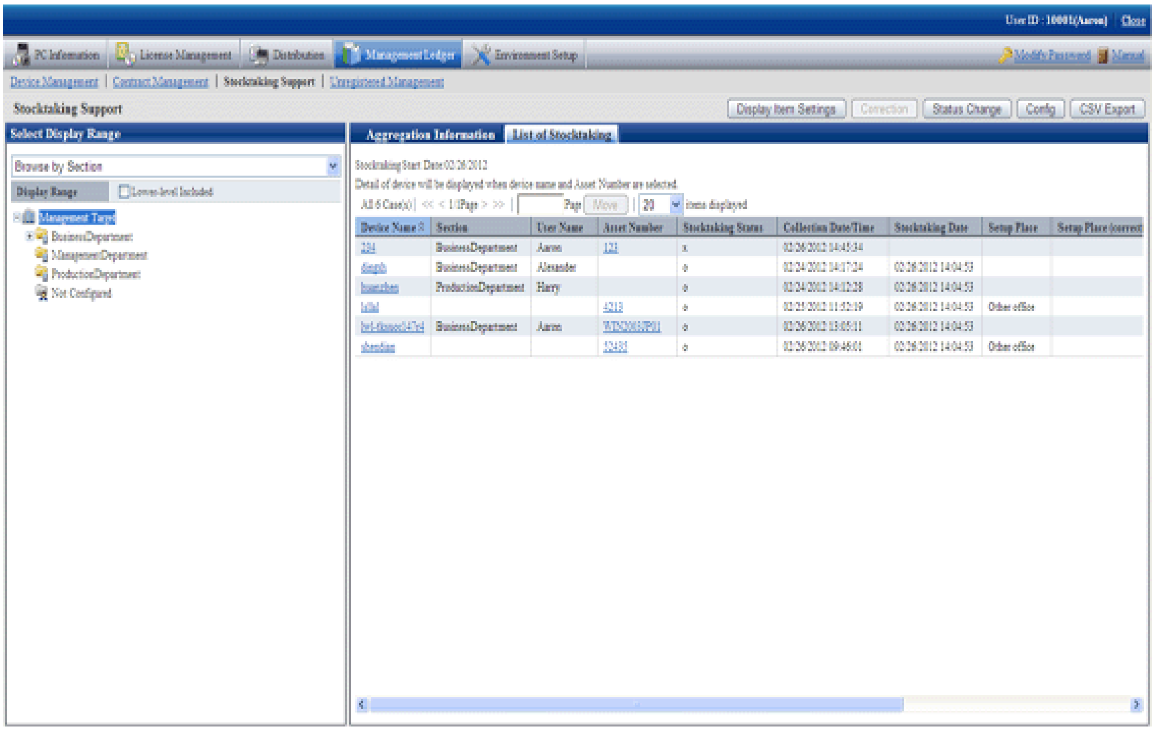
Section	Number of People Belonged	Number of Targets	Number of Stocktaking(s)	Number of Remaining	Number of Excluded
Total	26	6	5	1	0

Section	Number of People Belonged	Number of Targets	Number of Stocktaking(s)	Number of Remaining	Number of Excluded
BusinessDepartment	10	3	2	1	0
DevelopmentDepartment	5	0	0	0	0
ManagementDepartment	5	0	0	0	0
Not Configured	1	2	2	0	0
ProductionDepartment	5	1	1	0	0

List of Stocktaking

Display the list of stocktaking by section, type or location.

For example, the list of stocktaking are displayed by section as below:



Stocktaking Start Date:02/26/2012

Detail of device will be displayed when device name and Asset Number are selected.

Device Name	Section	User Name	Asset Number	Stocktaking Status	Collection Date/Time	Stocktaking Date	Setup Place	Setup Place (correct
234	BusinessDepartment	Aaron	123	x	02/26/2012 14:45:34			
dingzh	BusinessDepartment	Alexander		o	02/24/2012 14:17:24	02/26/2012 14:04:53		
huanzhen	ProductionDepartment	Harry		o	02/24/2012 14:12:28	02/26/2012 14:04:53		
lzlhl			4213	o	02/25/2012 11:52:19	02/26/2012 14:04:53	Other office	
bwl-tkmoo547e4	BusinessDepartment	Aaron	WIN2003JP01	o	02/26/2012 13:05:11	02/26/2012 14:04:53		
zhendian			12435	o	02/26/2012 09:46:01	02/26/2012 14:04:53	Other office	

Change stocktaking verification status

The administrator can change the inventory verification status of object devices manually. The setting contents are shown below:

- Set to Stocktaking Completed
- Set to Stocktaking Uncompleted

- Set to Excluded Stocktaking

Except "Inventory verification completed" and "Inventory verification not completed", the devices not considered as inventory verification objects can be set as Set to Excluded Stocktaking.

Stocktaking verification Operational Configuration

Operational Configuration of inventory verification object devices include:

- Stocktaking Start Date
- Method to determine stocktaking status
- Correction Result of Place

If the stocktaking start date of the object device has been set, the devices inventory verification period from the commencement date to the present time shall be confirmed. And it will turn into "inventory verification completed" automatically. For example, when Systemwalker Desktop Patrol collects inventory information for inventory verification, the setup of the inventory verification object devices will turn into "inventory verification completed".

After the stocktaking start date is set, the system administrator can confirm inventory verification status of the PC according to the inventory information collected in Systemwalker Desktop Patrol, or confirm inventory verification status through automatic detection on device information for the purpose of reducing inventory verification confirmation operation and carrying out management correctly.

In addition, when the inventory information collected in Systemwalker Desktop Patrol is used as the basis to judge the inventory verification status as "inventory verification completed", it is required to set the Method to determine stocktaking status.

Because the inventory verification objects are remote devices, the system administrator can set the object devices as "inventory verification completed" in the inventory verification status display window when it is impossible to carry out inventory verification according to the inventory information collected in Systemwalker Desktop Patrol. On the contrary, the devices set as "inventory verification completed" shall be restored to "inventory verification not completed".

The system administrator can change the setups (inventory verification completed/not completed) to support various applications.

Save device account of stocktaking verification status

Save inventory verification status (aggregation information, inventory verification object list) to CSV files respectively.

The saved data can be used in other documents, or linked with information of other systems, or used for data comparison.

Correction of Place

The user can correct the Setup Place through collecting inventory information and manual input according to the IP address recorded in the assets device account and network segment management information registered in advance by the administrator. If the IP address of the device changes due to removal, the user can correct the Setup Place during inventory verification, and reflect the Setup Place to the assets device account simply and correctly.

2.7.4 Unregistered Management

This is a function to automatically detect the devices connecting with the network to confirm the devices unregistered in the management device account. The following methods can be used for automatic detection on device information.

- Network Segment-based Check

  It is a method to install ADTs by network segment and detect device information.

- Batch Network Check

  It is a method to detect the information of devices supporting ICMP or SNMP via the CS server.

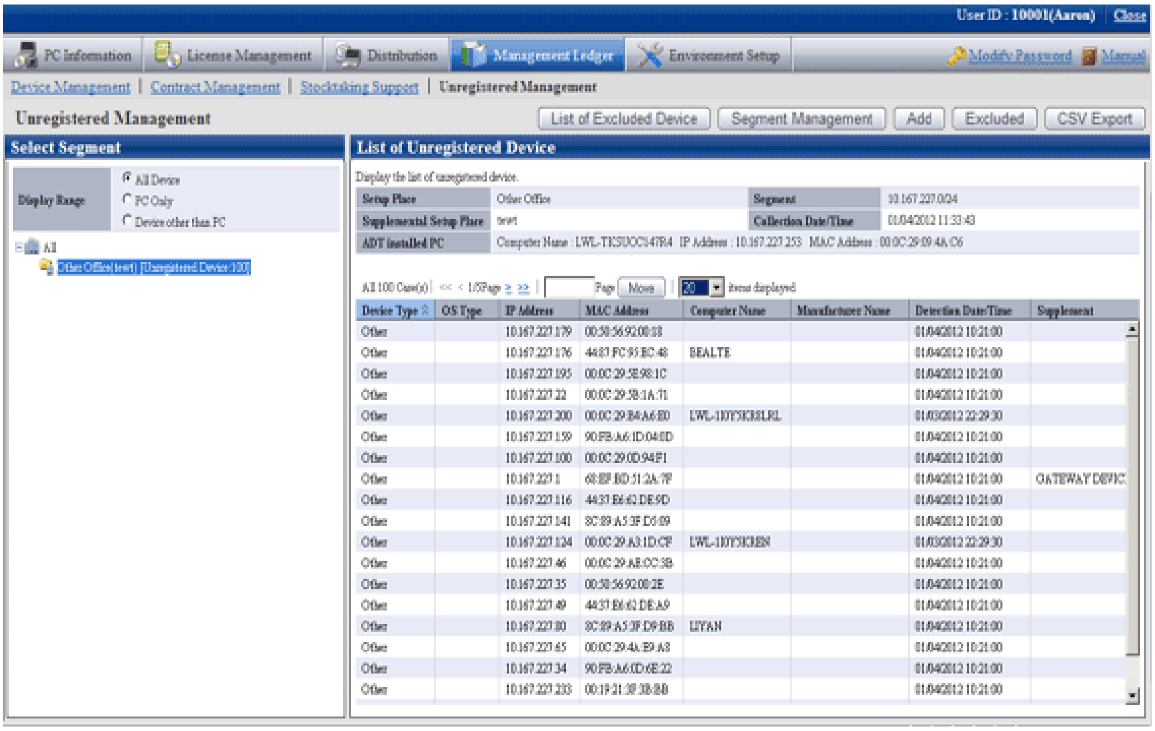
Register the unregistered devices in the unregistered device management window. Alternatively, the administrator can also export the unregistered devices to a file for registration at one time.

Unregistered device management includes:

- Confirming information of unregistered devices
- Registering unregistered devices
- Displaying non-object setup and non-registered target devices
- Network segment management
- Saving device account information of unregistered devices

Confirm unregistered devices

Unregistered devices can be displayed by network segment.



Display Range: ● All Device ○ PC Only ○ Device other than PC

Display the list of unregistered device.

Setup Place	Other Office	Segment	10.167.227.0/24
Supplemental Setup Place	test	Collection Date/Time	01/04/2012 11:33:43
ADT Installed PC	Computer Name : LWL-TKSUOC347R4 IP Address : 10.167.227.253 MAC Address : 00:0C:29:09:4A:C6		

All 100 Case(s) | << < 1/5Page > >> | Page Move | 20 items displayed

Device Type	OS Type	IP Address	MAC Address	Computer Name	Manufacturer Name	Detection Date/Time	Supplement
Other		10.167.227.179	00:50:56:92:00:18			01/04/2012 10:21:00	
Other		10.167.227.176	44:87:FC:95:EC:48	BEALTE		01/04/2012 10:21:00	
Other		10.167.227.195	00:0C:29:5E:98:1C			01/04/2012 10:21:00	
Other		10.167.227.22	00:0C:29:5B:1A:71			01/04/2012 10:21:00	
Other		10.167.227.200	00:0C:29:B4:A6:E0	LWL-10Y5KR8LRL		01/03/2012 22:29:30	
Other		10.167.227.159	90:FB:A6:1D:04:0D			01/04/2012 10:21:00	
Other		10.167.227.100	00:0C:29:0D:94:F1			01/04/2012 10:21:00	
Other		10.167.227.1	68:EF:BD:51:2A:7F			01/04/2012 10:21:00	GATEWAY DEVIC
Other		10.167.227.116	44:37:E6:62:DE:9D			01/04/2012 10:21:00	
Other		10.167.227.141	8C:89:A5:3F:D6:09			01/04/2012 10:21:00	
Other		10.167.227.124	00:0C:29:A3:1D:CF	LWL-10Y5KREN		01/03/2012 22:29:30	
Other		10.167.227.46	00:0C:29:AE:CC:3B			01/04/2012 10:21:00	
Other		10.167.227.35	00:50:56:92:00:2E			01/04/2012 10:21:00	
Other		10.167.227.49	44:37:E6:62:DE:A9			01/04/2012 10:21:00	
Other		10.167.227.80	8C:89:A5:3F:D9:BB	LIYAN		01/04/2012 10:21:00	
Other		10.167.227.65	00:0C:29:4A:E9:A3			01/04/2012 10:21:00	
Other		10.167.227.34	90:FB:A6:0D:6E:22			01/04/2012 10:21:00	
Other		10.167.227.233	00:19:21:3F:3B:B8			01/04/2012 10:21:00	

Register unregistered devices

Register the management target devices with assets device account in the unregistered device display window.

Display non-object setup and non-registered target devices

Display the detected unregistered devices which are not classified as management objects of assets device account. In addition, non-object devices can also be displayed.

Network segment management

Prior to displaying unregistered devices or using the registration function, it is required to link the network segment management setup and Setup Place.

Save device account of unregistered devices

Save the information of unregistered devices to CSV files.

The saved data can be used in other documents, or linked with information of other systems, or used for data comparison.

2.8 Report Output Function

Report output function is a function to output the asset information and security information managed in Systemwalker Desktop Patrol as reports (3 reports in total).

- Asset Information Report

- Security Auditing Report
- Power Saving Countermeasure Auditing Report

2.8.1 Asset Information Report

It refers to the function to output or print the Asset Information managed in Systemwalker Desktop Patrol in the form of report (Microsoft® Excel format).

Charts and tables can be included in the output reports so that the administrator can master the current status and problems through visual inspection.

The following operations can be carried out during outputting the asset information report.

- Output report format files
- Layout Editing report

Output report format files

The asset information managed in Systemwalker Desktop Patrol shall be output to report format files (Microsoft® Excel format) for printing and output.

The following effects can be expected through outputting the asset information in report format.

- Effectively mastering asset information

  Assets condition can be effectively mastered through browsing the output asset information overview and asset information list.

- Effectively mastering problems

  Different problems can be mastered through visual inspection on the charts and tables in the reports.

- Displaying assets management contents in written form

  The operation results (e.g. inventory verification) can be saved in written form

The following reports can be output:

- Assets utilization status

  Output the utilization status of assets in the form of report (used assets/idle assets).

- List of contracts

  Output the contract information in the form of report (lease/rent/maintenance)

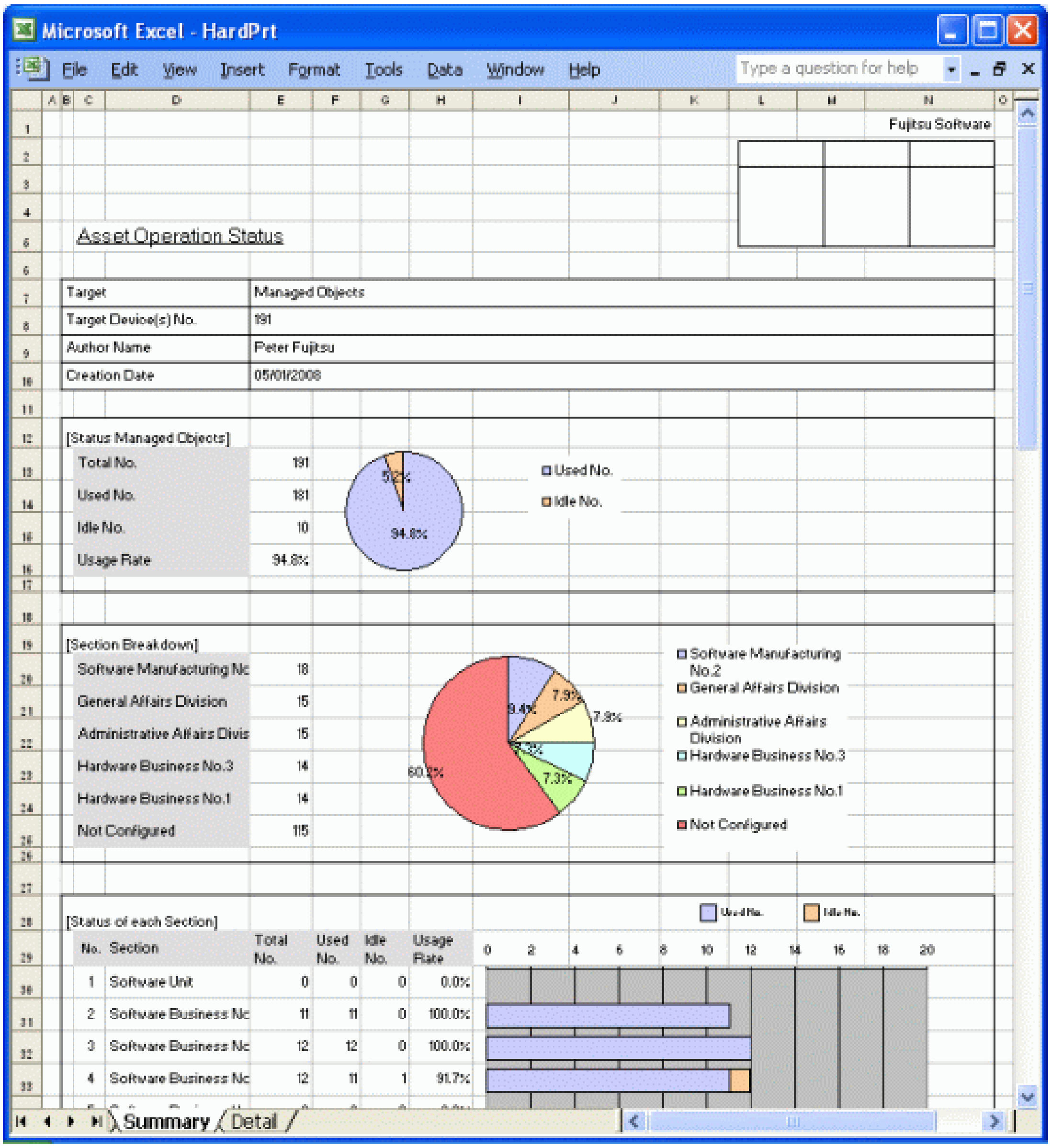
- Inventory verification status

  Output the inventory verification result of assets in the form of report.

- License application status

  Output the application status of software licenses in the form of report.

For example, the report of assets utilization status can be output as below:



Fujitsu Software

Asset Operation Status

Target	Managed Objects
Target Device(s) No.	191
Author Name	Peter Fujitsu
Creation Date	05/01/2008

[Status Managed Objects]

Total No.	191
Used No.	181
Idle No.	10
Usage Rate	94.8%

[Section Breakdown]

Software Manufacturing Nc	18
General Affairs Division	15
Administrative Affairs Divis	15
Hardware Business No.3	14
Hardware Business No.1	14
Not Configured	115

[Status of each Section]

No.	Section	Total No.	Used No.	Idle No.	Usage Rate
1	Software Unit	0	0	0	0.0%
2	Software Business Nc	11	11	0	100.0%
3	Software Business Nc	12	12	0	100.0%
4	Software Business Nc	12	11	1	91.7%

Edit report layout

It refers to changing the layout of the report of Asset information managed in Systemwalker Desktop Patrol, i.e. changing report title, filtering condition and the reports to be output.

In addition, report layout can be changed by means of Microsoft® Excel after the output data is saved in the form of report (Microsoft® Excel format).

2.8.2 Security Auditing Report

It is required to audit the application status of security countermeasures according to the auditing guide decided by the user. The security auditing result can be used for changing security countermeasures.

In addition, the security auditing result can be output in the form of report and used as attestation of correct execution of security countermeasures.

Auditing Pointer setups

Security guide is an evaluation standard to judge which security policy is the best based on security auditing. Security auditing shall be carried out in accordance with the auditing pointer. The following audited items are contained in the auditing pointer; the user shall decide which items to select.

- Hardware
- OS (system)
- OS (user)
- Internet Explorer
- Security patch application
- Anti-virus software
- Applied virus definition
- Access control
- Encryption status
- Installed auditing software
- Applications

Systemwalker Desktop Patrol provides “Information Leakage Countermeasure” and “Vulnerability Countermeasure” as recommended auditing pointer. The user can define the recommended auditing pointers of him/her and use them after changing the audited items according to application methods and the environment.

In addition, besides recommended auditing pointers, the user-defined auditing pointers can be used for security auditing.

Application method

Systemwalker Desktop Patrol recommends two application methods of auditing security countermeasure.

- Rectification Periodis set

  Because PCs always moves, it must be ensured that security auditing is carried out when executing the security countermeasures correctly every month. The problems can be handled during rectification period, so security auditing must be strictly carried out.

- Rectification Period is not set

  Being a safe execution policy of security auditing, the security auditing rectification period is not necessary to set, but it is necessary for judging security auditing status by month. Any problem must be completely handled before the next month.

Application method can be changed. For the newly installed Systemwalker Desktop Patrol, if the completion rate of security auditing is lower, it is required to set the security auditing rectification period, and the security auditing rectification period can be canceled after the Systemwalker Desktop Patrol can operate stably.

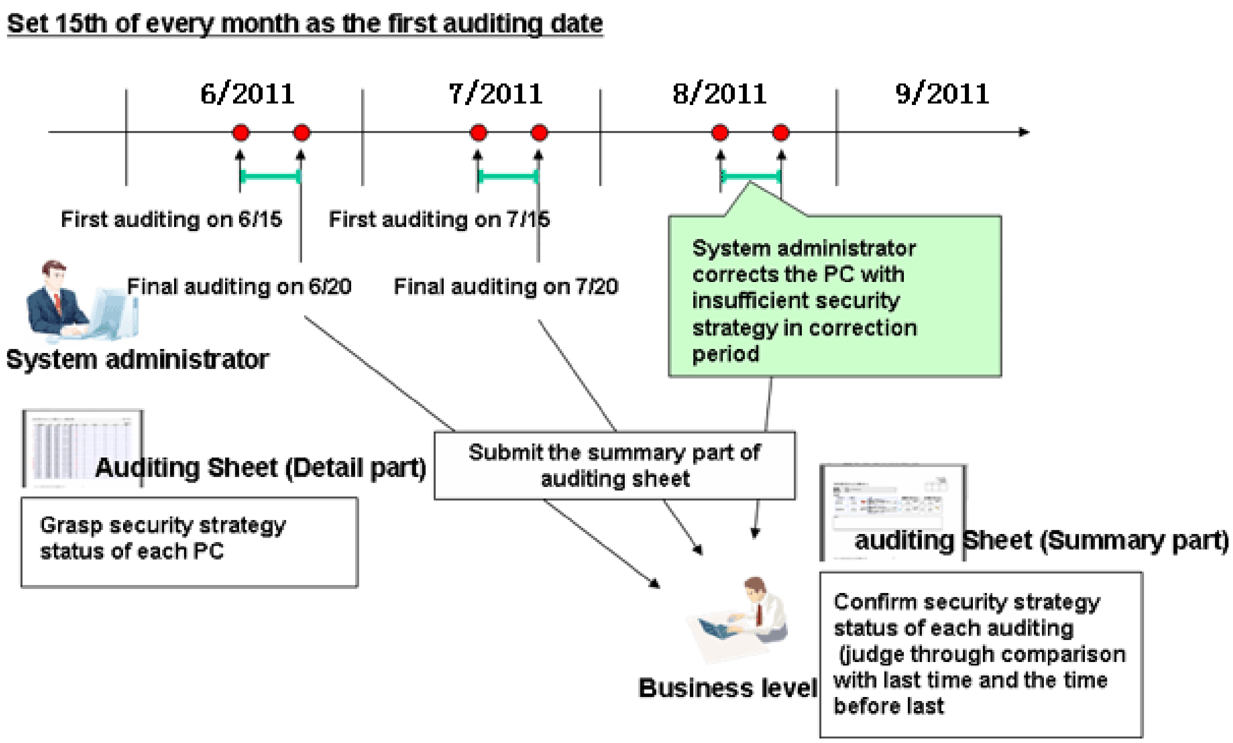
It is recommended that security auditing date and correction date should be set in Systemwalker Desktop Patrol so as to carry out periodic security auditing.

In addition, it is suggested that the information of Systemwalker Desktop Patrol should be imported by means of the automatic synchronous import function prior to the date of first auditing. Security auditing can be carried out by schedule at night.

Application status

Application on condition that a rectification period is set

When the 15th day in every month is set as the first auditing date, and the 20th day as the last auditing date, security auditing shall be carried out as the following case shown below. In the following case, it is required to execute security countermeasures and improve security countermeasure execution status from the first auditing date to the last.


Set 15th of every month as the first auditing date
6/2011
7/2011
8/2011
9/2011
First auditing on 6/15
First auditing on 7/15
Final auditing on 6/20
Final auditing on 7/20
System administrator corrects the PC with insufficient security strategy in correction period
System administrator
Auditing Sheet (Detail part)
Submit the summary part of auditing sheet
auditing Sheet (Summary part)
Grasp security strategy status of each PC
Confirm security strategy status of each auditing (judge through comparison with last time and the time before last
Business level

Security auditing shall be carried out according to the following procedure:

1. Output security auditing report at the first auditing date to master the current security countermeasure execution status.
2. Take security countermeasures after confirming that the security status is OK during the rectification period.

   Security auditing shall be carried out everyday during the rectification period, and security countermeasure shall be taken if the auditing result shows that the PC is not secure enough.

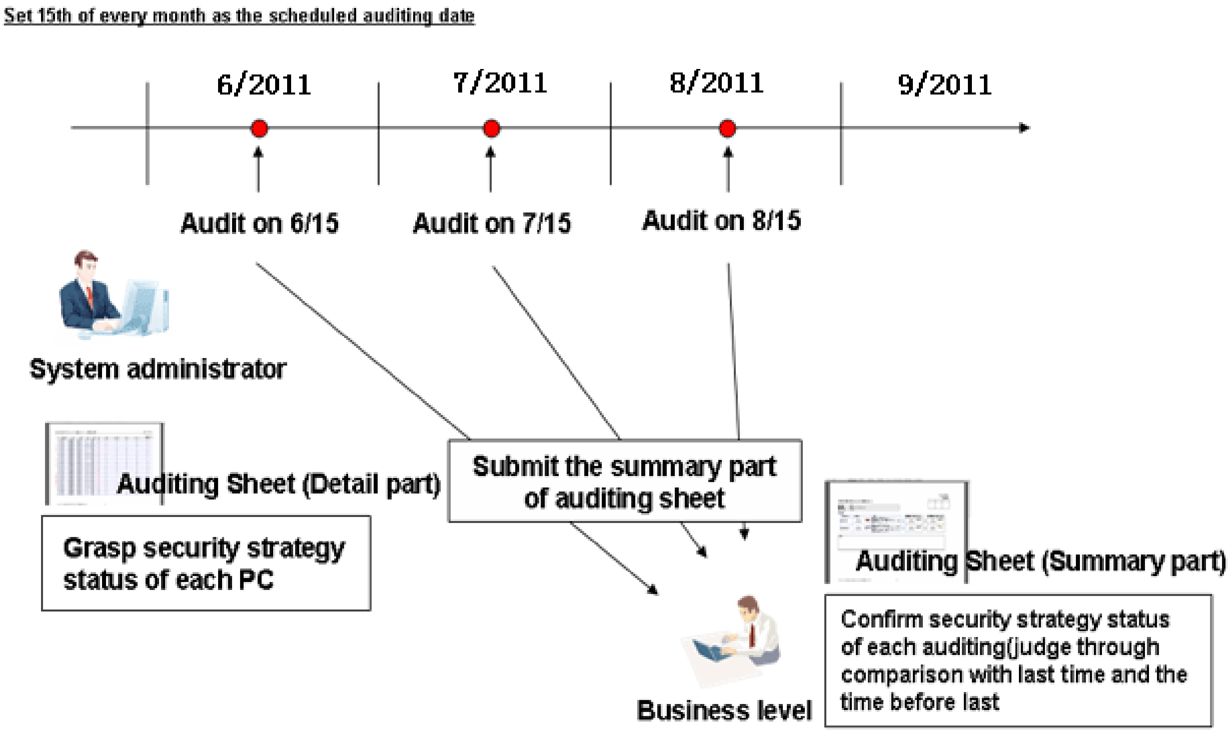
   After taking security countermeasures collect the inventory information from the PC and confirm no any problem exists according to the security auditing report.
3. On the last auditing date, output the final security auditing data as a security auditing report.

The system administrator shall carry out the first auditing at the 15th day in every month. In addition, the system administrator shall confirm the output security auditing result and correct the application status of the device to which security countermeasures should be taken prior to the 20th day. On the 20th day in every month, the system administrator shall submit the security auditing result to the manager in charge.

If the rectification period is set, when the auditing result has any problem, the user of the problematic PC can take security countermeasures. If the problem cannot be solved in a short time, a grace period (rectification period) can be given the PC user to solve the problem.

Application on condition that no rectification period is set

When the 15th day in every month is set as the first auditing date, security auditing shall be carried out as the following case shown below. In the following case, if no rectification period is set, the system administrator shall output the security auditing report to confirm the execution status of long-term security countermeasures.

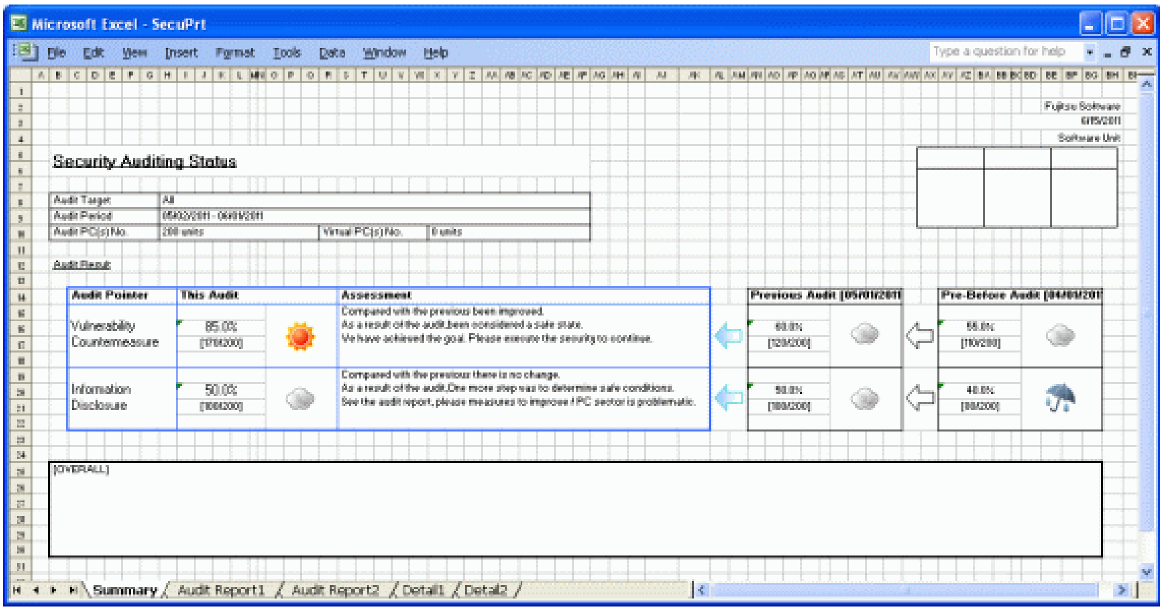

Set 15th of every month as the scheduled auditing date
6/2011
7/2011
8/2011
9/2011
Audit on 6/15
Audit on 7/15
Audit on 8/15
System administrator
Auditing Sheet (Detail part)
Grasp security strategy status of each PC
Submit the summary part of auditing sheet
Auditing Sheet (Summary part)
Confirm security strategy status of each auditing(judge through comparison with last time and the time before last
Business level

The system administrator shall take a regular security auditing at the 15th in every month. If security countermeasures have been taken, the system administrator shall carry out security auditing required when no rectification period is set when only needing to confirm the execution status of security countermeasures. If the auditing result becomes stable during the security auditing, the system administrator can give a judgment immediately.

Example of output security auditing report

Security auditing result shall be output as security auditing report. Security auditing report is a auditing or attestation report output to master and evaluate the application status of the security countermeasures against Systemwalker Desktop Patrol, Systemwalker Desktop Keeper and judge the risky section.

The following example is the output overview of security auditing report. The security auditing results for this time, last time or earlier can be output to confirm the changes in security status.



Fujitsu Software
6/15/2011
Software Unit

Security Auditing Status

Audit Target	All		
Audit Period	05/02/2011 - 06/01/2011		
Audit PC(s) No.	200 units	Virtual PC(s) No.	0 units

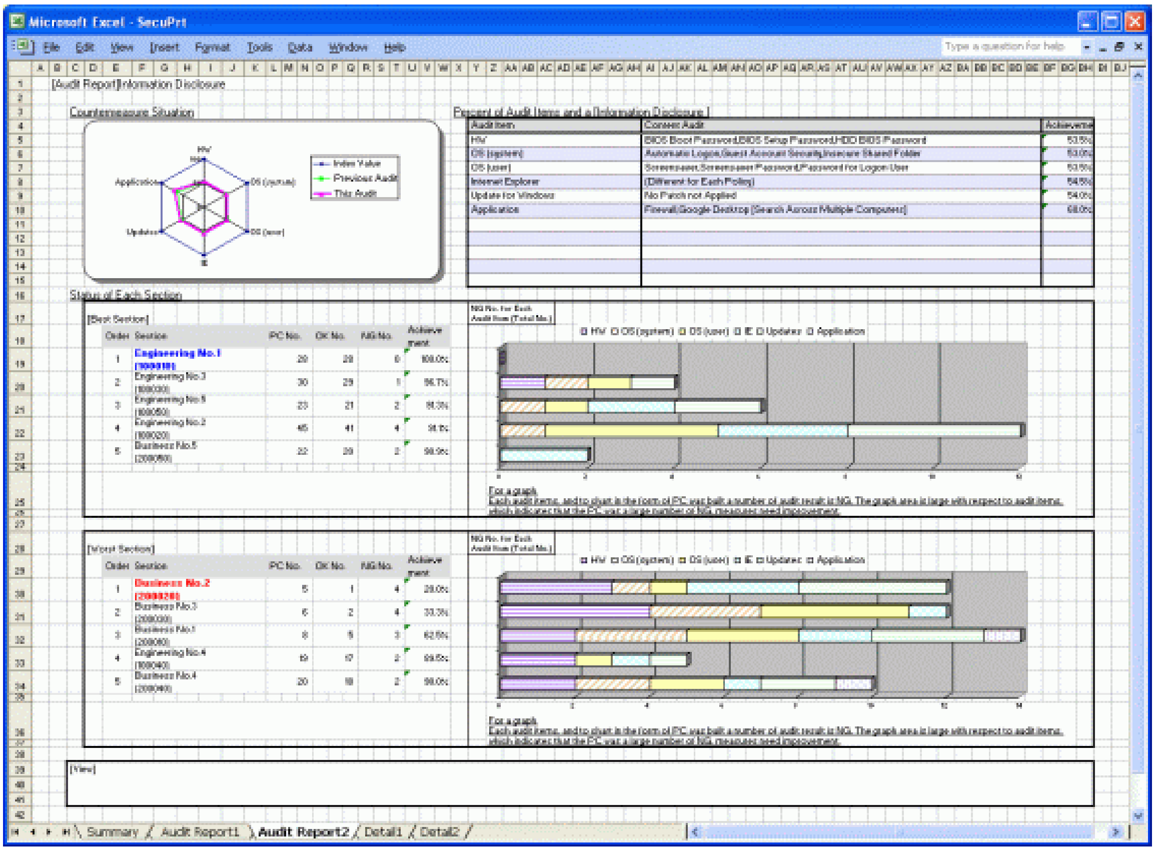
Audit Result

Audit Pointer	This Audit	Assessment	Previous Audit [05/01/2011	Pre-Before Audit [04/01/201
Vulnerability Countermeasure	85.0% [170/200]	Compared with the previous been improved. As a result of the audit,been considered a safe state. We have achieved the goal. Please execute the security to continue.	60.0% [120/200]	55.0% [110/200]
Information Disclosure	50.0% [100/200]	Compared with the previous there is no change. As a result of the audit,One more step was to determine safe conditions. See the audit report, please measures to improve / PC sector is problematic.	50.0% [100/200]	40.0% [80/200]

[OVERALL]

The following example is an output auditing report as part of security auditing report, which is used to display the auditing contents and completion rate of each audited item.

In addition, in the statistical result, it displays the best group having a higher percentage of OK events and the worst having a higher percentage of NG events, to urge the group taking insufficient security countermeasures to correct security countermeasures.


Microsoft Excel - SecuPrt
File Edit View Insert Format Tools Data Window Help
Type a question for help
HW
OS (system)
OS (user)
IE
Updates
Application
Index Value
Previous Audit
This Audit
NG No. for Each Audit Item (Total No.)
HW OS (system) OS (user) IE Updates Application
Summary
Audit Report1
Audit Report2
Detail1
Detail2

[Audit Report]Information Disclosure

Countermeasure Situation

Percent of Audit Items and a [Information Disclosure]

Audit Item	Content Audit	Achieveme
HW	BIOS Boot Password,BIOS Setup Password,HDD BIOS Password	53.5%
OS (system)	Automatic Logon,Guest Account Security,Insecure Shared Folder	53.0%
OS (user)	Screensaver,Screensaver Password,Password for Logon User	53.5%
Internet Explorer	(Different for Each Policy)	54.5%
Update for Windows	No Patch not Applied	54.0%
Application	Firewall,Google Desktop (Search Across Multiple Computers)	68.0%

Status of Each Section

[Best Section]

Order	Section	PC No.	OK No.	NG No.	Achievement
1	Engineering No.1 (100010)	20	20	0	100.0%
2	Engineering No.3 (100030)	30	29	1	96.7%
3	Engineering No.5 (100050)	23	21	2	91.3%
4	Engineering No.2 (100020)	45	41	4	91.1%
5	Business No.5 (200050)	22	20	2	90.9%

For a graph
Each audit items, and to chart in the form of PC was built a number of audit result is NG. The graph area is large with respect to audit items, which indicates that the PC was a large number of NG measures need improvement.

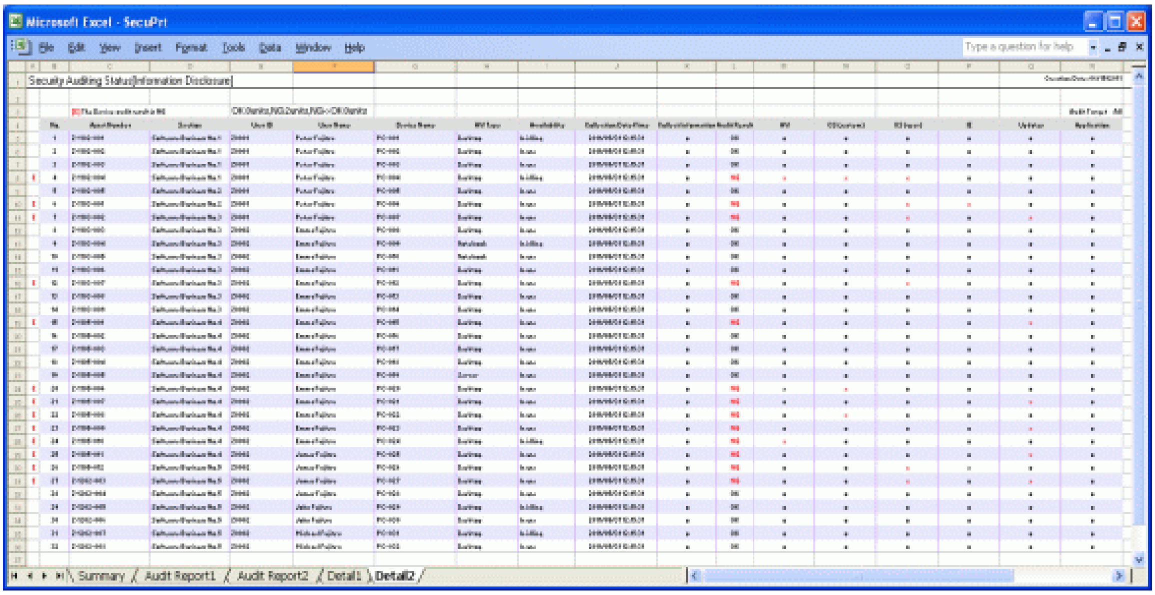
[Worst Section]

Order	Section	PC No.	OK No.	NG No.	Achievement
1	Business No.2 (200020)	5	1	4	20.0%
2	Business No.3 (200030)	6	2	4	33.3%
3	Business No.1 (200010)	8	5	3	62.5%
4	Engineering No.4 (100040)	19	17	2	89.5%
5	Business No.4 (200040)	20	18	2	90.0%

For a graph
Each audit items, and to chart in the form of PC was built a number of audit result is NG. The graph area is large with respect to audit items, which indicates that the PC was a large number of NG measures need improvement.

[View]

The following example is the detailed output of security auditing report, which displays security auditing result by device. According to the detailed output, you can find the devices to which insufficient security countermeasures are taken, and urge the system administrator to adjust security countermeasures.


Microsoft Excel - SecuPrt
File Edit View Insert Format Tools Data Window Help
Type a question for help
Summary
Audit Report1
Audit Report2
Detail1
Detail2

Security Auditing Status[Information Disclosure]

OK:0units,NG:2units,NG->OK:0units

[illegible]

2.8.3 Power Saving Countermeasure Auditing Report

It can audit the application status of power saving countermeasures according to the auditing policy decided by the user. The power saving auditing result can be used for modifying green IT countermeasures.

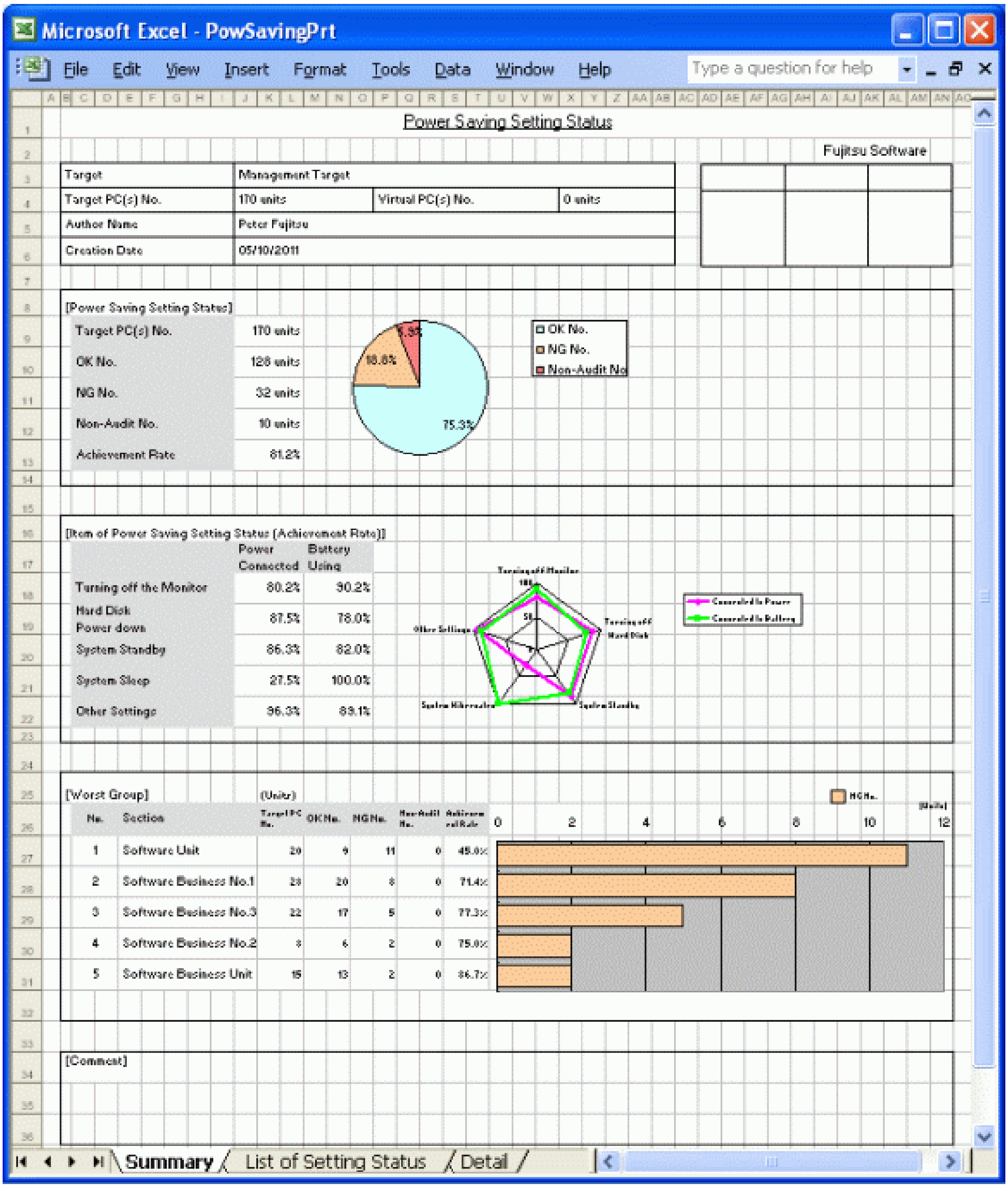
In addition, the power saving auditing result can be output in the form of report and used as attestation of correct execution of power saving countermeasures.

Example of output power saving auditing report

The power saving auditing report shall be output as power-auditing result. The power saving auditing report is an output auditing/attestation report so as to master and evaluate application status of power saving countermeasures and judge risky sections.

The following example is the output power saving auditing report.

- Power saving setup status report



Power Saving Setting Status

Fujitsu Software

Target	Management Target		
Target PC(s) No.	170 units	Virtual PC(s) No.	0 units
Author Name	Peter Fujitsu		
Creation Date	05/10/2011		

[Power Saving Setting Status]

Target PC(s) No.	170 units
OK No.	128 units
NG No.	32 units
Non-Audit No.	10 units
Achievement Rate	81.2%

[Item of Power Saving Setting Status (Achievement Rate)]

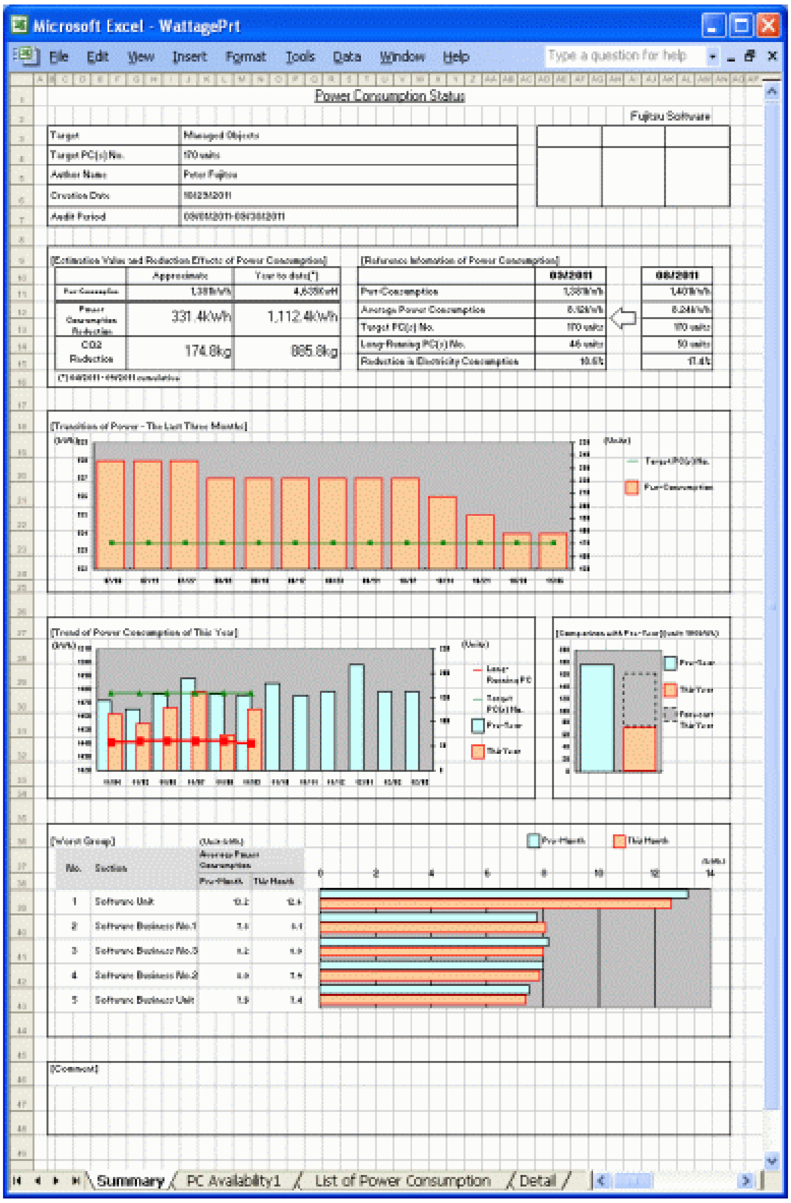
	Power Connected	Battery Using
Turning off the Monitor	80.2%	90.2%
Hard Disk Power down	87.5%	78.0%
System Standby	86.3%	82.0%
System Sleep	27.5%	100.0%
Other Settings	96.3%	89.1%

[Worst Group] (Units)

No.	Section	Target PC No.	OK No.	NG No.	Non-Audit No.	Achievement Rate
1	Software Unit	20	9	11	0	45.0%
2	Software Business No.1	28	20	8	0	71.4%
3	Software Business No.3	22	17	5	0	77.3%
4	Software Business No.2	8	6	2	0	75.0%
5	Software Business Unit	15	13	2	0	86.7%

[Comment]

- Power consumption auditing report


Microsoft Excel - WattagePrt
File Edit View Insert Format Tools Data Window Help
Type a question for help
Summary
PC Availability1
List of Power Consumption
Detail

Power Consumption Status

Fujitsu Software

Target	Managed Objects
Target PC(s) No.	170 units
Author Name	Peter Fujitsu
Creation Date	10/25/2011
Audit Period	09/01/2011-09/30/2011

[Estimation Value and Reduction Effects of Power Consumption]

	Approximate	Year to date(*)
Pwr Consumption	1,338kWh	4,638KwH
Power Consumption Reduction	331.4kWh	1,112.4kWh
CO2 Reduction	174.8kg	885.8kg

(*) 04/2011 - 09/2011 cumulative

[Reference Information of Power Consumption]

	09/2011	08/2011
Pwr Consumption	1,338kWh	1,407kWh
Average Power Consumption	8.12kWh	8.24kWh
Target PC(s) No.	170 units	170 units
Long Running PC(s) No.	46 units	50 units
Reduction in Electricity Consumption	10.6%	11.4%

[Transition of Power - The Last Three Months]

[Trend of Power Consumption of This Year]

[Comparison with Pre-Year]

[Worst Group]

(Unit:kWh)

No.	Section	Average Power Consumption	
		Pre-Month	This Month
1	Software Unit	13.2	12.6
2	Software Business No.1	7.6	8.1
3	Software Business No.3	8.2	8.0
4	Software Business No.2	8.0	7.9
5	Software Business Unit	7.5	7.4

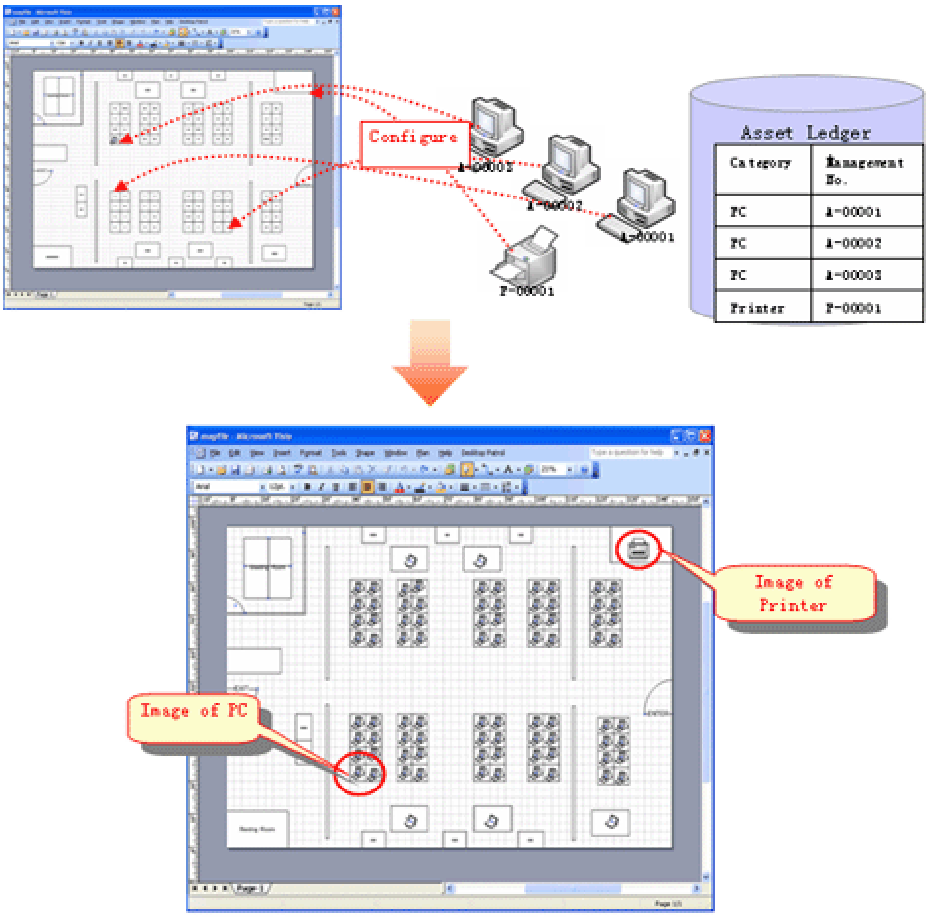
[Comment]

2.9 Location Map Function

The location map used to display the hierarchical structure can be managed after allocating the devices to the assets device account.

The system administrator can browse the Asset information of the device while he/she is visually confirming the device configuration.

Microsoft® Office Visio® is necessary for performing device management according to the location map.



Category	Management No.
PC	A-00001
PC	A-00002
PC	A-00003
Printer	P-00001

Map file

2.10 Environment Setup Function

User management

The user refers to the person who uses and manages the PCs installed with a CT; user functions will be collectively managed on the CS, including user registration and deletion, setting and change of user authority.

In addition, the registered users can be browsed via the “User List” window.

Section management

PC users usually belong to different divisions or sections, so the system administrator can manage sections through section registration or deletion.

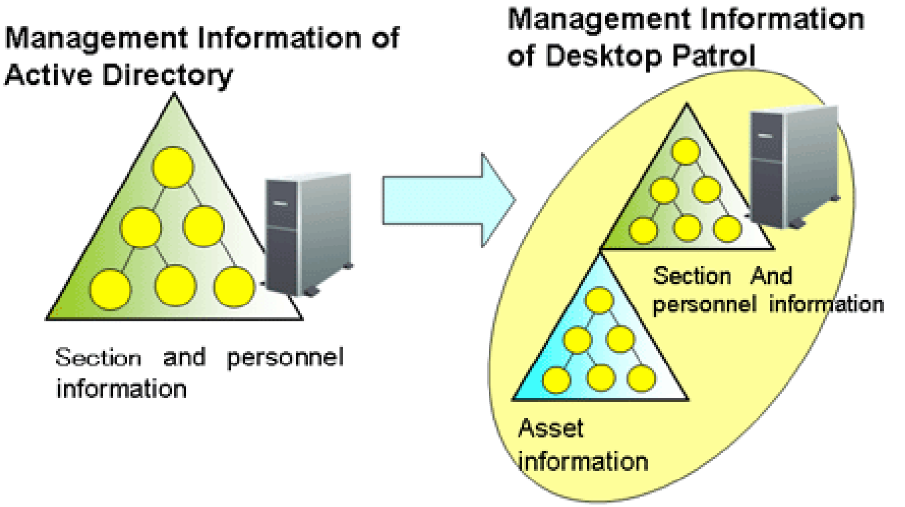
Active Directory Linkage Function

Active Directory provides the directory service to more effectively manage various resources (PC and printer, user information, etc) on the network. By linking Desktop Patrol with Active Directory, the system administrator can carry out management after the section and personnel information managed by Active Directory is related with the Asset information managed by Desktop Patrol. Also, the master data of Desktop Patrol can be generated automatically based on the section and personnel information of Active Directory. So, collective management can be realized without creating the master data of Desktop Patrol according to manual.

Further, because it is not allowed to link with the previous Active Directory, the system administrator can freely select the section to be linked with Active Directory to flexibly support users’ business.

However, linkage with Active Directory is only limited to single domain application. Active Directory can not link with Desktop Patrol in multi-domain application.

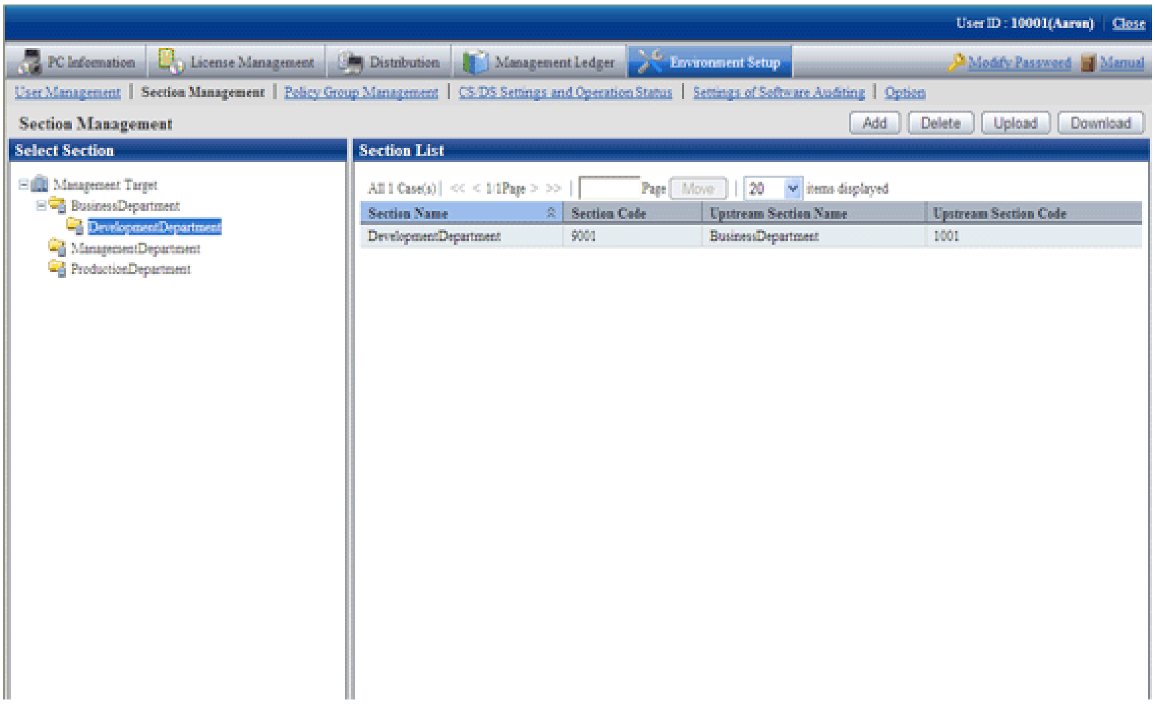
Linkage function of Active Directory is summarily shown below:


Management Information of Active Directory
Section and personnel information
Management Information of Desktop Patrol
Section And personnel information
Asset information

Add asset information to Section and personnel information of Active Directory through Desktop Patrol

The main menu of linkage with Active Directory is shown below:

The section information obtained through Active Directory will be displayed as a domain name under the section tree of the top section.


User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
User Management | Section Management | Policy Group Management | CS/DS Settings and Operation Status | Settings of Software Auditing | Option
Add
Delete
Upload
Download
All 1 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Section Management

Select Section

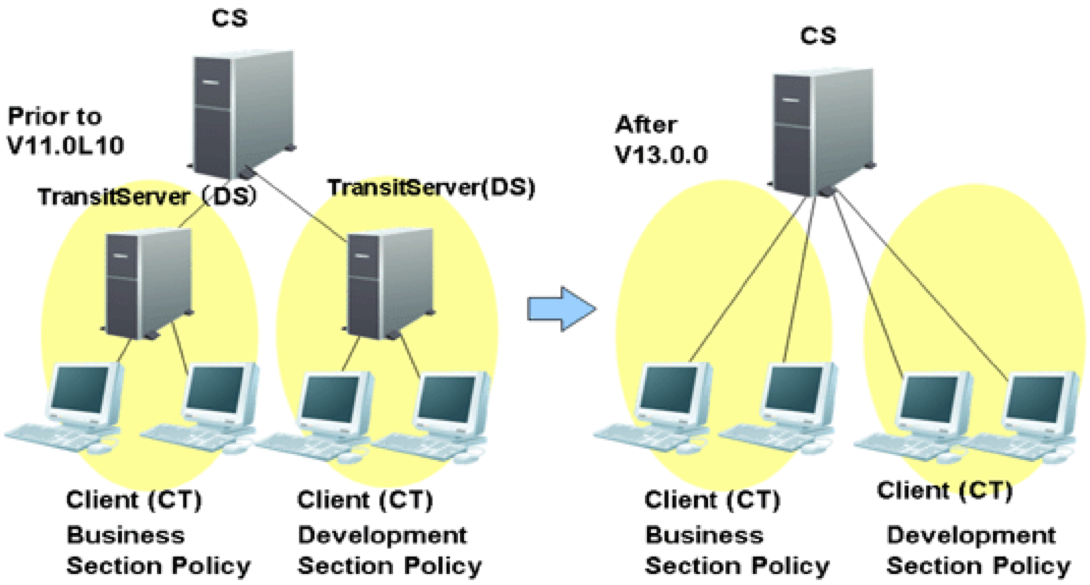
- Management Target
  - BusinessDepartment
    - DevelopmentDepartment
  - ManagementDepartment
  - ProductionDepartment

Section List

Section Name	Section Code	Upstream Section Name	Upstream Section Code
DevelopmentDepartment	9001	BusinessDepartment	1001

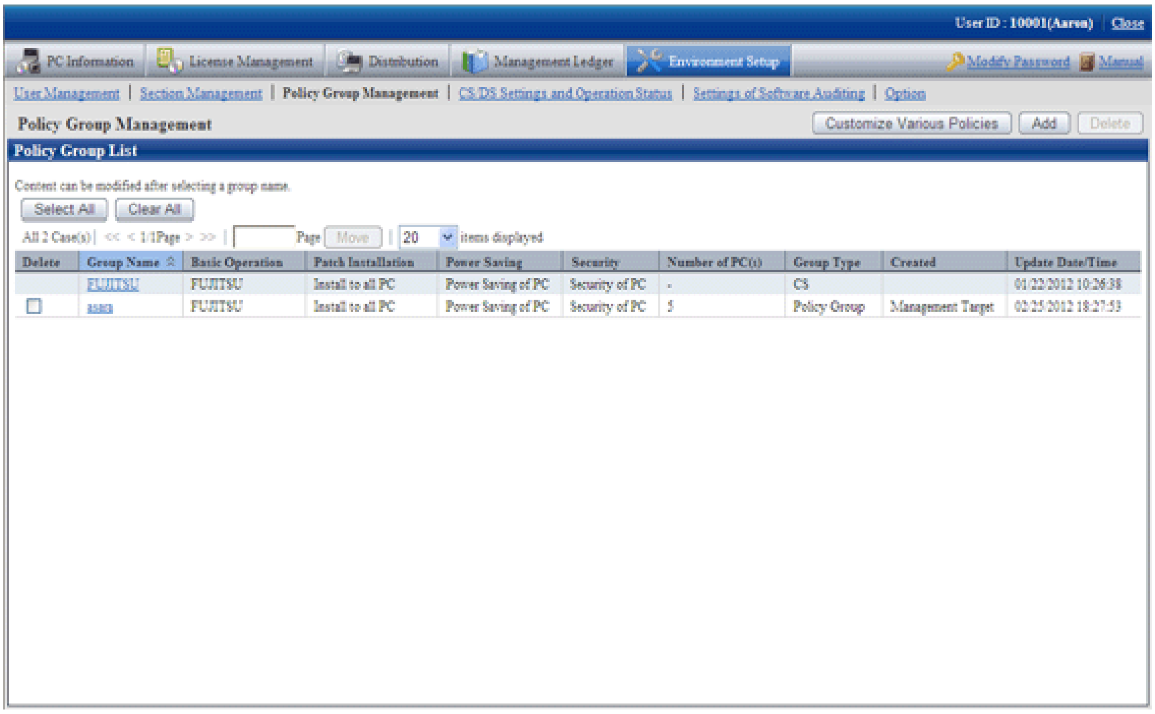
Policy Group management

Policy group management function refers to the function to set CT operation policies in each logic group, e.g. security patch application schedule and application operation, inventory collection schedule, software distribution condition, etc.



To change the previous operation policies, the system administrator can create multiple transit servers at each site. In this way, the PCs can be assigned to different logic groups instead of the transit servers whose operation policies have been changed.

Policy group shall be created in the following window of main menu.


User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
User Management | Section Management | Policy Group Management | CS DS Settings and Operation Status | Settings of Software Auditing | Option
Customize Various Policies
Add
Delete
Select All
Clear All
All 2 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Policy Group Management

Policy Group List

Content can be modified after selecting a group name.

Delete	Group Name	Basic Operation	Patch Installation	Power Saving	Security	Number of PC(s)	Group Type	Created	Update Date/Time
	FUJITSU	FUJITSU	Install to all PC	Power Saving of PC	Security of PC	-	CS		01/22/2012 10:26:38
□	asas	FUJITSU	Install to all PC	Power Saving of PC	Security of PC	5	Policy Group	Management Target	02/25/2012 18:27:53

Note

Notices for version (V11) combination

Only when the version of Systemwalker Desktop Patrol installed in the CT is higher than V13.0.0, policy group can exert it functions.

If the version of CT is V11, and the PC installed with this CT is allocated to the policy group, the PC will operate as the policies of the policy group instead of DS unit.

Settings of Software Auditing

The software dictionary shall be installed to determine the function of audited object software in the PC.

Software dictionary is used to collect the policy of Inventory information of the software used in the CT. There are two kinds of software dictionaries. Refer to “1.4.2 Software Dictionary” for details.

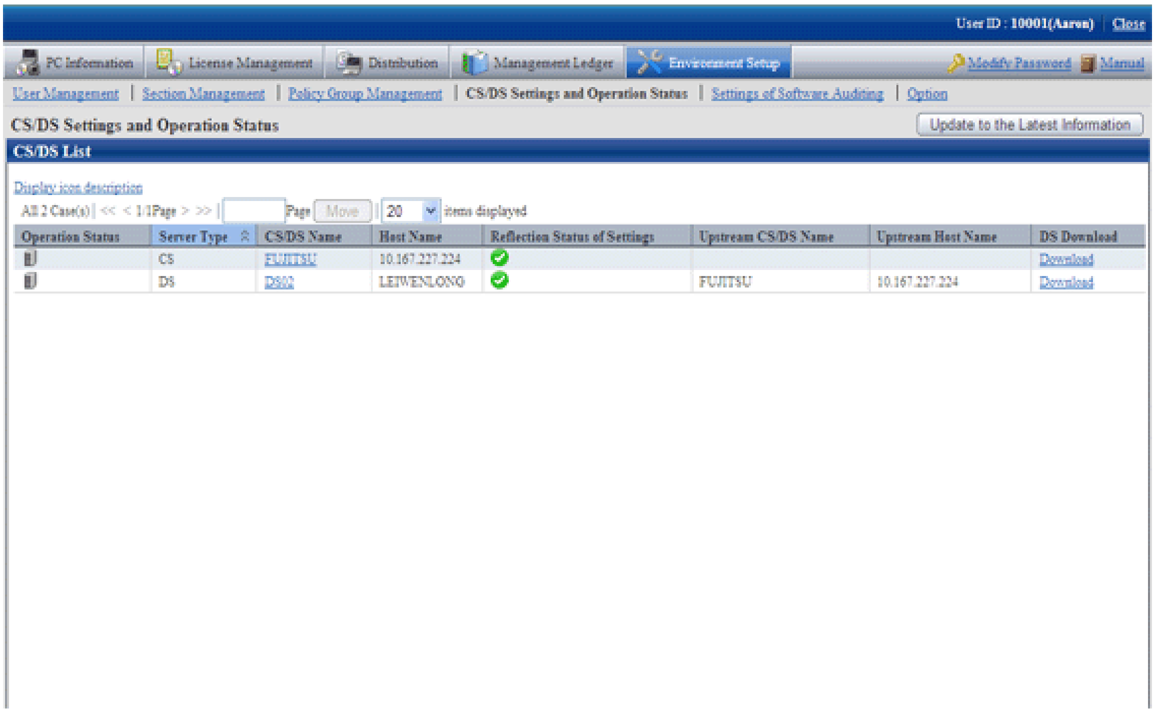
- Software dictionary defined by user

It is required to inform DS and CT of the edited policies in the root directory distributed by the software.

CS/DS Settings and Operation Status

Operating condition and communication setting function of CS or DS

Operating condition can be confirmed in the following window.



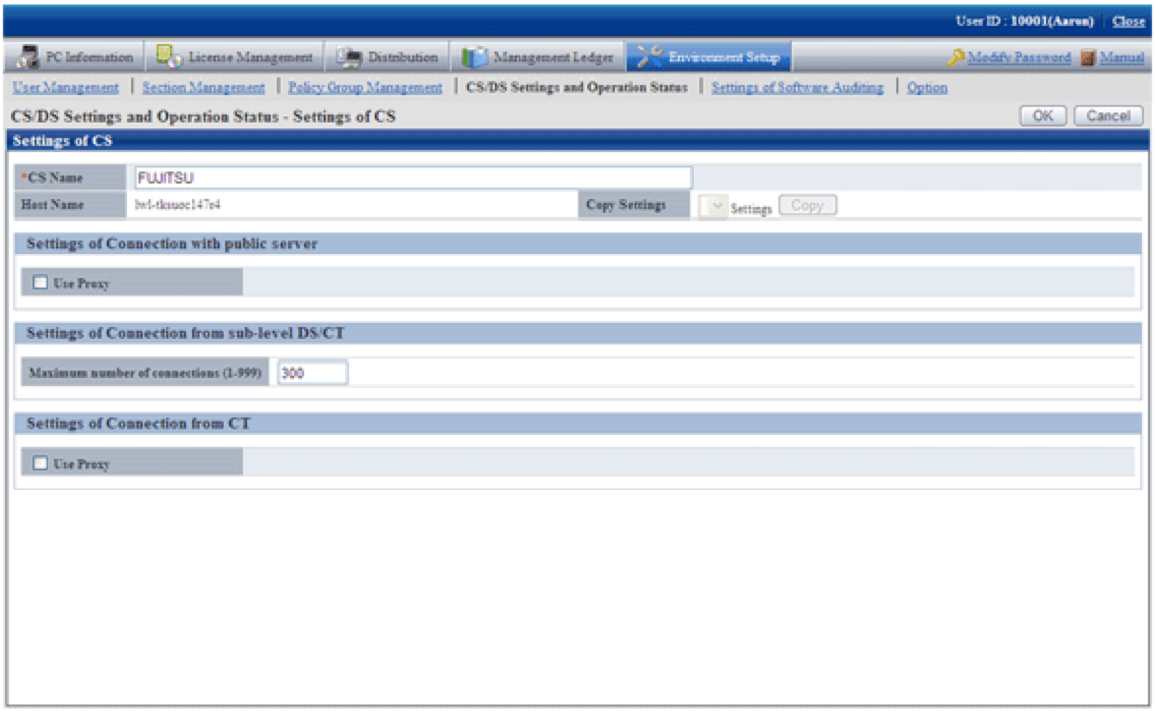
User ID : 10001(Aaron) | Close
PC Information
License Management
Distribution
Management Ledger
Environment Setup
Modify Password
Manual
User Management | Section Management | Policy Group Management | CS/DS Settings and Operation Status | Settings of Software Auditing | Option
Update to the Latest Information
Display icon description
All 2 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

CS/DS Settings and Operation Status

CS/DS List

Operation Status	Server Type	CS/DS Name	Host Name	Reflection Status of Settings	Upstream CS/DS Name	Upstream Host Name	DS Download
	CS	FUJITSU	10.167.227.224	✓			Download
	DS	DS02	LEIWENLONG	✓	FUJITSU	10.167.227.224	Download

Setup shall be carried out in the following window (taking CS as an example).



CS/DS Settings and Operation Status - Settings of CS

Settings of CS

*CS Name	FUJITSU		
Host Name	bwl-tksuoc147e4	Copy Settings	Settings

Settings of Connection with public server

□ Use Proxy

Settings of Connection from sub-level DS/CT

Maximum number of connections (1-999)	300

Settings of Connection from CT

□ Use Proxy

2.11 Remote Operation Function

Remote operation of Systemwalker Desktop Patrol supports the following functions

- Remote operation
- Two-way window transfer and receiving multiple windows
- Two-way file transfer and file system comparison
- Two-way clipboard transfer

For details of each function, refer to the Systemwalker Live Help Guide.

Remote operation

Remote Operation allows the system administrator to operate the terminal user's computer using the administrator's keyboard and mouse. The Administrator can also send a special key sequence to the terminal user's computer and logon to and logoff from it remotely.

Two-way window transfer and receiving multiple windows

The system administrator can not only receive and see the terminal user's windows and mouse movement in real time (remote operation), but also send windows from his/her device to the terminal user. This is especially useful in training. It is also possible to audit and remote operate multiple computers simultaneously. The incoming window can be scaled to fit in the current device's window.

Two-way file transfer, file system comparison

A two-way file transfer operation, similar to manipulating files with Windows Explorer can be easily done.

The function to compare the files and folders on the local and remote computers helps you to efficiently define problems of the file system.

Two-way clipboard transfer

Batch transmission of clipboard contents makes it easy to transfer a memo or obtain a bitmap of a window when a problem occurs.

2.12 Updater Function

This is the function of applying and revising the DS application and CT operation in the client system with simple operation.

The system administrator can register DS and CT correction through the updater registration command and the correction contents will be automatically applied to the DS and CT as dstribution objects. It is not necessary for DS and CT administrators to carry out the application operation because this is automatic application.

2.13 CT Prohibition Function

The user is prohibited to carry out the following operations on the PCs installed with a CT so as to make use of Systemwalker Desktop Patrol for security management.

- Stop CT services
- Uninstall CT
- Change the CT connection server

Prohibition for stopping CT service

The user is prohibited to stop CT service “ITBudgetMGR (INV)”.

Service stop prohibition means that:

- Prohibiting immediate stop of services
  - Inactivate the “Stop” button in the “Control Panel” - “Management Tools” - “Service Properties” -“Service Status” window, so that services cannot be stopped.
  - When using the "NET STOP" command of Windows standard command to stop services, the command will end abnormally, but services cannot be stopped.
- Even the service is changed to manual start, it will be restored to automatic start

  Regularly audit the "Startup Type" in properties window of "Control Panel" - "Management tools" - "Service Properties"- “Startup Type” window, when the setting has been changed to not "Automatic", restore it to the following settings by force.

  - Startup type: Automatic

This function is only available in the environment installed with a CT, and is not available in CS and DS.

Prohibition for uninstalling CT

When the user uninstalls the CT, the system will require the user to enter the password to prohibit uninstallation.

Password is required to uninstalling CT through the “Add or Delete Programs” window in the control panel menu. If the user needs to uninstall the CT, he/she should contact the administrator and confirm the password.

This function is only available in the environment installed with a CT, and is not available in CS and DS.

Prohibit changing the server connecting with CT

The user is prohibited to change the “Connected Server” in the CT environment setup window.

Grey the “Connected Server” input region in the “Switch Server” tab in the CT environment setup window to make the initial value unchangeable.

Chapter 3 Operating Environment

This chapter describes the environment required to operate Systemwalker Desktop Patrol.

3.1 Required Hardware

Hardware environment required to apply Systemwalker Desktop Patrol is described according to different components.

CS

- Required CPU specifications

  PentiumIV 2GHz or higher

- Required memory capacity (Note 1)

  Over 1024MB (excluding usage amount of OS)

- Required disk capacity (Note 1)

  737 MB + the size of registered software or more+ the size of registered patches (Note 2) + the size of CT operation status log (Note 3)

  Note 1: The required disk capacity shall meet the requirements shown below according to the above mentioned disk capacity and the size of database to be structured.

Number of PC(s)	EXE Information Collection	Software Operation Status Collection	Database Capacity
500	None	None	About 4.0GB
	None	Exist	About 4.8GB
	Exist	None	About 5.6GB
	Exist	Exist	About 6.4GB
1000	None	None	About 6.1GB
	None	Exist	About 7.7GB
	Exist	None	About 9.3GB
	Exist	Exist	About 10.8GB
3000	None	None	About 13.1GB
	None	Exist	About 17.2GB
	Exist	None	About 21.4GB
	Exist	Exist	About 25.5GB
10000	None	None	About 38.7GB
	None	Exist	About 52.3GB
	Exist	None	About 66.2GB
	Exist	Exist	About 79.8GB
20000	None	None	About 75.3GB
	None	Exist	About 102.5GB
	Exist	None	About 130.2GB
	Exist	Exist	About 157.5GB

Note 2: The size of registered patch is important when an automatic patch installation function is used. The disk capacity shall reach 7 GB or higher.

Note 3: The disk capacity must meet the following requirement for saving CT operation status log

In addition, the information of the log file will be used in the partial (operation status) information which is displayed via the CT operating status inspection command. If no CT operation status log is saved in CS, “Operation Status” will not be displayed.

Size of CT operation status log = 30 KB × User quantity × Save days

Registration or distribution of software or automatic application security patches shall be executed after confirming that there is enough usable disk capacity for processing object software. In addition, the software save directory shall be defined as other spaces except the installation disk of OS in order to prevent insufficient disk capacity due to registration or distribution of software or automatic application security patches. Further, please properly set the maximum size of software save directory.

- When updating from V11.0L10, a disk capacity 4 times of the old database (SQL Server/Oracle) is required --- this is the demand of Systemwalker for fixing the capacity and ensuring the space.
  Disk capacity can be changed by increasing or reducing “Number of PC(s)”.

DS

- Required CPU specifications

  Pentium 550MHz or higher

- Required memory capacity

  Over 464MB (excluding usage amount of OS)

- Required disk capacity

  85MB + the size of downloaded software + the size of downloaded patches or higher (Note)

  Note: The size of downloaded patch is important when an automatic patch application function is used. The disk capacity shall reach 7 GB or higher.

AC

- Required CPU specifications

  Pentium IV 2GHz or higher

- Required memory capacity (Note)

  Over 256MB (excluding usage amount of OS)

- Required disk capacity (Note)

  Over 50MB

  Note: The file system shall be “NTFS (NT File System)”.

CT

- Required CPU specifications

  Pentium 300MHz or higher

  Pentium®II 266 MHz or higher (when collecting software operation status)

- Required memory capacity

  Over 36MB (excluding usage amount of OS)

  Minimum resident memory

  - At normal time: 6.0 MB
  - When collecting software operation status: 6.0 MB
  - Non-resident memory for command mode CT.
- Required disk capacity

  11 MB or more (regular version) + size of operating disk during patch installation (Note)

  2.3 M or more (command mode CT)

  Note: Capacity of operating disk during installation of a patch will be required when an auto patch installation function is used an installation function.

  When a security patch (Hotfix) is used.

  - Installed: 20 MB or more.
  - When a service pack is installed: approximately 9 GB.

ADT

- Required CPU specifications

  Pentium IV 1GHz or higher

- Required memory capacity

  Over 512MB or higher (excluding usage amount of OS)

- Required disk capacity (Note)

  Over 5MB

  Note: The file system shall be “NTFS (NT File System)”.

Management Target PC of PC Operation Management Function

When the PC operation management function is being used, as a PC of operation management target, it shall support Intel® vPro or Intel® Centrino® Pro. Up to August 2010,

- FMV-D5330
- FMV-D5340
- FMV-D5350
- FMV-H8240
- FMV-D5370
- FMV-D5380
- FMV-D5390
- FMV-E8270
- FMV-E8380
- LIFEBOOK E780/A

Printer (used for inventory verification/asset information conformation/report output)

The printer can be used when setting via AC and printing the asset information report.

The used printer shall have the following performances:

- Capable of printing A4 paper
- Capable of printing A4 paper in black and white
- Resolution exceeds 600 dpi

A color printer is recommended to print the asset information report.

3.2 Software

Software environment required to apply Systemwalker Desktop Patrol is described according to different components.

3.2.1 Operating OS

The operating systems in which the respective components can run are listed below:

Note

Systemwalker Desktop Patrol English version described in this manual can be installed in the OS of following languages.

Japanese OS

English OS

Chinese OS

It can not be installed in the OS or Language Packs except the languages mentioned above.

CS

- Microsoft® Windows Server® 2003, Standard Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack no /2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack no /2
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack no /2
- Microsoft® Windows Server® 2008 Foundation Service Pack no/2
- Microsoft® Windows Server® 2008 Standard Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ Service Pack no /1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Service Pack no /1/2(Note)
- Microsoft® Windows Server® 2008 R2 Foundation
- Microsoft® Windows Server® 2008 R2 Standard Service Pack no/1(Note)
- Microsoft® Windows Server® 2008 R2 Enterprise Service Pack no/1(Note)

Note) Server Core is unusable.

DS

- Microsoft® Windows Server® 2003, Standard Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2008 Foundation Service Pack no/2
- Microsoft® Windows Server® 2008 Standard Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ without Service Pack/1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ without Service Pack/1/2(Note)
- Microsoft® Windows Server® 2008 R2 Foundation
- Microsoft® Windows Server® 2008 R2 Standard Service Pack no/1 (Note)
- Microsoft® Windows Server® 2008 R2 Enterprise Service Pack no/1(Note)

Note) Server Core is unusable.

AC

- Microsoft® Windows® XP Professional Service Pack 3
- Microsoft® Windows® XP Home Edition Service Pack 3
- Microsoft® Windows Vista® Ultimate Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise Service Pack no/1/2
- Microsoft® Windows Vista® Business Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic Service Pack no/1/2
- Microsoft® Windows Vista® Ultimate x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Business x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic x64 Edition Service Pack no/1/2
- Windows® 7 Enterprise Service Pack no/1
- Windows® 7 Ultimate Service Pack no/1
- Windows® 7 Professional Service Pack no/1
- Windows® 7 Home Premium Service Pack no/1

CT

- Microsoft® Windows Server® 2003, Standard Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2008 Foundation Service Pack no/2
- Microsoft® Windows Server® 2008 Standard Service Pack no/1/2 (Note)
- Microsoft® Windows Server® 2008 Enterprise Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 R2 Foundation
- Microsoft® Windows Server® 2008 R2 Standard Service Pack no/1(Note)
- Microsoft® Windows Server® 2008 R2 Enterprise Service Pack no/1(Note)
- Microsoft® Windows® XP Professional Service Pack no/1/1a/2/3
- Microsoft® Windows® XP Home Edition Service Pack no/1/1a/2/3
- Microsoft® Windows Vista® Ultimate Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise Service Pack no/1/2
- Microsoft® Windows Vista® Business Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic Service Pack no/1/2
- Microsoft® Windows Vista® Ultimate x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Business x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic x64 Edition Service Pack no/1/2
- Windows® 7 Enterprise Service Pack no/1
- Windows® 7 Ultimate Service Pack no/1
- Windows® 7 Professional Service Pack no/1
- Windows® 7 Home Premium Service Pack no/1

Note) Server Core is unusable.

Note

- In Windows® XP, when selecting “Keep the computer up-to-date often” checkbox (it is “Automatic (Recommended)” in Windows® XP SP2) in the setting of automatic updates window, security patches cannot be installed automatically.

- When restarting Windows® XP SP2 (if applied), “Automatic Updates” will be started in “Please protect your computer”, and please select “Not Enable Now”.
- When selecting “Immediately open automatic updates to protect computer”, please select the checkboxes except “Automatic (Recommended)” from the “Automatic Updates” of system properties menu.

ADT

- Microsoft® Windows Server® 2003, Standard Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack no/1/2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 1/2
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack no/2
- Microsoft® Windows Server® 2008 Foundation Service Pack no/2
- Microsoft® Windows Server® 2008 Standard Service Pack no/1/2 (Note)
- Microsoft® Windows Server® 2008 Enterprise Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Service Pack no/1/2(Note)
- Microsoft® Windows Server® 2008 R2 Foundation
- Microsoft® Windows Server® 2008 R2 Standard(Note)
- Microsoft® Windows Server® 2008 R2 Enterprise (Note)
- Microsoft® Windows® XP Professional Service Pack no/1/1a/2/3
- Microsoft® Windows® XP Home Edition Service Pack no/1/1a/2/3
- Microsoft® Windows Vista® Ultimate Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise Service Pack no/1/2
- Microsoft® Windows Vista® Business Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic Service Pack no/1/2
- Microsoft® Windows Vista® Ultimate x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Enterprise x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Business x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Premium x64 Edition Service Pack no/1/2
- Microsoft® Windows Vista® Home Basic x64 Edition Service Pack no/1/2
- Windows® 7 Enterprise Service Pack no/1
- Windows® 7 Ultimate Service Pack no/1
- Windows® 7 Professional Service Pack no/1
- Windows® 7 Home Premium Service Pack no/1

Note) Server Core is unusable.

3.2.2 Required Software

The following software is required to implement the functions of Systemwalker Desktop Patrol.

Required software

[CS]

The server installed with CS requires the following software.

- **Web server**

  Any one of the following products is required.

  - Internet Information Services 6.0
  - Internet Information Services 7.0
  - Internet Information Services 7.5

The following software is required to edit CSV files.

- **Editor software for editing CSV files**

  Microsoft® Windows NOTEPAD, WORDPAD or Microsoft® Excel

[AC]

The PC installed with AC requires the following software.

- **Microsoft® Excel**

  Any one of the following products is required.

  - Microsoft® Office Standard Edition 2003(Note 1)
  - Microsoft® Office Professional Edition 2003(Note 1)
  - Microsoft® Office Ultimate 2007(Note 2)
  - Microsoft® Office Enterprise 2007(Note 2)
  - Microsoft® Office Standard 2007(Note 2)
  - Microsoft® Office Professional 2007(Note 2)
  - Microsoft® Office Professional Plus 2007 (Note 2)
  - Microsoft® Office Personal 2007(Note 2)
  - Microsoft® Office Professional Plus 2010 (Note 3)
  - Microsoft® Office Standard 2010(Note 3)
  - Microsoft® Office Professional 2010(Note 3)
  - Microsoft® Office Home and Business 2010(Note 3)
  - Microsoft® Office Personal 2010(Note 3)
  - Microsoft® Office Excel 2003
  - Microsoft® Office Excel 2007

  Note 1: Microsoft® Office Excel 2003 is necessary.

Note 2: Microsoft® Office Excel 2007 is necessary.

Note 3: Microsoft® Office Excel 2010 is necessary.

The following software is required for apply location map.

- **Microsoft® Visio**

  Any one of the following products is required.

  - Microsoft® Office Visio® Standard 2003
  - Microsoft® Office Visio® Professional 2003
  - Microsoft® Office Visio® Standard 2007
  - Microsoft® Office Visio® Professional 2007
  - Microsoft® Office Visio® Standard 2010
  - Microsoft® Office Visio® Professional 2010
  - Microsoft® Office Visio® Premium 2010

Note

Microsoft® Excel(x64 Edition) or Microsoft® Visio(x64 Edition) is not supported.

[CT]

The PC installed with CT does not require any software.

[ADT]

The PC installed with ADT does not require any software.

[Web Browser]

The PC using Web browser requires one of the following products.

- Microsoft® Internet Explorer 6
- Windows® Internet Explorer® 7
- Windows® Internet Explorer® 8
- Windows® Internet Explorer® 9

Relevant software

Software that cannot be used in the virtual OS

[CS/DS]

- VMware Infrasructure 3
- VMware vSphere 4
- Microsoft Hyper-V™

[CT/AC/ADT]

- VMware Infrasructure 3
- VMware vSphere 4
- VMware View 3
- VMware View 4
- Citrix XenDesktop 4.0
- Citrix XenDesktop 5.0
- Microsoft Hyper-V™

E-mail software

It is necessary for the user of system account or section management account to receive E-mails according to warning notifications.

Microsoft® Outlook Express

Microsoft® Outlook etc.

3.2.3 Database

Systemwalker Desktop Patrol uses Symfoware Server as a database and automatically installs its functions during the installation of packages.

- If CT is installed
  - Symfoware Server server function
  - Symfoware Server CT function
- If AC is installed
  - Symfoware Server CT function

In addition, Systemwalker Desktop Patrol also can use Symfoware Server that bundle with Systemwalker Desktop Keeper V14.2.0 as database.

If the server and CT function of the above Symfoware Server products are installed during installation of packages, the used Symfoware Server will not be installed any more.

When the functions are not installed, and the version of installed Symfoware Server product is identical with that of the used Symfoware Server, the functions will be automatically installed.

Failure to automatic installation will cause installation error, so it is required to install the server function of Symfoware Server and Symfoware Server CT function of the same version to installed Symfoware Server products.

Note

- It is impossible to install CS in the environment where only Symfoware Server function is installed.
  Please install Symfoware Server function and Symfoware Server client function in advance.
  Additionally, the used Symfoware Server can only be used after uninstalling the client function of Symfoware Server.
  Please determine whether to install or uninstall Symfoware Server according to the environment.

3.2.4 Products That Cannot Coexist

Products that cannot coexist with CS

When installing CS, the following products cannot coexist.

- Systemwalker Desktop Keeper V13.0.0/V13.2.0 (Note 1)
- Systemwalker Desktop Keeper V14.2.0(Note 2)
- Systemwalker Centric Manager (earlier than V12.0) (Note 3)
- Systemwalker Centric Manager V13.0.0 ~ V13.3.1 Application Management Server (Note 1)
- Systemwalker Centric Manager(x86 Edition) V13.4.0 Application Management Server (Note 1)
- Systemwalker Centric Manager(x64 Edition) V13.4.0 ~ V13.5.0 Application Management Server
- Symfoware Server Enterprise Edition (all versions)
- SymfoWARE Programmer's Kit(all versions)
- Products bundled with Symfoware Server Enterprise Edition (x64 Edition)(Note 1)

Note 1: the conditions that allow coexistence are as follows:

- Coexistence is allowed when it is installed ahead of Systemwalker Desktop Patrol.

Note 2: the conditions that allow coexistence are as follows:

- Coexistence is allowed when it is installed ahead of Systemwalker Desktop Patrol.
- Coexistence is allowed when Symfoware Server that bundle with Systemwalker Desktop Keeper is installed.

Note 3: the conditions that allow coexistence are as follows:

- Coexistence is allowed when “Help Desktop CT (ODBC)” is not installed in the section server or service server of Systemwalker Centric Manager (earlier than V12.0).
- Coexistence is allowed when either of “Help Desktop CT (ODBC)”or “Help Desktop Database” is not installed in the help desktop server of Systemwalker Centric Manager (earlier than V12.0).

Please confirm the installation information of Systemwalker Centric Manager according to the “Product Information Display Command” of Systemwalker Centric Manager. Refer to “Systemwalker Centric Manager Guidebook” for how to apply “Product Information Display Command”.

Products that cannot coexist with AC

When installing AC, the following PCs cannot coexist.

- PC installed with [SymfoWARE Server] with version earlier than V5.0L21
- PC only installed with [Symfoware Server function]
- PC installed with [SymfoWARE Programmer's Kit] with version earlier than V5.0
- PC installed with [Symfoware Server Client function] with version earlier than V5.0

If the above software has been installed, please restore the PC to the previous state with the above software uninstalled or uninstall the above software according to the requirement.

3.3 About Versions That Can Coexist

The section gives a description about different versions according to the components of Systemwalker Desktop Patrol.

The used CS and DS shall have the same version (they can not be used in case the versions are different).

It is unable to connect with the DTP of Japanese version

Compatible status when the version of CS and DS is different from that of CT is shown in the following table:

		“ Systemwalker Desktop Patrol CT ”			
		V14.2.0	V13.2.0	V13.0.0	V11.0L10
Upstream Server(Note)	V14.2.0	○	△	△	△
	V13.2.0	×	○	△	△
	V13.0.0	×	×	○	△
	V11.0L10	×	×	×	○

Note: Upstream Server is a general designation of CS and DS.

○: Connectable (Versions can coexist)

△: Connectable (only the lower version functions can be used)

×: Unconnectable (Versions cannot coexist)

Chapter 4 Link with Other Products

Combining with other products allows for a more effective operation of assets management..

4.1 List of Linkage Products

The products which can be linked with Systemwalker Desktop Patrol are shown as follows:

Type	Product Name	Function Profile
In-house product	Systemwalker Desktop Keeper V13/ V14g	- Collect and display the policy setup status of Systemwalker Desktop Keeper via the CT. - Display the usage status of Systemwalker Desktop Keeper in Status Window when its version is V14.2.0.
	Systemwalker Centric Manager V13	- It can import the Inventory information accumulated in the database of usage management server Systemwalker Centric Manager into the database of Systemwalker Desktop Patrol. - It can display the event log of Systemwalker Desktop Patrol in the auditing window of Systemwalker Centric Manager and provide auditing service via Systemwalker Centric Manager.
Products from other companies	The arbitrary products of the other company	The Inventory information (only device information) of the products from other companies can be imported into the assets management ledger and manage the device information collected via the products of other companies in Systemwalker Desktop Patrol.
CSV (text file) link	CSV Data Link Interface	It can be used as a standard interface to perform the link in CSV format with the non-above mentioned products. The Inventory information files in CSV format exported through the link object products can be edited as the files in CSV format used for link of company products and imported into the database of Systemwalker Desktop Patrol.

4.2 Event Linkage

Event linkage refers to displaying and auditing the event logs of Systemwalker Desktop Patrol in the auditing window of Systemwalker Centric Manager. Systemwalker Desktop Patrol can perform the link of the following events.

- Event linkage via alarm and notification
- Event linkage via event log output

The version of Systemwalker Centric Manager to perform event link and the auditing window to display the alarm function of Systemwalker Desktop Patrol are shown below:

Product Name	Auditing Window
Systemwalker CentricMGR SE/EE V10.0L20 or later	Systemwalker control console

Event linkage via alarm and notification

The alarm messages, e.g. license violation, unapplied security patch, can be displayed in the auditing window of Systemwalker Centric Manager by means of the alarm and notification function of Systemwalker Desktop Patrol.

Event linkage via event log output

The events about CS or DS can be displayed in the auditing window of Systemwalker Centric Manager by outputting the events occurring in Systemwalker Desktop Patrol to the event log.

The following events shall be output to the event log.

Type	Description
Message	- Start or stop service - - Download security patches from the public sites of Microsoft.
Warning	When an automatic recovery or minor faults have no impact on continuous operation
Error	When abnormal conditions which have an impact on utilization appear in CS or DS

4.3 Collection of Inventory Information

It is possible to collect Inventory information in Systemwalker Desktop Patrol by means of other products functions.

Inventory information can be collected in the following manners:

- To collect Inventory information, using function of Systemwalker Centric Manager
- To collect Inventory information, linking with CSV (text file)

Inventory information that can be collected is as shown below:

	Collection Method		
Collect Information	Centric Manager Linkage		CSV Linkage
	Windows	UNIX	
Hardware information	○	○	○
Software information - file search	○	×	○
Software information- registry search (searched by program name)	○	×	○
Software information - registry search(searched by any key word and value)	×	×	○
User information	○ (Note)	○ (Note)	○
Software operation status	×	×	○
Registry information	×	×	×
EXE information	×	×	×

○:can be collected ×: cannot be collected

Note: The inventory collection of auditing function of installation-free proxy is uncollectable.

Collecting inventory information using function of Systemwalker Centric Manager

The collected Inventory information can be imported into Systemwalker Desktop Patrol via Systemwalker Centric Manager. Therefore, even the Inventory information about the OS unsupported by Systemwalker Desktop Patrol, e.g. UNIX, can also become the assets management target of Systemwalker Desktop Patrol.

Please refer to “Operation Guide: for Administrators” for how to set..

The version of Systemwalker Centric Manager which can perform Inventory collection link is shown as follows:

Product Name	Note
Systemwalker Centric Manager V13.0.0 above	It is possible to be linked with operation management server or section management server (Note)

Note: It can only be linked with the operation management server when collecting the Inventory of auditing function of installation-free proxy. It can coexist with the operation management server if it coexists with Centric Manager. If it does not coexist with Centric Manager, Inventory information can be imported from the operation management server.

Collecting inventory information, linking with CSV (text file)

The Inventory information entered in CSV format prescribed in Systemwalker Desktop Patrol can be captured.

Please refer to “Operation Guide: for Administrators” for record format and usage instructions.

4.4 Security Auditing

The security information set in other products can be collected as Inventory information by Systemwalker Desktop Patrol and is audited as security information.

Versions of the product for security auditing is shown below:

- Systemwalker Desktop Keeper V13.0.0 above

Auditing security settings information of Systemwalker Desktop Keeper

The security settings status of Systemwalker Desktop Keeper can be audited in the client.

4.5 Creation of Assets Management Ledger of Other Products

The Inventory information (only device information) of products from other companies can be imported to the assets management ledger and the device information collected by products from other companies can be managed through Systemwalker Desktop Patrol.

Appendix A Term Table

Terms that are changed since V13.0.0

Term that are changed since V13.0.0 are as follows:

Terms in V11.0L10	Terms in V13.0.0 or later	Note
Web Tools	Desktop Patrol Main Menu Desktop Patrol Download Menu	
Name of Application	Name of Program	
Add or Remove Applications	Add or Remove Programs	
Error PC	PC without configuration	
Enterprise Policy	Software Dictionary	
System Administrators Privilege Administrators Privilege	System account or Section management account	When all operations of "Systemwalker Desktop Patrol" are performed, system account is used. When the operations of section and affiliated section are performed, section management account is used.
Client Privilege	User account	
Employee	User	
Employee ID	User ID	
Employee master Employee password master E-mail Information master Affiliated master	User Management Information	
Building master	Building Management Information	
Division	Section	
Master	Master Management Information	
Machine	PC	
Metering Information	Software Operation Status	

Terms that are changed since V13.2.0

Terms that are changed since V13.2.0 are as follows:

Terms in V13.0.0 or earlier	Terms in V13.2.0	Note
Manage License	License Definition	
License Purchase	Current License Management	

Terms that are changed in V14.2.0

Terms that are changed in V14.2.0 are as follows:

Terms in V13.2.0 or earlier	Terms in V14.2.0	Note
Assets Management	PC Information	
Security Management	-	
Setup Management	Environment Setup	
Security Management	PC Information - Security Information	
Installation of Software	Software Audit	
Installation of Anti-Virus Software	Software Audit	
Application of Security Patch	Software Audit	
Setup Management - DS Download	Environment Setup- CS/DS Settings and Operation Status	
Setup Management - Policy Group Management/Client Policy	Setting Working Group of CT	
MC - Enterprise Policy	Environment Setup - Settings of Software Auditing	
MC - Software/Patch	Software Distribution	
MC - Server Policy/Property	Environment Setup - CS/DS Settings/ Option	
Enterprise Policy	Software Dictionary	
Enterprise	Support Center Definition	
Local	User Definition	
Anti-Virus Software	Anti-Virus Software	
LicenseSoftware	Software	
Automatic Patch Application	Security Patch	
Prohibition Application	Prohibition Software	
Creating Date of Software Dictionary	Creating Date by Support Center	
Updating Date of Software Dictionary	Date of Software Dictionary Update	
Application Name/Name	Name	
License Group	Software Group	
License Code	Software Code	
Version	Note	
License Relation Definition/ Judgment Formula	Combination Condition	
Distribution Status	Distribution Preparation Status	
Regular Name	CS/DS Name	
Contents	Software Distribution	
Server Name	CS/DS Name	
Contents Distribution	Software Distribution	
Use Prohibition Application	Prohibition Software	
Download	CSV Export	
Only Departmen/All Departments	Low-level Included	

Terms in V13.2.0 or earlier	Terms in V14.2.0	Note
Contents Download	Software Download	
PC Model Name	Model Name	
PC Manufacturer	Manufacturer Name	
PC Serial Number	Serial Number	

Glossary

AC

It is the abbreviation of Systemwalker Desktop Patrol Asset Console.

After starting AC, the system administrator and section administrator can output reports, and register/modify asset information.

ADT

It is the abbreviation of Systemwalker Desktop Patrol Auto Detection Terminal

ADT is configured on each network segment. ADT automatically detects device that is connecting to the network on the same network segment. Then the ADT sends the detected device information to the CS.

Agent Mode

It is the mode of automatically collecting latest information and building the IT assets database when the CT is installed on PC.

Application Check

It is selected when the software dictionary code is collected as the object for Inventory collection. It can become the Inventory collection object through application check in the main menu.

Asset Information

It is the information of devices and contracts that are managed with ledger.

Auditing Pointer

It defines evaluation criteria for security auditing. The security policy should ensure that no problem will occur.

Auditing Result Saving Period

It indicates the period when the auditing results can be saved. To ensure that the new auditing result can be checked and compared with the earlier result, set this parameter to 2 months, 6 months, or 1 year.

Auto-processing

The administrator can set that the power saving and security items are processed automatically.

Settings can be modified automatically when power saving and security settings violate the requirement.

Auditing Schedule

It defines the time to perform security auditing. The certain date and start time must be set in every month.

Batch Processing

It modifies settings automatically when power saving and security settings violate the requirement based GUI operations of PC users.

Batch Network Check

It detects the ICMP devices connecting to the network automatically by using the CS server around the network segment where ADT is not installed.

Building Management Information

It records the summary of work area (office) information, which is necessary for management.

Construction of Master Data

It relates to the registration of Master management information such as Inventory and license information that is viewed by user and section unit respectively.

CS

It is the abbreviation of Systemwalker Desktop Patrol Corporate Server (CS).

CS Operation Log

It records operations for the CS such as modification, registration, deletion, login/logout in logs through the following menus:

Main menu

Download menu

Client Policy

It defines the CT operation policy.

Combination Condition

One dictionary code is registered for a group of software according to software definition. Users can manage license details based on the group.

Collection Timing

Specify the timing of Inventory collection. The options are specified timing, power-on, and logon. The information collected at this time will be different from the previous collection of information from CT. When collecting the latest Inventory information, select Start > Systemwalker Desktop Patrol CT > Inventory Collection or use the main menu to re-collect as the administrator.

Collection Unit

The time unit of the CT Inventory collection can be chosen among daily, weekly, or not collect.

Contract Information

It indicates the contract-related information about devices that are managed with ledger, such as contract class company, and date.

Command Mode CT

It is a function of exporting Inventory information on the PC to a file by executing a command. It is used for Inventory collection on a PC disconnected from the network or on networks that are slow.

CT

It is the abbreviation of Systemwalker Desktop Patrol Client Terminal (CT).

CT Operation Status Log

CT operation status will be saved in Systemwalker Desktop Patrol CS as a log. According the CT operation status log, the administrator can check the following operation status of Systemwalker Desktop Patrol CT:

- Operation record of Systemwalker Desktop Patrol
  - Start/Stop of Systemwalker Desktop Patrol service
  - Policy reception
  - Inventory collection
  - Patch installation
  - Software distribution
  - Application updater
- Operation record of Windows
  - Windows logon/logoff
  - Windows suspend/suspend recovery

- Battery application/AC application
- LAN connection enabled/disabled

Desktop Keeper Information

On the PC which has Systemwalker Desktop Keeper installed, the installation and setting status of this security policy software can be collected as security information.

Device

It indicates PCs and devices that are managed using the management ledger function of Systemwalker Desktop Patrol.

Device

It indicates devices in which CT cannot be installed such as printers and HUBs and furniture such as desks and chairs.

Device Information

It contains model name, manufacturer, and asset classification of devices that are managed with the ledger.

Diagnosis result window of operation settings

It displays the diagnosis results of power saving and security settings.

PC users check the diagnosis results and modify related settings on this GUI.

Dictionary Code

It allocates codes according to software details such as the version, level, and edition and software summary.

It is essential for user definition.

DS

It is the abbreviation of Systemwalker Desktop Patrol Domain Server (DS).

DS Unit

It is the CT configured under the same upstream server as a management unit. The client policy is used based on the management unit.

DS is used to distribute physical load such as hardware performance and bandwidth. The client that is configured as DS is a DS unit.

EXE Information

It refers to the properties information about executable files (file with extension name .exe) on the PC. Through inventory collection function, the properties information of executable files on "Systemwalker Desktop Patrol CT" can be viewed.

Environment Setup

It is the function of performing operational configuration of Systemwalker Desktop Patrol.

Environment setup is required when user management, section management, policy group setting, and Systemwalker Desktop Keeper use the structure information between each other.

File Distribution Function

It distributes files to several CTs according to the distribution settings on CS. The distribution result can be checked on CS.

Hardware Information

It is a kind of Inventory information. The information includes physical memory capacity and hard disk capacity.

ICMP

It is the abbreviation of Internet Control Message Protocol ICMP is a protocol that transfers messages about status of PCs and network connected through TCP/IP.

Inventory Collection Function

It is the function of sending Inventory information collected from CT to CS or DS.

Inventory Information

It is required when managing the actual PC status. The information includes CPU and hard disk capacity, installed software, version management of virus pattern file of anti-virus software, and patch installation.

License Management Function

Administrator manages the license number according to each license dispensed through **License management** > **License Giving menu** from the main menu. Only the administrator has such authority.

Using license management, illegal and unused licenses can be identified.

Live Help Client

It is installed on user PCs that require help and servers that require remote operation. When the message “How to do with GUI messages?” or “How to operate application programs?” occurs, users can use Live Help Expert to get remote help.

Live Help Expert

It is a component of Live Help Client. With this software, you can directly connect to the PC of the client user and provide remote assistance.

Main Menu

It provides access to Desktop Patrol service to view Inventory information that is collected from each PC, manage licenses, and perform security auditing.

Management Target

The system administrator can view and set all sections that contain unconfigured items. A section administrator can view and set the home section, while a common user can only view the home section.

The sections that users at each level can view and set are defined as management targets.

Users can log in to the main menu and access the section tree to view and set sections.

Network Segment-based Check

It sets ADT on each network segment. This helps user to automatically detect devices connecting to the network on the same network segment and send the detection result to CS.

Operation Log Collection

It saves user operations in logs and collects the log files on the PC where the CT is installed.

PC Information

Collects Inventory and user information from each PC, registers the collected information to database, and provides centralized management on the CS.

It can manage hardware, software installation, and software operation during use.

Policy

It indicates the assembled functions of Systemwalker Desktop Patrol (DTP) according to certain rules.

The policy contains information about patch installation schedule and action, Inventory collection schedule, and file distribution schedule intended for DS and CT.

Policy Group

It creates a logic group and applies policies to the group as a unit. To distinguish policies, the administrator creates a policy group and registers PCs where clients are installed with the group without being limited by the physical network.

The administrator can manage policies of any PCs for upstream servers.

The operation of the policy group unit can be set in the main menu.

Program Information

It collects information displayed in the **Add or Remove Programs** menu.

Processing Window

It is the page displayed when you click the status link on the main menu.

On the processing GUI, users can:

- Message Sending.
- Inventory Collection.
- Inventory Delete.
- Security Patch Installation.
- Security Settings Modification.
- Power Saving Settings Modification.

Rectification Period

This indicates the period from knowing to acknowledging the current security status. During this period, security auditing report is generated and security policy of the OK level is implemented

Remote Operation Function

It indicates the Systemwalker Live Help function bound with Systemwalker Desktop Patrol. This function allows users to operate PCs remotely including image receiving, file transfer, file comparison, and clipboard transfer.

Registry Information

It indicates information in the OS registry. Users can check the information when configuring registry information in the main menu.

SNMP

It is the abbreviation of Simple Network Management Protocol. SNMP monitors servers and network devices connected through TCP/IP around the network.

Status Window

It displays the operation condition of Systemwalker Desktop Patrol in a list in the main menu.

User can process according to status displayed in this window.

Status Icon

It displays the bar chart of the status window at the top-left corner, indicating the percentage of the problem PCs.

Section Management Account

It allows logon users to set and view information under their section and the section directory.

Section Management Information

It is the information about the section. It is the necessary information for construction of management information.

Security Auditing

It audits the PCs where correct patches and anti-virus software are installed. This enhances the capability in defending security weakness and virus threats.

Security Auditing Function

It manages security auditing information related to PC security policy.

Security Auditing Report

It indicates the auditing and certificate report for knowing and judging sections and PCs with potential risks. The security policy covers Systemwalker Desktop Patrol, Systemwalker Desktop Keeper.

Software Operation Status

It indicates whether software is operating properly, that is, whether files are operating. Users can obtain such information from the main menu, and view section information from the software operation status.

Software Dictionary

The software dictionary is distributed by Systemwalker randomly.

Software Information

It is a kind of Inventory information. The information includes the name and version of the software that is found by the search dictionary or installed on the PC. The software information can be determined according to the file name, file size, and storage path contained in Windows registry information.

Software License Definition

When managing a License, the search conditions for determining whether the software has been installed must been defined.

In Systemwalker Desktop Patrol, the definition of these search conditions is collectively called software dictionary.

Software Distribution Function

It manages software that is distributed to CT. The management includes registration, update, deletion, and incremental distribution.

Software Distribution

It is registered to CS or DS through the main menu. In Systemwalker Desktop Patrol, registration can be performed from file to software.

Software Group for Distribution

It is created during software distribution and used when software is distinguished by category.

System Account

It is an account that can access set all main menu items on the main menu.

System Security

It can be viewed as the security information of the system. It collects settings status of BIOS and logon status of system from each PC.

Systemwalker Desktop Keeper

It focuses on **Record**, **Prohibit**, and **Manage** to prevent internal information disclosure.

Systemwalker Desktop Patrol Corporate Server (CS)

It is a server that defines operation policies for software distribution and collection policies for Inventory information, and distributes them to each server.

CS uses the Web browser to provide security patch, security auditing, and license management services by saving data on IT assets (IT policies), users, and sections. Generally, a corporation installs Systemwalker Desktop Patrol CS.

It is abbreviated as Desktop Patrol CS or CS.

Systemwalker Desktop Patrol Client Terminal (CT)

It transfers device information to PC that manages assets through Inventory collection. It is used to download distribution software and receive security patches.

It is sometimes called Desktop Patrol CT or CT in short.

Systemwalker Desktop Patrol Domain Server (DS)

It is a server relays or stores operation policies, Inventory information, and distributed software to collect and distribute.

This server is installed for load sharing and so on. It is effective when a client is remote via a low-speed network or an attempt is made to distribute large-capacity contents.

It is sometimes abbreviated as Desktop Patrol DS or DS.

Universal Naming Convention (UNC)

It indicates network resources on the Windows network environment.

Updater

It is an update module distributed from CS to DS/CT. The module is automatically updated with the latest content when the administrator is processing information through the main menu.

Updater Function

It is a function that requires simple operation to apply the update to the client systems.

It can be automatically applied through the update of DS and CT, and the registration on the “MC Window”. Since the application is running automatically, the administrator need not operate the device on DS and CT.

User Memo(DTPA)

It is the information which can be set freely for devices.

User Account

It is the authority to view the login user information and registered user ID/password that is allocated when building the management information using main menu items.

User Management Information

It is the information of assembled users, which is necessary fro construction of management information.

User Asset Software Dictionary

The software dictionary that is created according to user assets management information is called user asset software dictionary.

After executing the user asset software dictionary creation command (dtplocaldic.exe), users can add definitions from the **Environment Setup**> **User definition menu**.

User security

It allows users to collect setting status of Screen saver and security level of Internet Explorer from each PC, as the security information for user setting.

User Definition

The administrator creates the criteria for checking the unregistered software in the software dictionary, and defines software use inside enterprises.

Index