FUJITSU

FUJITSU Software
Systemwalker Desktop Patrol

User's Guide

Windows

B1WD-3286-04ENZ0(00)
July 2015

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 V15.1.0

Systemwalker is a generic name for the distributed system operation management products 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
- General knowledge regarding smart devices

Structure of this guide

The structure of this guide is as follows:

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.

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 Release Information	Functions modified and added to Systemwalker Desktop Patrol, and items that become incompatible after a version upgrade.

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 install Systemwalker Desktop Patrol, change the operation environment, and perform maintenance.
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. 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.
|	Indicates that one of the items separated by this symbol should be specified.
{ }	Indicates that one of the items enclosed in these symbols should be specified.

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, Systemwalker Desktop Patrol CT or Systemwalker Desktop Patrol SS 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
Systemwalker Desktop Patrol SS	SS
Systemwalker Desktop Patrol Client	Smart device CT

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

Abbreviation	Full Name
Windows Server(R) 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter
Windows Server(R) 2012	Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter
Windows Server(R) 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise
Windows Server(R) 2008	Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise

Abbreviation	Full Name
Windows(R) 8.1	Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise
Windows(R) 8	Windows(R) 8 Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise
Windows(R) 7	Windows(R) 7 Enterprise Windows(R) 7 Ultimate Windows(R) 7 Professional Windows(R) 7 Home Premium
Windows Vista(R)	Microsoft(R) Windows Vista(R) Ultimate Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Home Premium Microsoft(R) Windows Vista(R) Home Basic Microsoft(R) Windows Vista(R) Ultimate 64-bit Edition Microsoft(R) Windows Vista(R) Enterprise 64-bit Edition Microsoft(R) Windows Vista(R) Business 64-bit Edition Microsoft(R) Windows Vista(R) Home Premium 64-bit Edition Microsoft(R) Windows Vista(R) Home Basic 64-bit Edition
Windows	Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise Windows(R) 8 Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 7 Enterprise Windows(R) 7 Ultimate Windows(R) 7 Professional Windows(R) 7 Home Premium Microsoft(R) Windows Vista(R) Ultimate Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Home Premium Microsoft(R) Windows Vista(R) Home Basic

Abbreviation	Full Name
	Microsoft(R) Windows Vista(R) Ultimate 64-bit Edition Microsoft(R) Windows Vista(R) Enterprise 64-bit Edition Microsoft(R) Windows Vista(R) Business 64-bit Edition Microsoft(R) Windows Vista(R) Home Premium 64-bit Edition Microsoft(R) Windows Vista(R) Home Basic 64-bit Edition
IIS	Internet Information Services 6.0 Internet Information Services 7.0 Internet Information Services 7.5 Internet Information Services 8.0 Internet Information Services 8.5
IE	Microsoft(R) Internet Explorer(R) 6.0 Windows(R) Internet Explorer(R) 7 Windows(R) Internet Explorer(R) 8 Windows(R) Internet Explorer(R) 9 Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11
Android	Android(TM) 3.0 - Android(TM) 5.0
iOS	iOS 5.0 - iOS 8.1

Shortcuts in the Start window of Windows(R) 8 and Windows Server(R) 2012

To check which product a shortcut in the **Start** window is for, right-click the shortcut and click **Open File Location** from the menu at the bottom of the screen. This will open the file location in **Windows Explorer**, where the product name can be checked.

Halfwidth characters

In this guide, the "halfwidth characters to be handled" refer to the following ASCII characters, except in places where limitations for the halfwidth characters that can be used are described.

- Halfwidth spaces
- Halfwidth symbols

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- Halfwidth numbers

  0 1 ... 9
- Halfwidth alphabetic characters

  A B ... Z

  a b ... z

Characters other than the above are treated as fullwidth characters.

Version notation

The following versions of this product do not have an English version - ignore references to them.

- Systemwalker Desktop Patrol V12.0L10
- Systemwalker Desktop Patrol V13.3.0
- Systemwalker Desktop Patrol V14.0.0
- Systemwalker Desktop Patrol V14.0.1
- Systemwalker Desktop Patrol V14.1.0
- Systemwalker Desktop Patrol V14.3.0
- Systemwalker Desktop Patrol V14.3.1

- Systemwalker Desktop Patrol V15.0.0
- Systemwalker Desktop Patrol V15.0.1

For example, read "V15.0.1 or later" as "V14.2.0 or later", because V15.0.1 does not have an English version.

Likewise, read "V14.0.0 or earlier" as "V13.2.0 or earlier", because V14.3.1 does not have an English version.

The table below shows the available versions:

Japanese version	English version
V11.0L10	V11.0L10
V12.0L10	V11.0L10
V13.0.0	V13.0.0
V13.2.0/V13.2.1	V13.2.0
V13.3.0	V13.2.0
V14.0.0/V14.0.1	V13.2.0
V14.1.0	V13.2.0
V14.2.0	V14.2.0
V14.3.0	V14.2.0
V14.3.1	V14.2.0
V15.0.0	V14.2.0
V15.0.1	V14.2.0
V15.1.0	V15.1.0

Export management regulations

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

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.

Google, the Google logo, Android, the Android logo, Google Play, the Google Play logo, Gmail, and the Gmail logo are trademarks or registered trademarks of Google Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Apple, the Apple logo, and Mac OS are trademarks of Apple Inc., registered in the United States and other countries.

All other trademarks are the property of their respective owners.

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

July 2015

First edition, July 2015

Contents

Chapter 1 Overview of Systemwalker Desktop Patrol....1
1.1 Product Positioning....1
1.2 Features....2
1.3 System Structure....4
1.3.1 Components of Systemwalker Desktop Patrol....4
1.3.2 Software Dictionary....5
1.3.3 System Structure....6
1.3.4 System Structure When CT is Installed in the Virtual Desktop Environment....13
1.3.5 Communications Security....15

Chapter 2 Systemwalker Desktop Patrol Functions....16
2.1 PC Information Collection/Browse Function....16
2.1.1 How to Collect....16
2.1.2 Inventory Information....18
2.1.3 Product Information....34
2.1.4 Software Auditing Information....35
2.1.5 Software Operation Status....38
2.1.6 Security Information....39
2.1.7 PC Operation Management....45
2.1.8 File Collection....46
2.1.9 Display of Usage Status and Application Processing....46
2.1.10 Command of Inspection on CT Operation Status....48
2.1.11 Operation Log Collection 48
2.2 PC Auditing/Control Function....49
2.2.1 Auditing Control of Power Saving Setup....49
2.2.2 Auditing/Control of Security Setup....51
2.3 License Management Function....53
2.3.1 License Management....53
2.3.2 Control Execution File....55
2.4 File Distribution Function....55
2.4.1 File Distribution Settings & Distribution Target....55
2.4.2 File Download....56
2.4.3 Distribution Result Confirmation....57
2.5 Software Distribution Function....59
2.5.1 Management on Software Distribution....60
2.5.2 Setup of Software Distribution Target....61
2.5.3 Download of Software Distribution....62
2.6 Security Patches Distribution /Application Function....64
2.6.1 Automatic Application of Security Patches....64
2.6.2 Manual Application of Security Patch....65
2.6.3 Selection of Security Patches Applied to Specific PC....65
2.7 Smart Device Management Function....66
2.7.1 Managing an Individually Owned Smart Device (Android Device Only)....66
2.8 Application Distribution Function (to Smart Devices)....66
2.9 Management Ledger Function....67
2.9.1 Device Management....67
2.9.2 Contract Management....71
2.9.3 Stocktaking Support....74
2.9.4 Unregistered Management....76
2.10 Report Output Function....78
2.10.1 Asset Information Report....78
2.10.2 Security Auditing Report....79
2.10.3 Power Saving Countermeasure Auditing Report....83
2.11 Location Map Function....86
2.12 Environment Setup Function....86

2.13 Remote Operation Function........91
2.14 Updater Function........92
2.15 CT Prohibition Function........92

Chapter 3 Operating Environment........94
3.1 Required Hardware........94
3.2 Software........98
3.2.1 Operating System........98
3.2.2 Required Software........103
3.2.3 Products That Cannot Coexist........106
3.3 Operations with Mixed Versions or Levels........106

Chapter 4 Link with Other Products........108
4.1 List of Linkage Products........108
4.2 Event Linkage........108
4.3 Collection of Inventory Information........109
4.4 Configuration Information........110
4.5 Security Auditing........110
4.6 Creation of Assets Management Ledger of Other Products........111

Glossary........112

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

The Systemwalker Desktop series consists of a group of products designed to perform security measures. The measures include security patch application to counter risks associated with the work type and environment, restrictions on PC operations, log collection and analysis, restrictions on file operations, and block of unauthorized PCs through correct understanding of your assets. In addition, this series offers functions to promote green ICT.

Positioning of Systemwalker Desktop Patrol

Systemwalker Desktop Patrol is a set of ICT 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.

Furthermore, asset management is now possible on Android(TM) /iOS-based smart devices, making it easier to understand how smart devices are used for work.

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

Green ICT plan

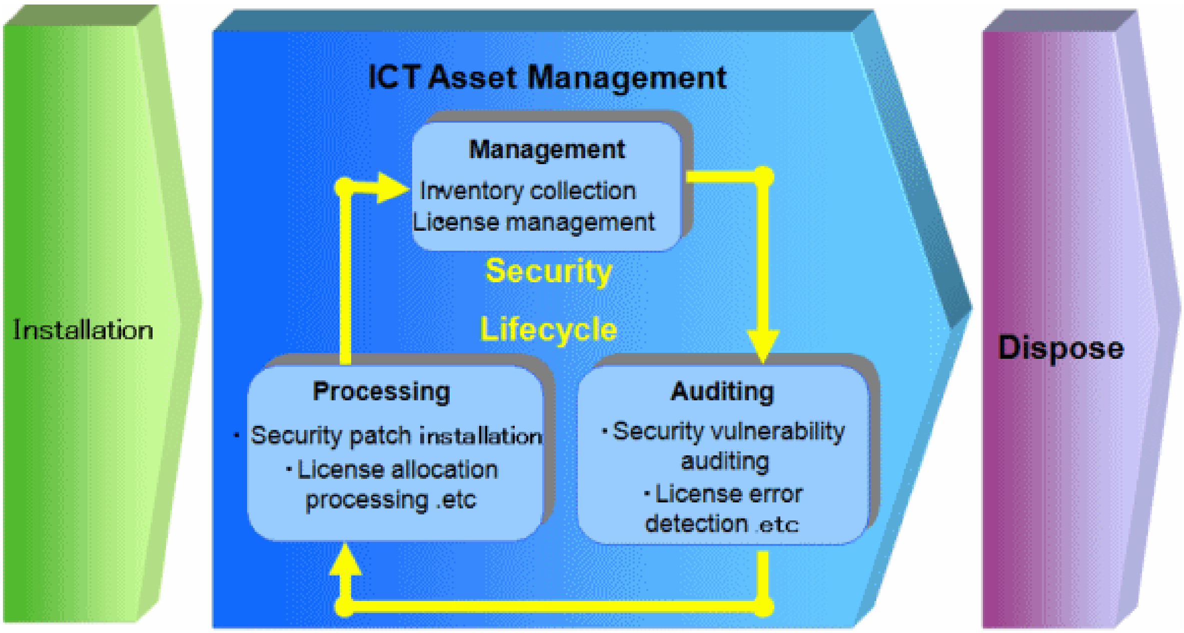
Because of the severe environmental problems, enterprises must enhance their environmental protection consciousness and improve the energy saving methods. Based on the previous client management function, Systemwalker Desktop Patrol provides the function of decreasing the PC power consumption, supporting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

PC power saving policy can be set based on PC usage, be it company-wide or per section, and PCs violating it can have their settings forcibly changed to maintain the power saving state. This restricts wasteful uses of PCs, and thus contributes to reduction of PC power consumption.

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.

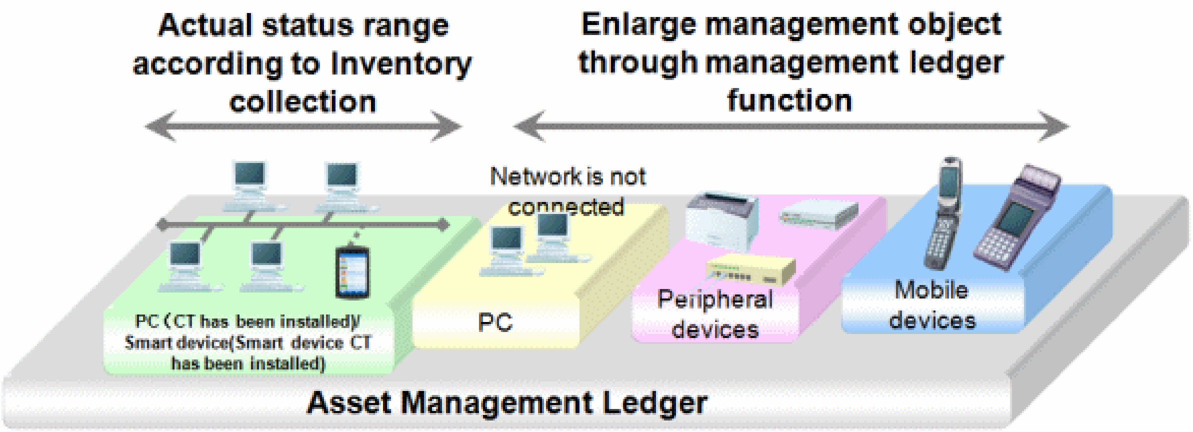
The anti-disclosure function in Systemwalker Desktop Patrol is enhanced to protect the ICT assets. The life cycle from software installation to discard can be protected.


ICT Asset Management
Installation
Management
Inventory collection
License management
Security
Lifecycle
Processing
・Security patch installation
・License allocation processing .etc
Auditing
・Security vulnerability auditing
・License error detection .etc
Dispose

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 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, equipment, or smart devices 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)/ Smart device(Smart device CT has been installed)
PC
Peripheral devices
Mobile devices
Asset Management Ledger

1.2 Features

For an enterprise, ICT investment is strategic and necessary. In the ICT 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, device (PC, equipment or smart devices) assets management and client security management are important for enterprises.

The device (PC, equipment or smart devices) 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 management

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

Unified ICT assets management

Systemwalker Desktop Patrol allows you to see the setup place, quantity, and actual usage of ICT 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 ICT 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 System Structure

This section describes the structure of Systemwalker Desktop Patrol.

1.3.1 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 ICT 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.

Systemwalker Desktop Patrol SS (Smartdevice Server)

This server must be installed between the Systemwalker Desktop Patrol CS and smart device CT to manage smart devices. To notify the inventory information from the smart device to the CS, it relays that data.

Systemwalker Desktop Patrol Client

This is a client that is used for smart devices, and is hereafter referred to as a "smart device CT". It is installed on the smart device that manages the assets through inventory collection.

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.

1.3.2 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.

Also, the association of SAM Assessment & Certification (SAMAC) Software Dictionary can be imported and used in Systemwalker Desktop Patrol.

The SAMAC Software Dictionary has the following characteristics:

- As of January 2014, it contains approximately 70,000 data items. More than 6,000 data items are added every year.

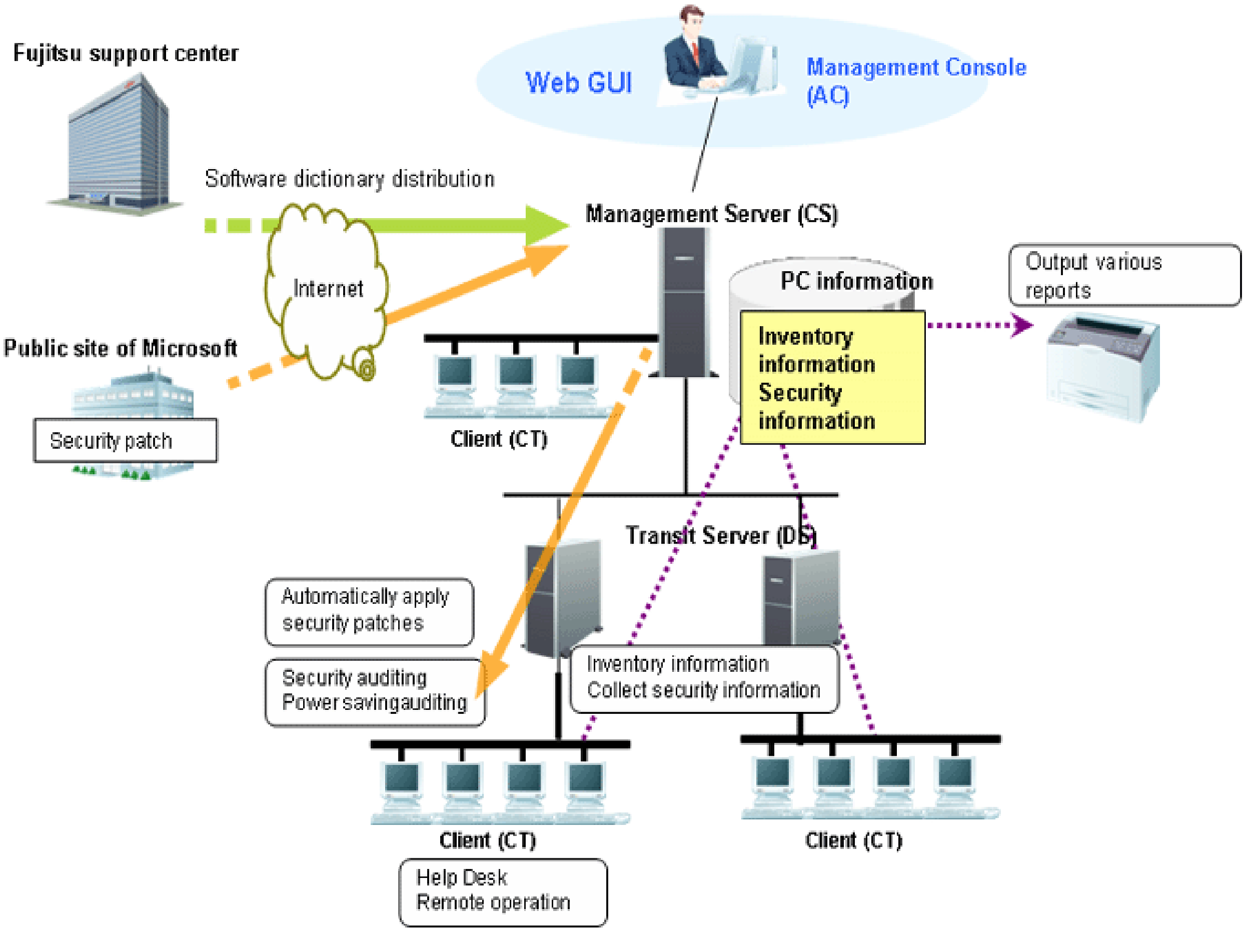
- It covers commercial software, freeware, and drivers.

- It is created based on the installed program names displayed in **Uninstall a program** and **View installed updates** in **Add or Remove Programs** or **Programs and Features**.

To import the SAMAC Software Dictionary, the user must enter into an agreement with SAMAC and obtain it.

1.3.3 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

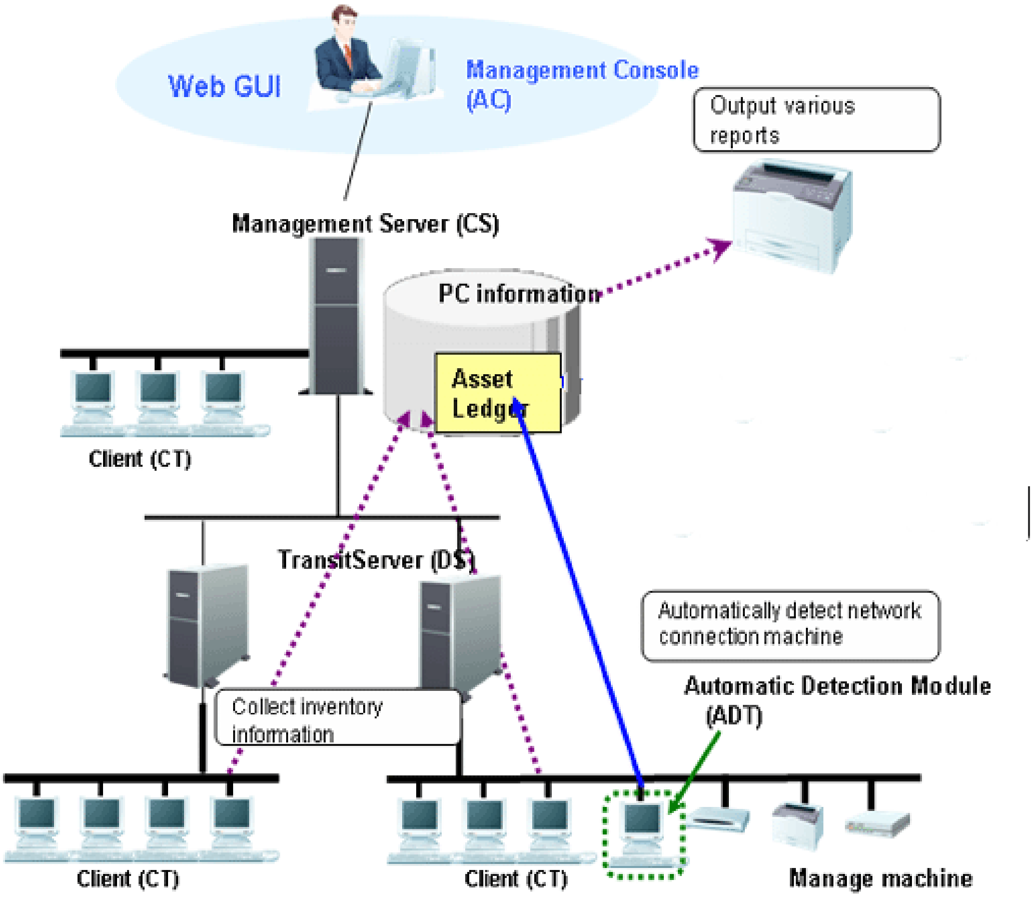
   The administrator confirms the software installation status and hardware information.

   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 ICT 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.

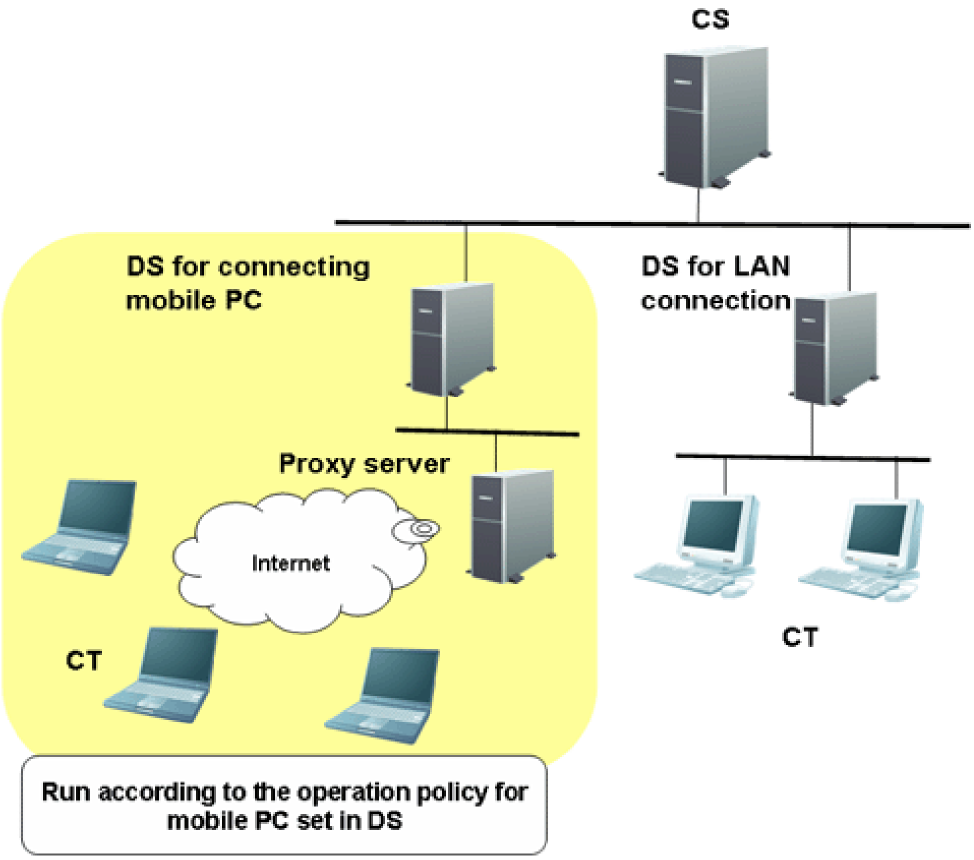
   c. Set on the page

      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 .

System configuration for smart device assets management

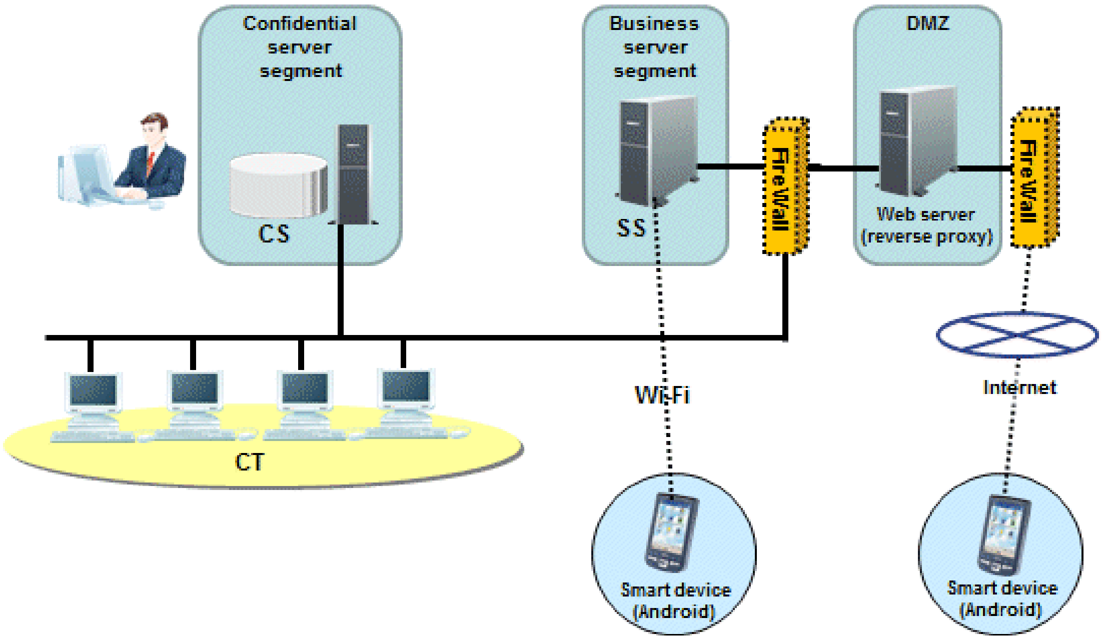
To manage smart device assets, Systemwalker Desktop Patrol SS must be installed between the Systemwalker Desktop Patrol CS and smart device CT.

If collecting the smart device inventory information via the internet, install a reverse proxy server in the DMZ. The server must be operated in the recommended configuration shown below.

- Smart device operation patterns

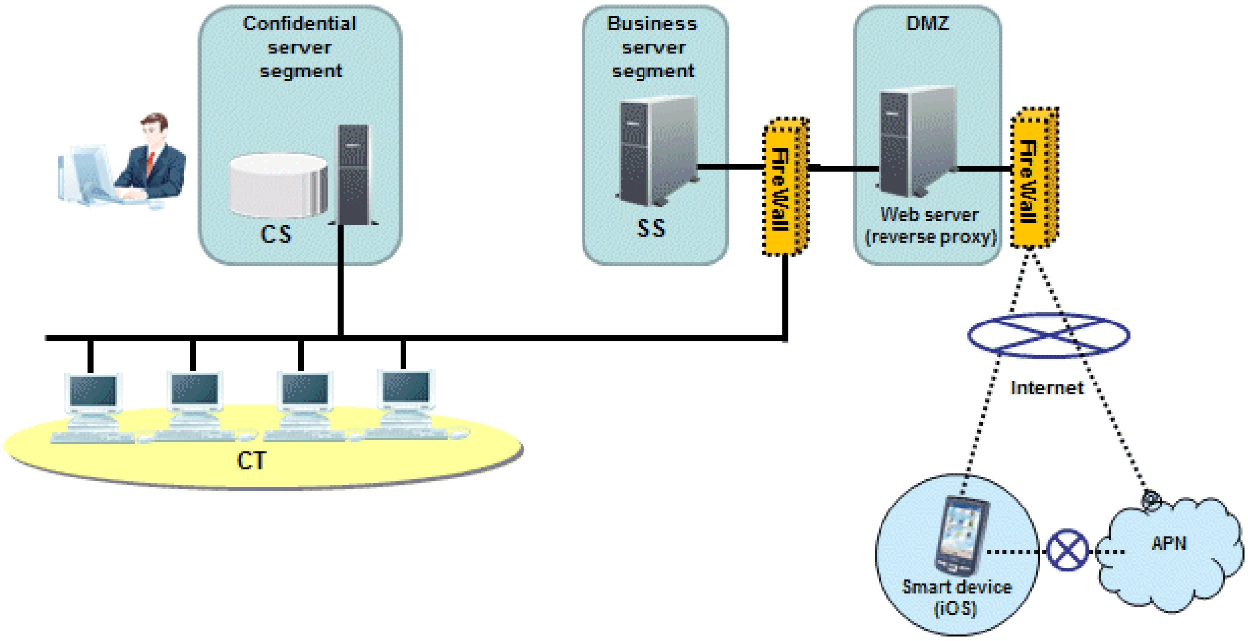
  Smart devices are typically used on the company's intranet and in locations outside the company.

Smart device (Android)



If the smart device assets are managed in an intranet environment only, then the Systemwalker Desktop Patrol SS and Systemwalker Desktop Patrol CS can coexist. To enable the SS and CS to coexist, the CS must be installed before the SS.

Smart device (iOS)



When using iOS devices to manage assets, it is necessary to have an environment in which Systemwalker Desktop Patrol SS and smart devices can connect to the APN (Apple Push Notification Service). Assets cannot be managed in an intranet environment.

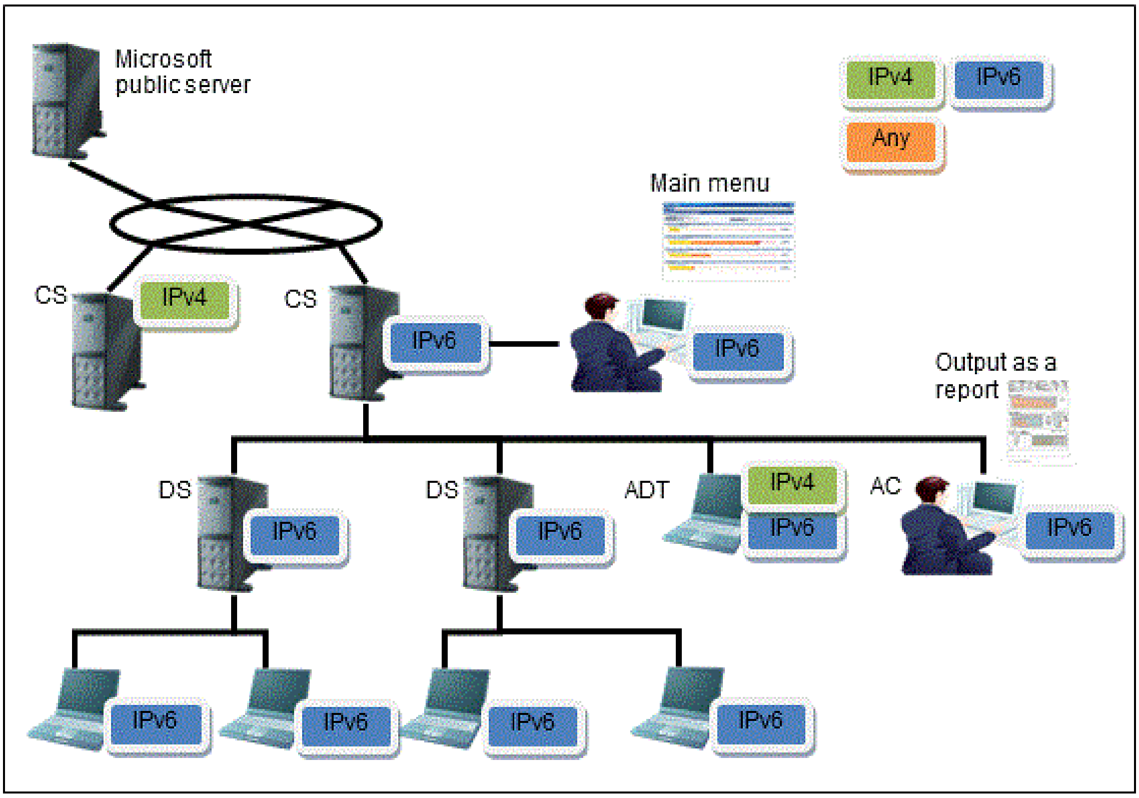
System configuration supporting IPv6

IPv6 network configuration supported in Systemwalker Desktop Patrol is shown below.

Note

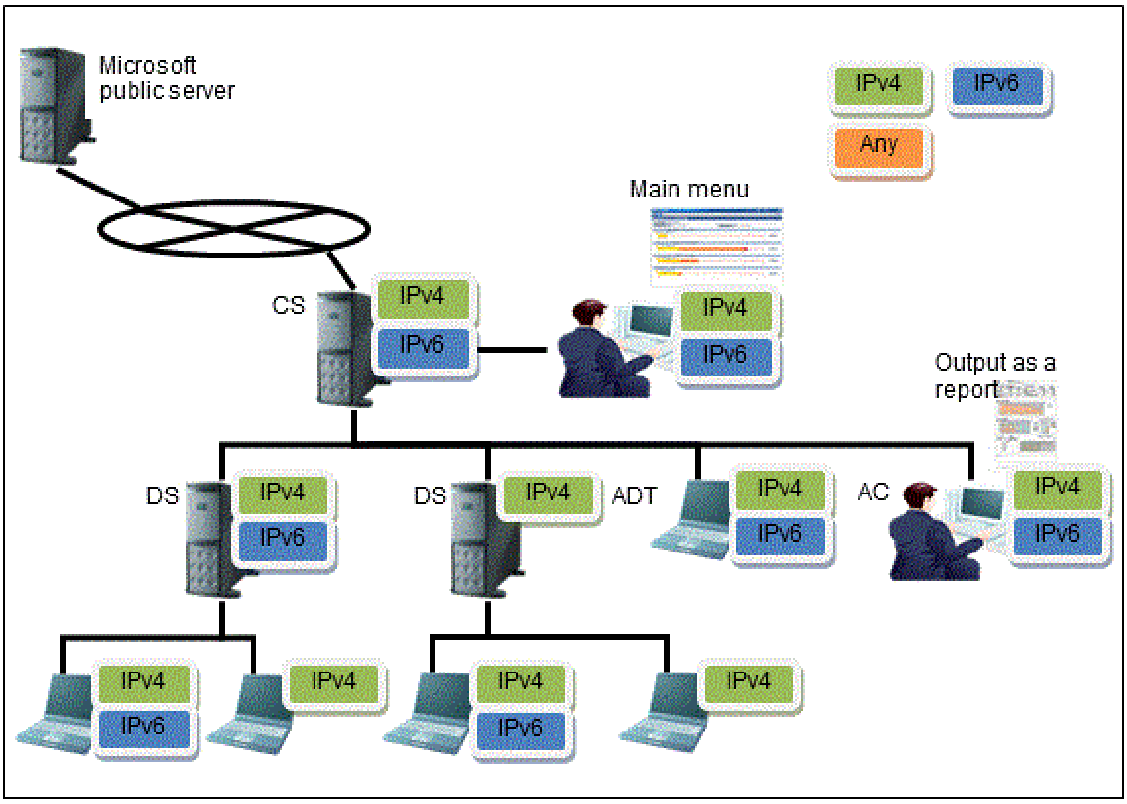
- If the Systemwalker Desktop Patrol CS is in an IPv6-only environment, you will not be able to connect to the Systemwalker support center. For the CS, a dual stack environment must be built.

- IPv6-only environment



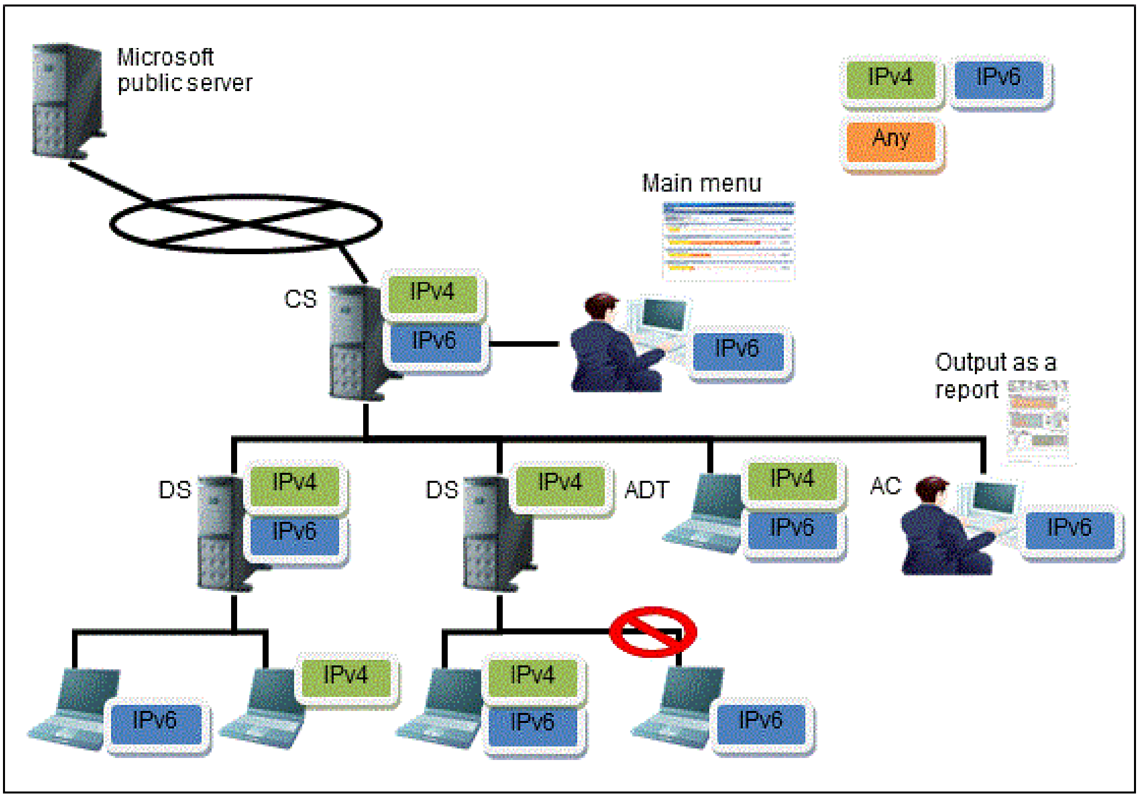
Function	Operation result
Inventory information	IPv6 network information is collected in the CT, and IPv6 information can be viewed in the main menu.
Network communication	Communication is performed using the IPv6 network environment.
Unregistered device detection (ADT)	IPv6-only environment is not supported.
Systemwalker support center	Only IPv4 is supported.
CS	A dual stack environment must be built. If the CS is in an IPv6-only environment, you will not be able to connect to the Systemwalker support center.

- IPv4 and IPv6 dual stack environment



Function	Operation result	Note
Inventory information	IPv4 and IPv6 network information is collected in the CS, and the IPv4 and IPv6 information can be viewed in the main menu.	If the collection target is V14.2.1 or earlier, then only the IPv4 information can be collected and viewed.
Network communication	In a dual stack CT environment, communication is attempted with only the first IP address retrieved.	

- Where IPv4 and IPv6 network environments coexist



Function	Operation result	Note
Inventory information	IPv4 and IPv6 network information is collected in the CT, and the IPv4 and IPv6 information can be viewed in the main menu. - In an IPv4-only CT environment, only IPv4 can be collected and viewed. - In an IPv6-only CT environment, only IPv6 can be collected and viewed. - In a dual stack CT environment, IPv4/IPv6 can be collected and viewed.	
Network communication	Communication is performed as shown below: - IPv4 communication in an IPv4-only CT environment - IPv6 communication in an IPv6-only CT environment - In a dual stack CT environment, communication is attempted with only the first IP address retrieved.	A downstream server in an IPv6-only environment cannot connect to an upstream server in an IPv4-only environment. Connection is possible only if the downstream server is also in an IPv4-only environment.

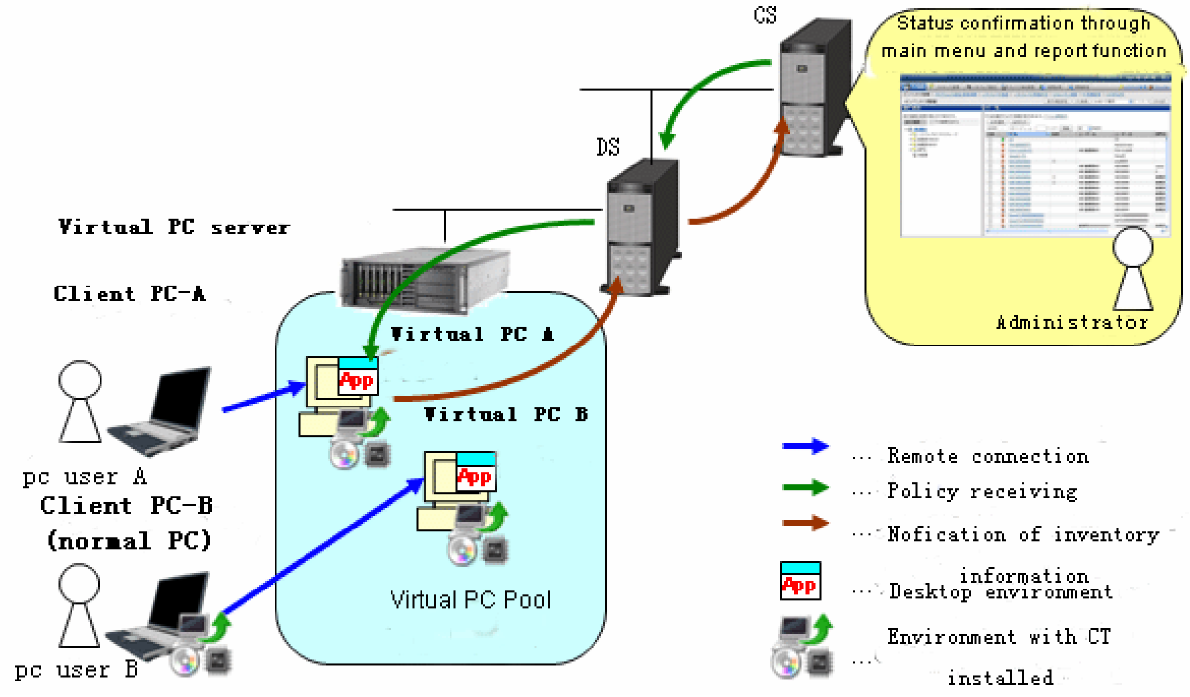
1.3.4 System Structure When CT is Installed in the Virtual Desktop Environment

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.

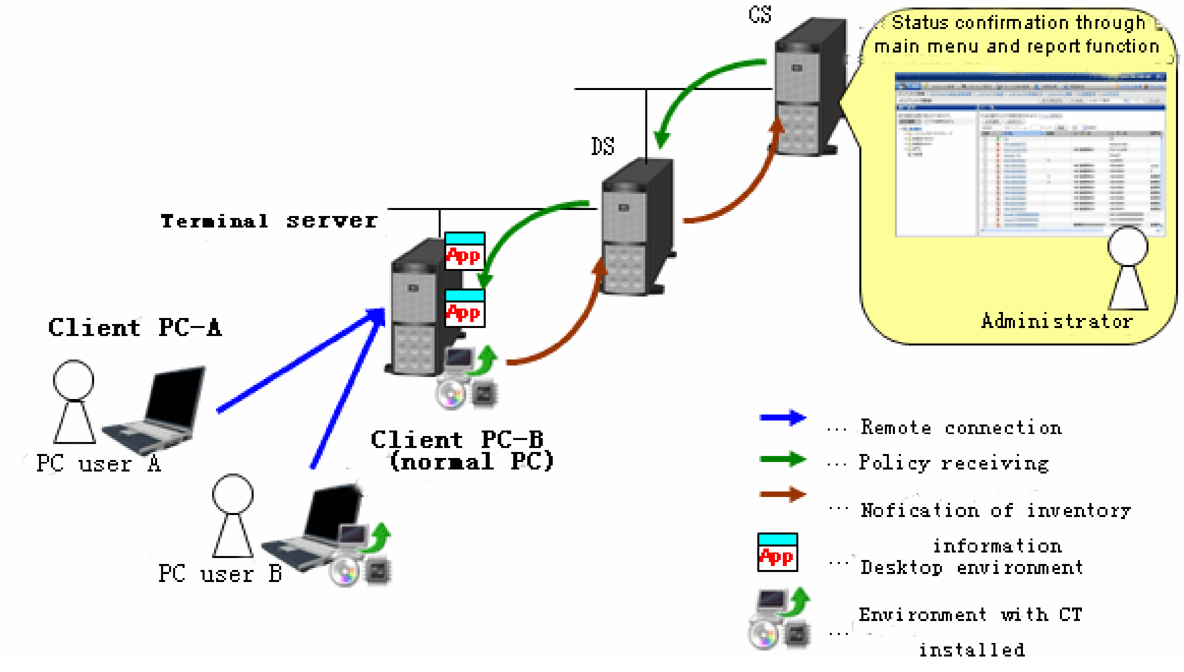


Virtual PC server: PC which is running VMware ESX, VMware vSphere, and Microsoft Hyper-V.
Client PC: Common notebook computer or desktop computer.
Virtual PC Pool: Set groups for virtual PCs.

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.

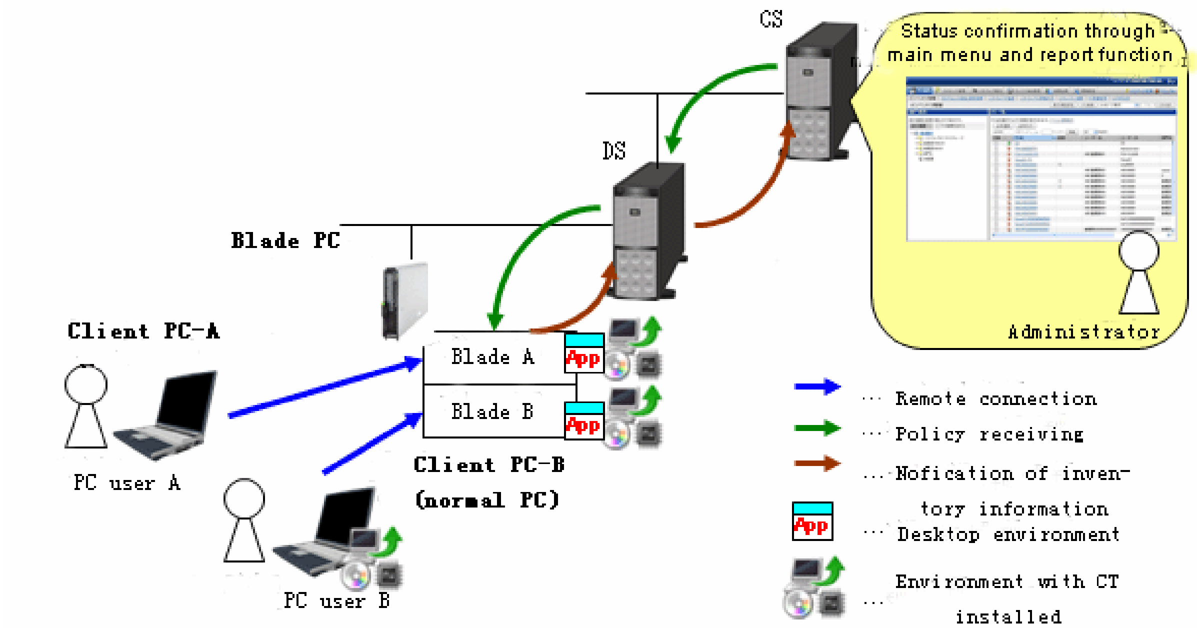


Terminal server: As a Windows server (Windows Server 2008), the environment for the terminal server or remote desktop session host is installed.
Client PC: Common notebook computer or desktop computer.

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.



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

1.3.5 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
- Smart Device Management Function
- Application Distribution Function (to Smart Devices)
- Management Ledger Function
- Report Output Function
- Location Map Function
- Environment Setup Function
- Remote Operation Function
- Updater Function
- CT Prohibition Function

Also, 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. USB memory.
    - 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	Collectable	
	Agent Mode	Command Mode
Basic Information (OS Information, Hardware Information)	Y	Y
Software Information	Y	Y
Anti-Virus Software	Y	Y
Product Information	Y	Y
User Information	Y	Y
EXE Information	Y	Y
Registry Information	Y	Y
Unapplied Patch Information	Y	Y
Security Information: System Security Information User Security Information	Y	Y
Security Information: Desktop Keeper information	Y	N
Power saving auditing information: Power saving setting value	Y	Y
Power saving auditing information: Power saving status	Y	N
Software Operation Status	Y	N
Files Collection	Y	N
Simple operation logs	Y	N

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
- Product Information
- User Info
- EXE Info
- Registry Info
- Unapplied Patch Info
- Contract Information
- Security Information
- Power Saving Information

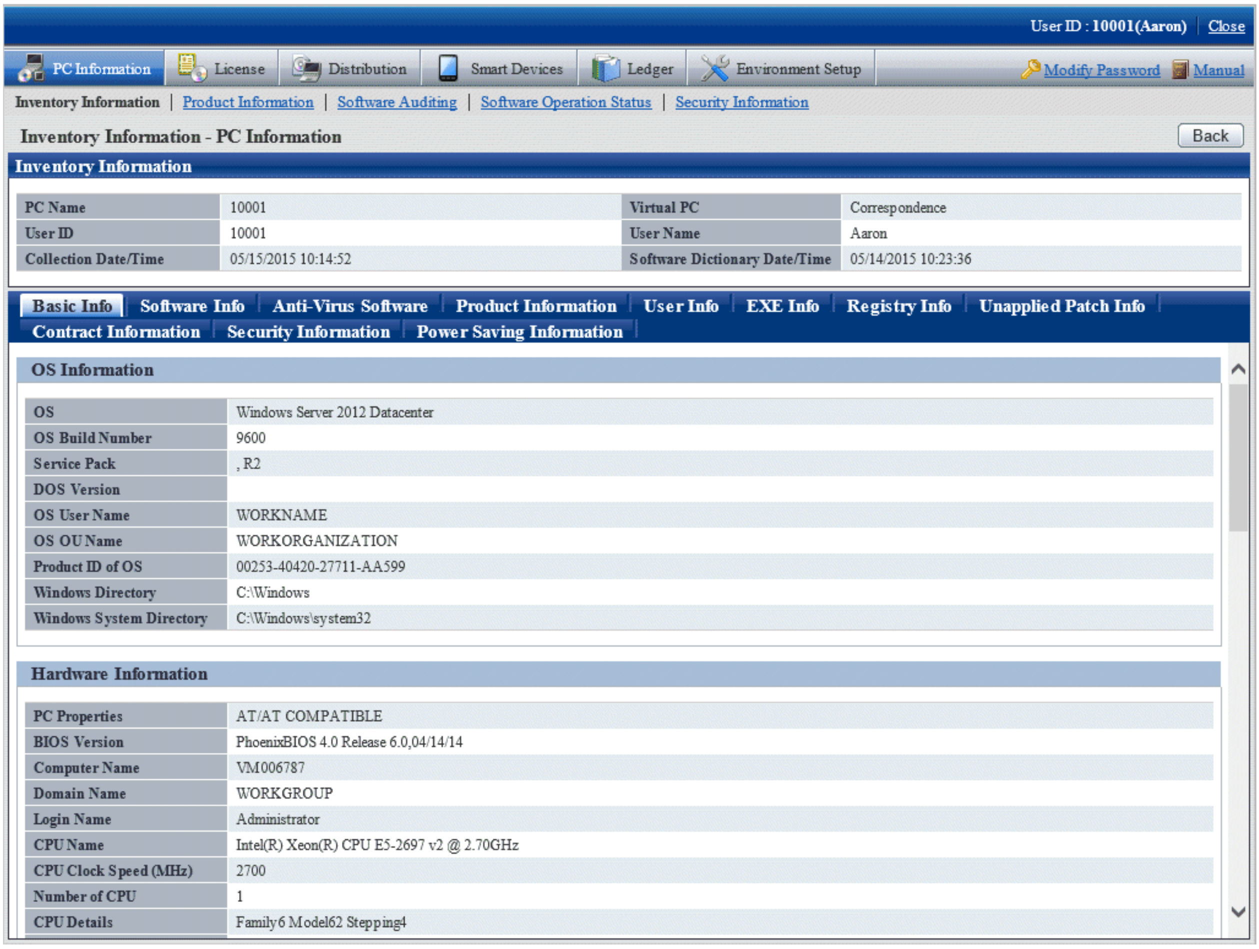
The information is mainly displayed in the **PC Information** > **Inventory Information** window of the main menu.

In addition, in the OS installed with Systemwalker Desktop Keeper V14.2.0 or later, 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).


User ID : 10001(Aaron)
Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Product Information | Software Auditing | Software Operation Status | Security Information
Back
Basic Info | Software Info | Anti-Virus Software | Product Information | User Info | EXE Info | Registry Info | Unapplied Patch Info
Contract Information | Security Information | Power Saving Information

Inventory Information - PC Information

Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/15/2015 10:14:52	Software Dictionary Date/Time	05/14/2015 10:23:36

OS Information

OS	Windows Server 2012 Datacenter
OS Build Number	9600
Service Pack	, R2
DOS Version	
OS User Name	WORKNAME
OS OU Name	WORKORGANIZATION
Product ID of OS	00253-40420-27711-AA599
Windows Directory	C:\Windows
Windows System Directory	C:\Windows\system32

Hardware Information

PC Properties	AT/AT COMPATIBLE
BIOS Version	PhoenixBIOS 4.0 Release 6.0,04/14/14
Computer Name	VM006787
Domain Name	WORKGROUP
Login Name	Administrator
CPU Name	Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
CPU Clock Speed (MHz)	2700
Number of CPU	1
CPU Details	Family6 Model62 Stepping4

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	Vista	Vista 64bit	7/8	7 64bit / 8 64bit	2008	2008 64bit / 2012	Remarks
Hardware Information	PC Properties	Y	Y	Y	Y	Y	Y	
	BIOS Version	D	D	D	D	D	D	
	Computer Name	Y	Y	Y	Y	Y	Y	
	Domain Name	Y	Y	Y	Y	Y	Y	Obtain the work group name if domain setup is not available.
	Login Name	Y	Y	Y	Y	Y	Y	
	CPU Name	Y	Y	Y	Y	Y	Y	
	CPU Clock Speed	D	D	D	D	D	D	
	Number of CPU	Y	Y	Y	Y	Y	Y	
	CPU Details	Y	Y	Y	Y	Y	Y	
	Memory Size	Y	Y	Y	Y	Y	Y	This is different from the **Installed memory (RAM)** displayed by

Class	Item	Vista	Vista 64bit	7/8	7 64bit / 8 64bit	2008	2008 64bit / 2012	Remarks
								Control Panel > **System** (except for Windows Vista Original Release).
	Swap File Size	Y	Y	Y	Y	Y	Y	
	Name of Keyboard Type	Y	Y	Y	Y	Y	Y	
	Installing Language	Y	Y	Y	Y	Y	Y	
	Mouse Type Name	Y	Y	Y	Y	Y	Y	
	Mouse Button Number	Y	Y	Y	Y	Y	Y	
	PC Manufacturer Name	D	D	D	D	D	D	
	PC Model Name	D	D	D	D	D	D	
	PC Serial Number	D	D	D	D	D	D	
	Primary Cache/ Secondary Cache	D	D	D	D	D	D	
OS Information	OS	Y	Y	Y	Y	Y	Y	
	OS Build Number	Y	Y	Y	Y	Y	Y	
	Service Pack	Y	Y	Y	Y	Y	Y	E.g. Displayed as "ServicePack X". If the OS is Windows Server(R) 2008 R2, add ", R2" to it. E.g. Service Pack 1, R2.
	DOS Version	Y	N	Y	N	Y	N	
	OS User Name	D	D	D	D	D	D	If OS is Vista, Vista x64 Edition, Windows 7 or Windows 8, collect the user name originally created when installing the OS. If the OS is 2008, 2008 x64 Edition, 2008 R2 or 2012, collect "Windows User".
	OS OU Name	U	U	U	U	U	U	
	Product ID of OS	Y	Y	Y	Y	Y	Y	

Class	Item	Vista	Vista 64bit	7/8	7 64bit / 8 64bit	2008	2008 64bit / 2012	Remarks
	Windows Directory	Y	Y	Y	Y	Y	Y	
	Windows System directory	Y	Y	Y	Y	Y	Y	
Displayer Information	Screen Resolution (Note 3)	Y	Y	Y	Y	Y	Y	
	Video Adapter	Y	Y	Y	Y	Y	Y	
	Video Memory Size	Y	Y	Y	Y	Y	Y	
	Resolution	Y	Y	Y	Y	Y	Y	
	Screen Saver (Note 3)	D	D	D	D	D	D	
	Monitor Name	Y	Y	Y	Y	Y	Y	
	Screen Refresh Rate (Note 3)	D	D	D	D	D	D	
Drive information (Note 2)	Drive Name	D	D	D	D	D	D	
	Drive Type	D	D	D	D	D	D	
	Drive Capacity	D	D	D	D	D	D	
	Drive Free Capacity	D	D	D	D	D	D	
	Volume	D	D	D	D	D	D	
	File System Type	D	D	D	D	D	D	
CD-ROM information	Device Name	D	D	D	D	D	D	
Disk Information	Manufacturer Name	D	D	D	D	D	D	
	Model Name	D	D	D	D	D	D	
	Disk capacity	Y	Y	Y	Y	Y	Y	
	Disk IF	D	D	D	D	D	D	
	Description	Y	Y	Y	Y	Y	Y	
Memory Information	Device Locator	D	D	D	D	D	D	
	Size	D	D	D	D	D	D	
Network card information (Note 1)	Network Card	D	D	D	D	D	D	Multiple results can be obtained. To obtain the logical names when grouping the multiple network cards.

Class	Item	Vista	Vista 64bit	7/8	7 64bit / 8 64bit	2008	2008 64bit / 2012	Remarks
	MAC Address	Y	Y	Y	Y	Y	Y	Multiple results can be obtained.
TCP/IP Information (Note 2)	Host name	Y	Y	Y	Y	Y	Y	Multiple results can be obtained
	IP Address	Y	Y	Y	Y	Y	Y	
	Subnet Mask	Y	Y	Y	Y	Y	Y	
	Default Gateway	Y	Y	Y	Y	Y	Y	
	DHCP Server	Y	Y	Y	Y	Y	Y	
	DNS Server	D	D	D	D	D	D	
Network sharing information (Note 3)	Network Path Name	D	D	D	D	D	D	
	Network Service Supplier Name	D	D	D	D	D	D	
	Drive Letter	D	D	D	D	D	D	
Printer Information (Note 3)	Printer Name	D	D	D	D	D	D	
	Printer Type	D	D	D	D	D	D	

Y: Collectable.

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

N: Not collectable.

U: Uncollected or no corresponding information.

Vista: Windows Vista(R)

Vista 64bit: Windows Vista(R) x64 Edition

7: Windows(R) 7

7 64bit: Windows(R) 7 x64 Edition

8: Windows(R) 8

8 64bit: Windows(R) 8 x64 Edition

2008: Windows Server(R) 2008

2008 64bit: Windows Server(R) 2008 x64 Edition

2012: Windows Server(R) 2012

Note 1:

- During the application of DHCP, if IP address cannot 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, the TCP/IP value distributed by the DHCP server can be obtained.
- If the DHCP server does not exist, 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 cannot 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, 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.

Note 2:

If an IPv6 environment is set for the PC network, the IPv6 network information will be collected, and the server will be notified. Also, if a dual stack environment with an IPv4 environment is set, then the IPv4 network information, too, will be collected, and the server will be notified.

The inventory information sent to the server can be viewed and searched in the main menu.

- Inventory collection in an IPv6 environment

  The following items are collected as IPv6 network information:

Collected item	Collected		
	IPv6	IPv4	Remark
IP address	Y	Y	Link-local address is not collected.
Subnet mask	Y	Y	In IPv6, the prefix length (subnet prefix length) is sent.
Default gateway	Y	Y	In IPv6, multiple IP addresses can be specified.
DNS server	Y	Y	
DHCP server	N	Y	

Note 3:

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

- Screen resolution

  In Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012, the resolution is 1024x768.

- 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 Vista(R)	Windows sign
Windows(R) 7	Windows sign
Windows(R) 8	Windows sign
Windows Server(R) 2008	Windows sign
Windows Server(R) 2012	Windows sign

- Screen refresh rate

  In Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012, the refresh rate is 60Hz.

- 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 cannot 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

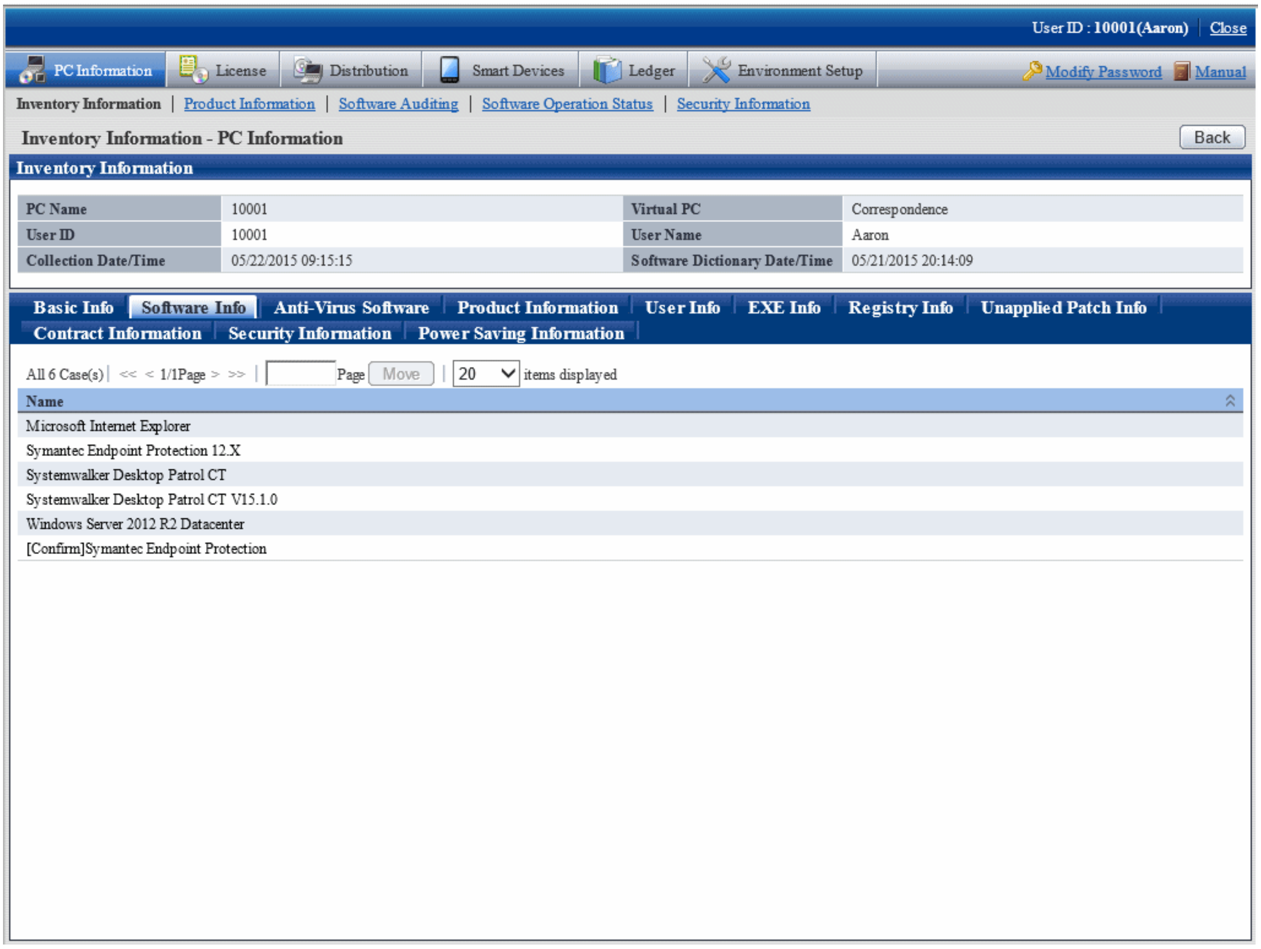
  Printer information can be collected through Inventory collection in command mode. Inventory collection is impossible in agent mode.

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 **Uninstall or change a program** information name
  - Retrieval according to any registry (Key Name, Value Name)



Inventory Information - PC Information

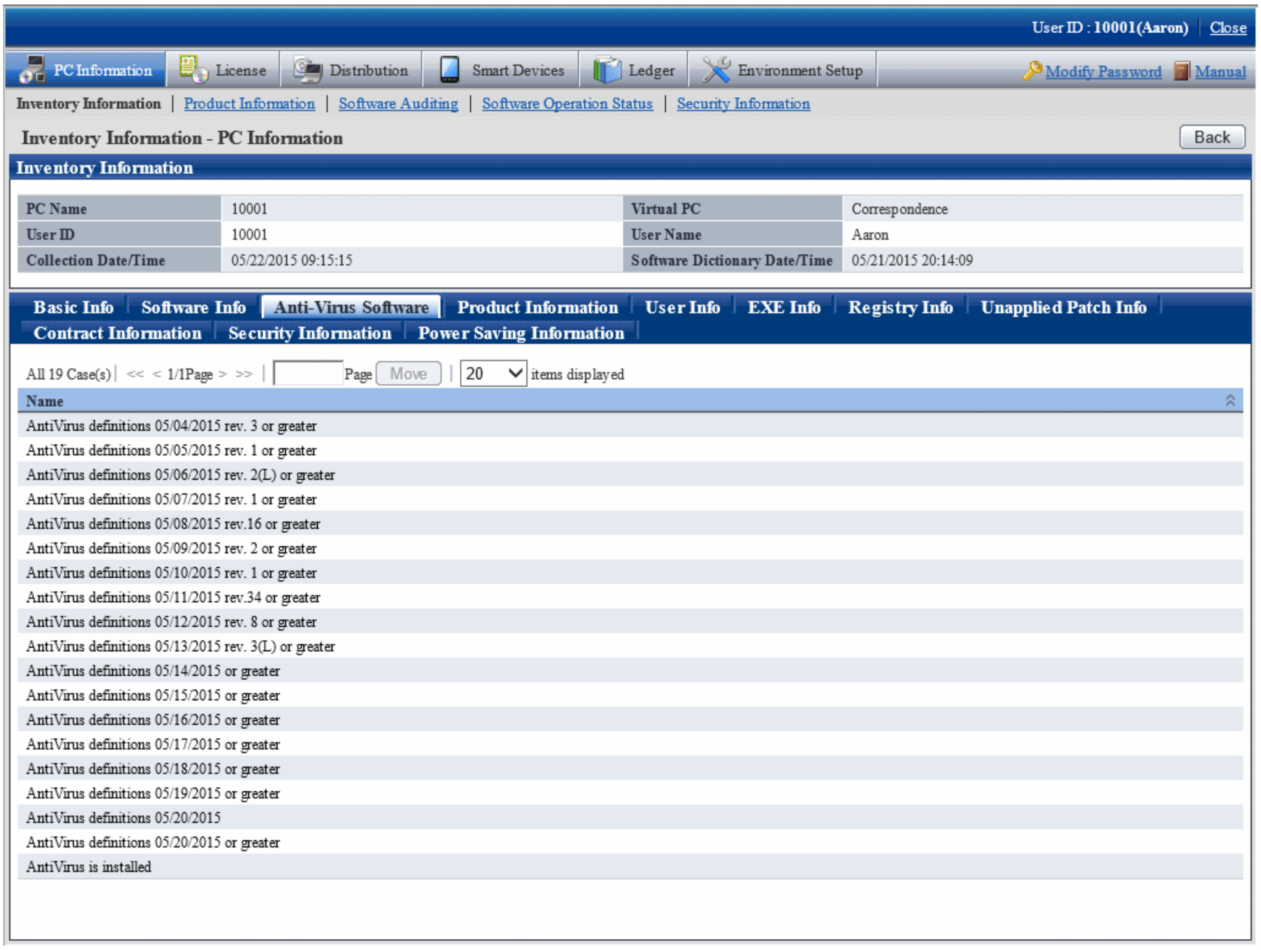
Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 09:15:15	Software Dictionary Date/Time	05/21/2015 20:14:09

Name
Microsoft Internet Explorer
Symantec Endpoint Protection 12.X
Systemwalker Desktop Patrol CT
Systemwalker Desktop Patrol CT V15.1.0
Windows Server 2012 R2 Datacenter
[Confirm]Symantec Endpoint Protection

Anti-Virus software

Collect the anti-virus software installed in the PC.



Inventory Information - PC Information

Inventory Information

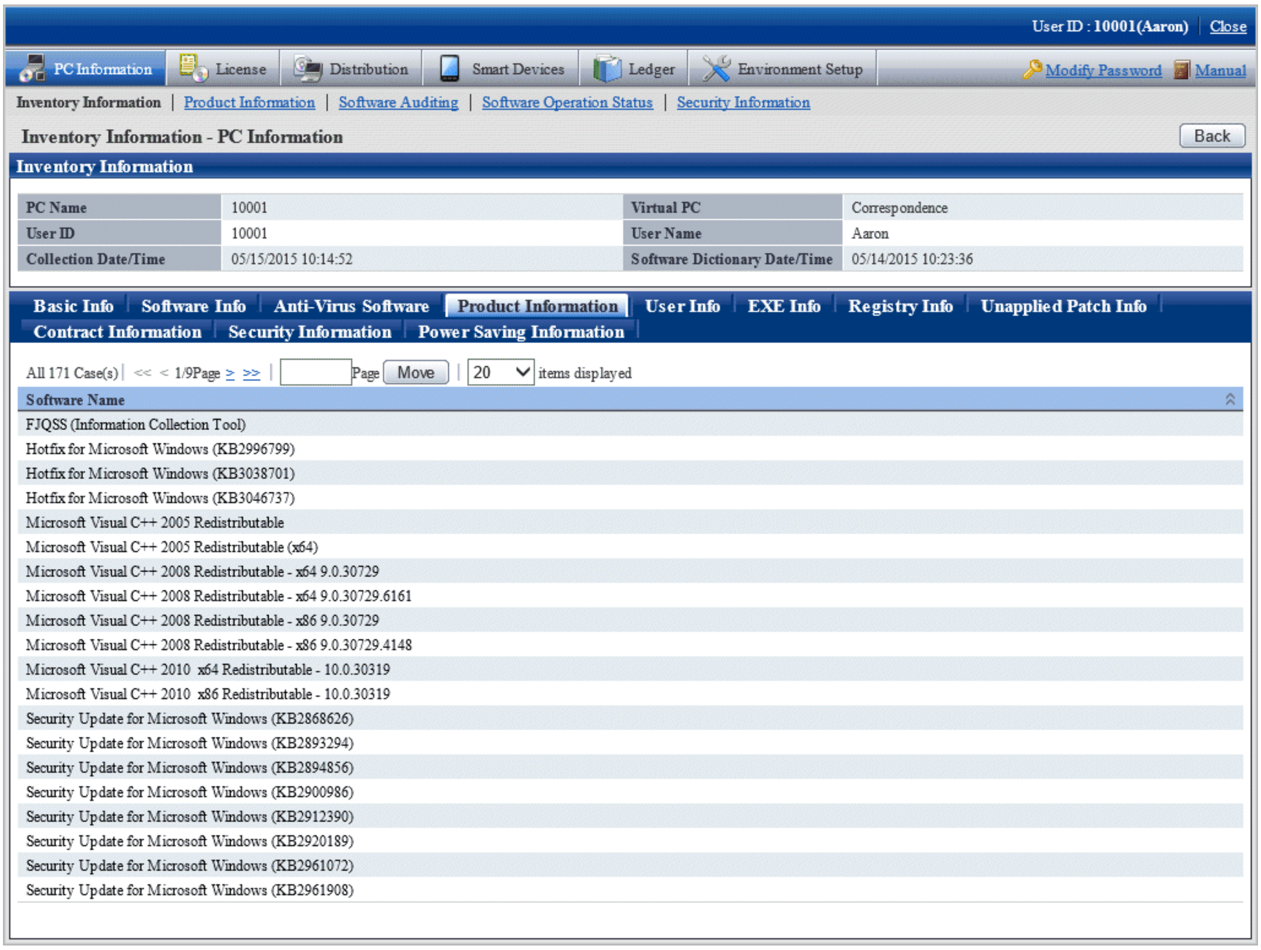
PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 09:15:15	Software Dictionary Date/Time	05/21/2015 20:14:09

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

Name
AntiVirus definitions 05/04/2015 rev. 3 or greater
AntiVirus definitions 05/05/2015 rev. 1 or greater
AntiVirus definitions 05/06/2015 rev. 2(L) or greater
AntiVirus definitions 05/07/2015 rev. 1 or greater
AntiVirus definitions 05/08/2015 rev.16 or greater
AntiVirus definitions 05/09/2015 rev. 2 or greater
AntiVirus definitions 05/10/2015 rev. 1 or greater
AntiVirus definitions 05/11/2015 rev.34 or greater
AntiVirus definitions 05/12/2015 rev. 8 or greater
AntiVirus definitions 05/13/2015 rev. 3(L) or greater
AntiVirus definitions 05/14/2015 or greater
AntiVirus definitions 05/15/2015 or greater
AntiVirus definitions 05/16/2015 or greater
AntiVirus definitions 05/17/2015 or greater
AntiVirus definitions 05/18/2015 or greater
AntiVirus definitions 05/19/2015 or greater
AntiVirus definitions 05/20/2015
AntiVirus definitions 05/20/2015 or greater
AntiVirus is installed

Product information

Collect some of the information in **Uninstall a program** and **View installed updates** in **Add or Remove Programs** or **Programs and Features** in the PC.



Inventory Information - PC Information

Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/15/2015 10:14:52	Software Dictionary Date/Time	05/14/2015 10:23:36

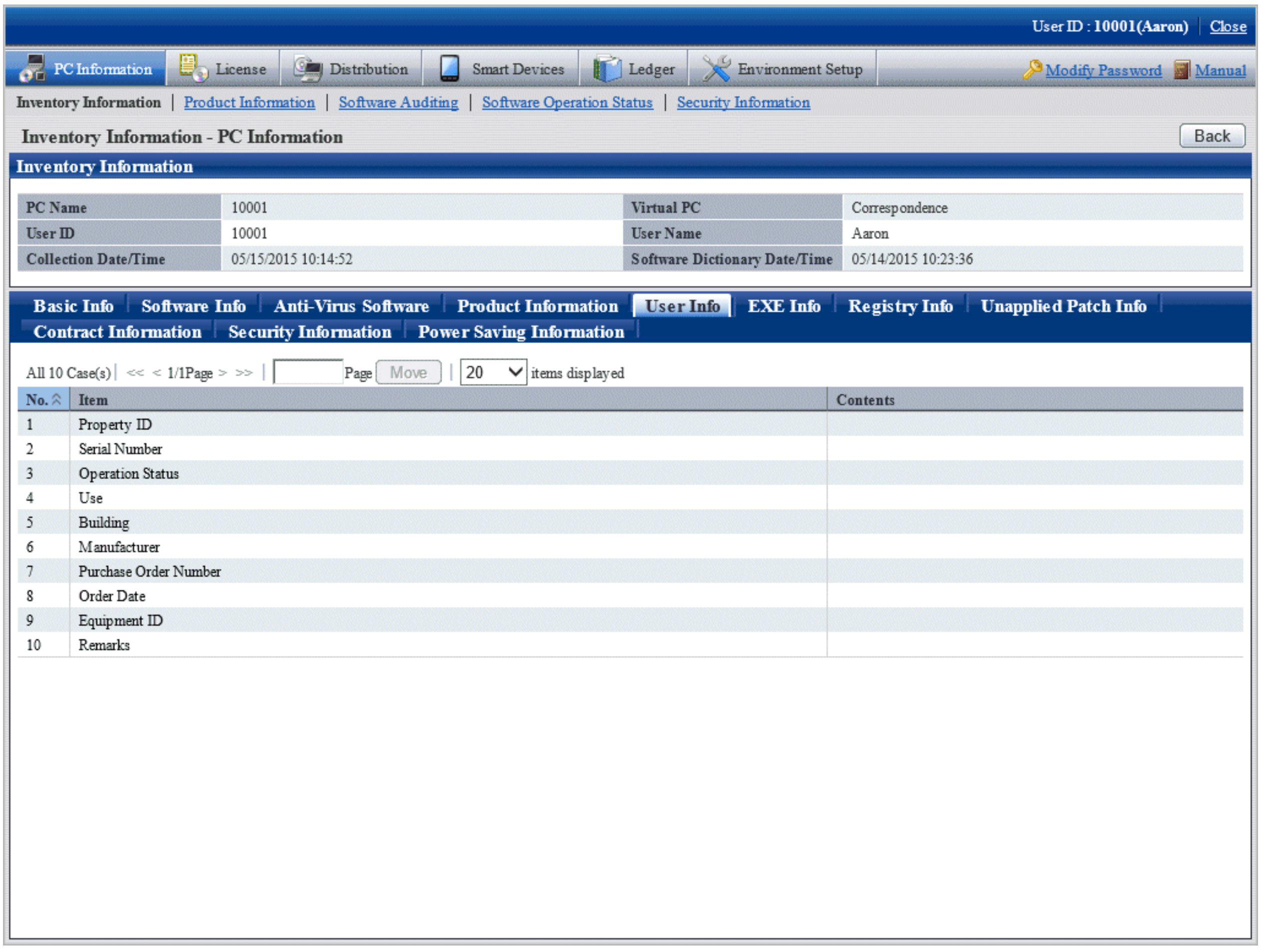
Software Name
FJQSS (Information Collection Tool)
Hotfix for Microsoft Windows (KB2996799)
Hotfix for Microsoft Windows (KB3038701)
Hotfix for Microsoft Windows (KB3046737)
Microsoft Visual C++ 2005 Redistributable
Microsoft Visual C++ 2005 Redistributable (x64)
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319
Security Update for Microsoft Windows (KB2868626)
Security Update for Microsoft Windows (KB2893294)
Security Update for Microsoft Windows (KB2894856)
Security Update for Microsoft Windows (KB2900986)
Security Update for Microsoft Windows (KB2912390)
Security Update for Microsoft Windows (KB2920189)
Security Update for Microsoft Windows (KB2961072)
Security Update for Microsoft Windows (KB2961908)

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

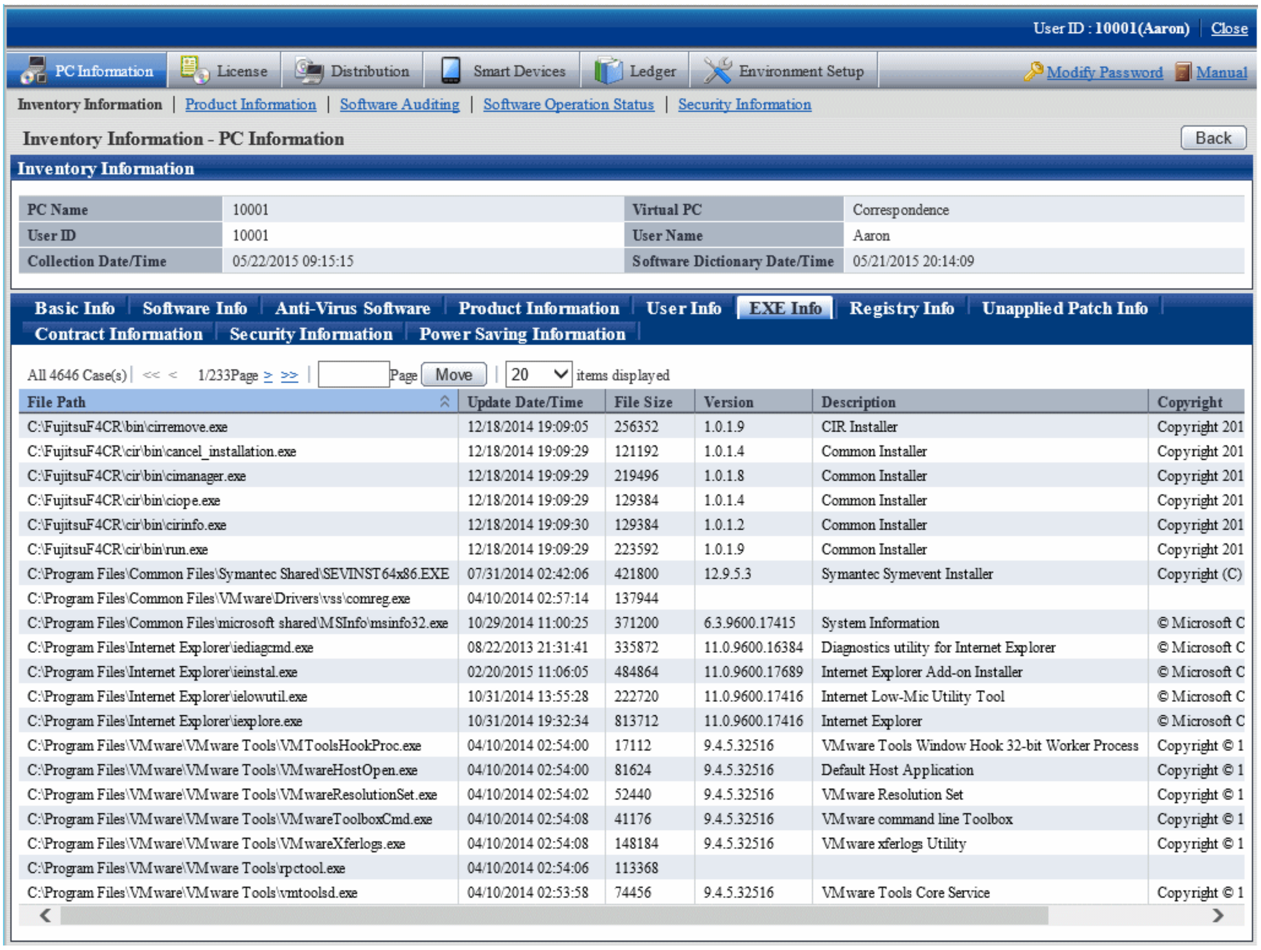
Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/15/2015 10:14:52	Software Dictionary Date/Time	05/14/2015 10:23:36

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	Equipment 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	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 09:15:15	Software Dictionary Date/Time	05/21/2015 20:14:09

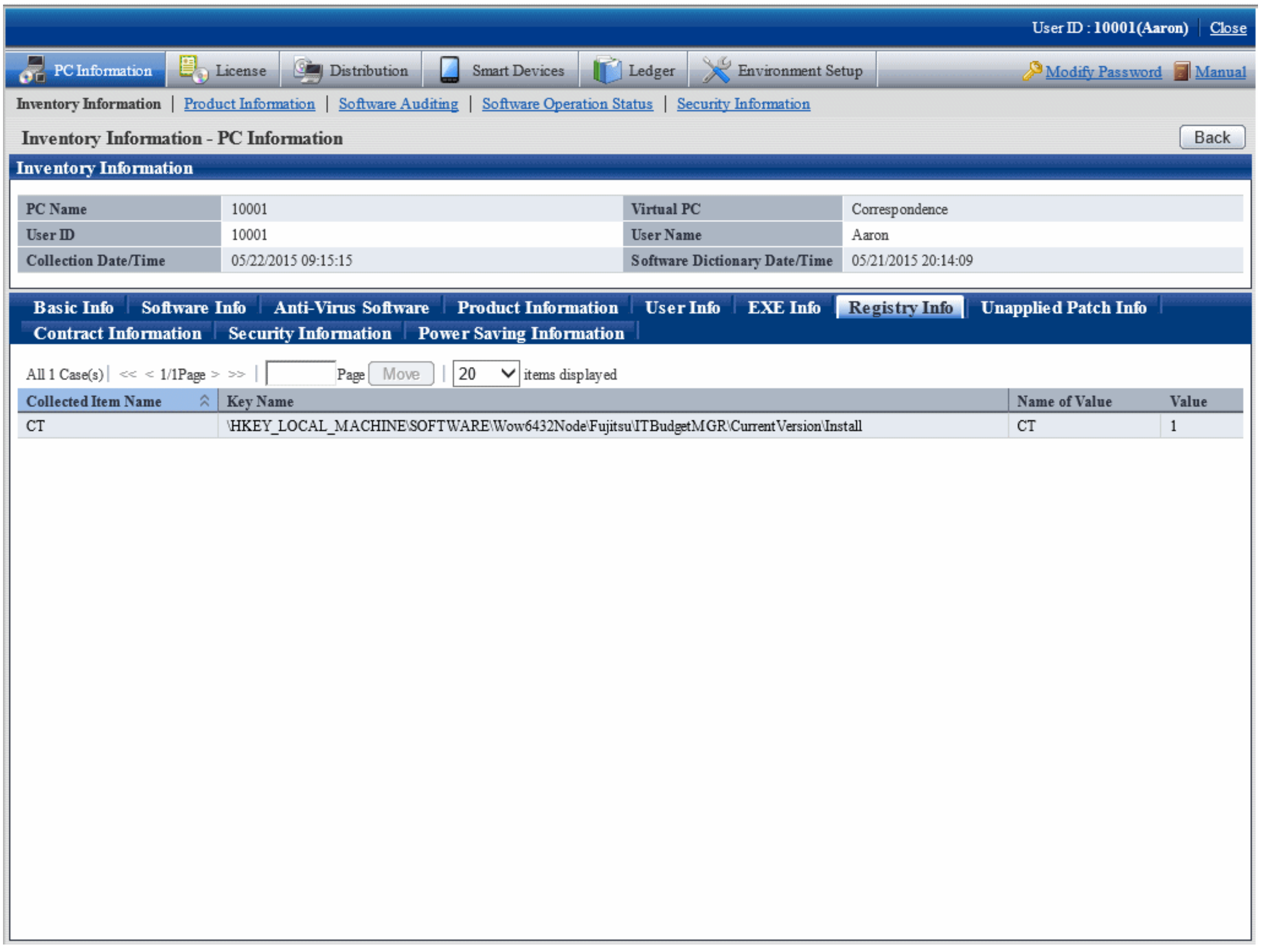
All 4646 Case(s) | 20 items displayed

File Path	Update Date/Time	File Size	Version	Description	Copyright
C:\FujitsuF4CR\bin\cirremove.exe	12/18/2014 19:09:05	256352	1.0.1.9	CIR Installer	Copyright 201
C:\FujitsuF4CR\cir\bin\cancel_installation.exe	12/18/2014 19:09:29	121192	1.0.1.4	Common Installer	Copyright 201
C:\FujitsuF4CR\cir\bin\cimanager.exe	12/18/2014 19:09:29	219496	1.0.1.8	Common Installer	Copyright 201
C:\FujitsuF4CR\cir\bin\ciope.exe	12/18/2014 19:09:29	129384	1.0.1.4	Common Installer	Copyright 201
C:\FujitsuF4CR\cir\bin\cirinfo.exe	12/18/2014 19:09:30	129384	1.0.1.2	Common Installer	Copyright 201
C:\FujitsuF4CR\cir\bin\run.exe	12/18/2014 19:09:29	223592	1.0.1.9	Common Installer	Copyright 201
C:\Program Files\Common Files\Symantec Shared\SEVINST64x86.EXE	07/31/2014 02:42:06	421800	12.9.5.3	Symantec Symevent Installer	Copyright (C)
C:\Program Files\Common Files\VMware\Drivers\vss\comreg.exe	04/10/2014 02:57:14	137944			
C:\Program Files\Common Files\microsoft shared\MSInfo\msinfo32.exe	10/29/2014 11:00:25	371200	6.3.9600.17415	System Information	© Microsoft C
C:\Program Files\Internet Explorer\iediagcmd.exe	08/22/2013 21:31:41	335872	11.0.9600.16384	Diagnostics utility for Internet Explorer	© Microsoft C
C:\Program Files\Internet Explorer\ieinstal.exe	02/20/2015 11:06:05	484864	11.0.9600.17689	Internet Explorer Add-on Installer	© Microsoft C
C:\Program Files\Internet Explorer\ielowutil.exe	10/31/2014 13:55:28	222720	11.0.9600.17416	Internet Low-Mic Utility Tool	© Microsoft C
C:\Program Files\Internet Explorer\iexplore.exe	10/31/2014 19:32:34	813712	11.0.9600.17416	Internet Explorer	© Microsoft C
C:\Program Files\VMware\VMware Tools\VMToolsHookProc.exe	04/10/2014 02:54:00	17112	9.4.5.32516	VMware Tools Window Hook 32-bit Worker Process	Copyright © 1
C:\Program Files\VMware\VMware Tools\VMwareHostOpen.exe	04/10/2014 02:54:00	81624	9.4.5.32516	Default Host Application	Copyright © 1
C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe	04/10/2014 02:54:02	52440	9.4.5.32516	VMware Resolution Set	Copyright © 1
C:\Program Files\VMware\VMware Tools\VMwareToolboxCmd.exe	04/10/2014 02:54:08	41176	9.4.5.32516	VMware command line Toolbox	Copyright © 1
C:\Program Files\VMware\VMware Tools\VMwareXferlogs.exe	04/10/2014 02:54:08	148184	9.4.5.32516	VMware xferlogs Utility	Copyright © 1
C:\Program Files\VMware\VMware Tools\rpctool.exe	04/10/2014 02:54:06	113368			
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	04/10/2014 02:53:58	74456	9.4.5.32516	VMware Tools Core Service	Copyright © 1

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:


User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Product Information | Software Auditing | Software Operation Status | Security Information
Back
Basic Info | Software Info | Anti-Virus Software | Product Information | User Info | EXE Info | Registry Info | Unapplied Patch Info
Contract Information | Security Information | Power Saving Information
All 1 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Inventory Information - PC Information

Inventory Information

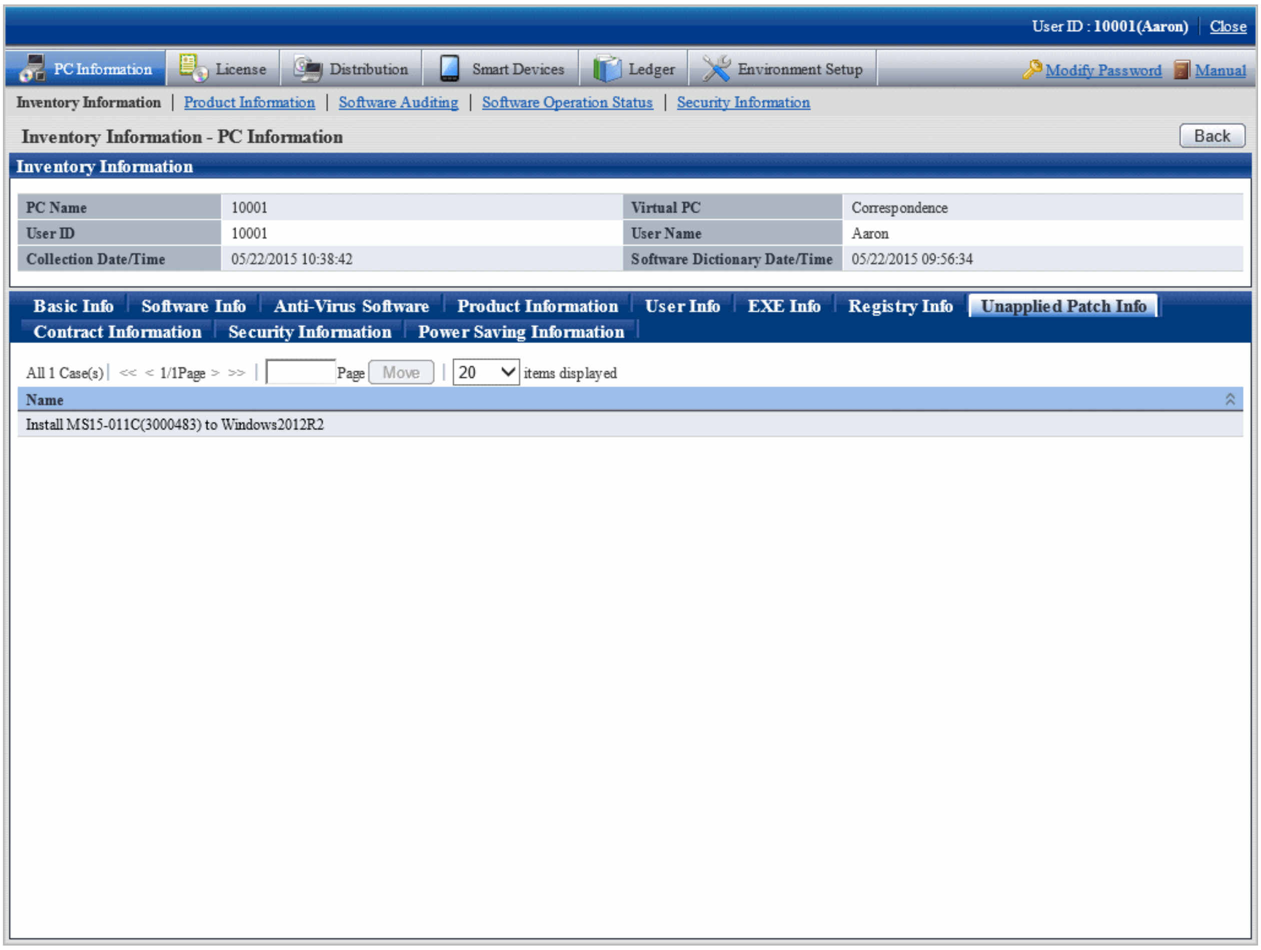
PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 09:15:15	Software Dictionary Date/Time	05/21/2015 20:14:09

Collected Item Name	Key Name	Name of Value	Value
CT	\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\ITBudgetMGR\CurrentVersion\Install	CT	1

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:



Inventory Information - PC Information

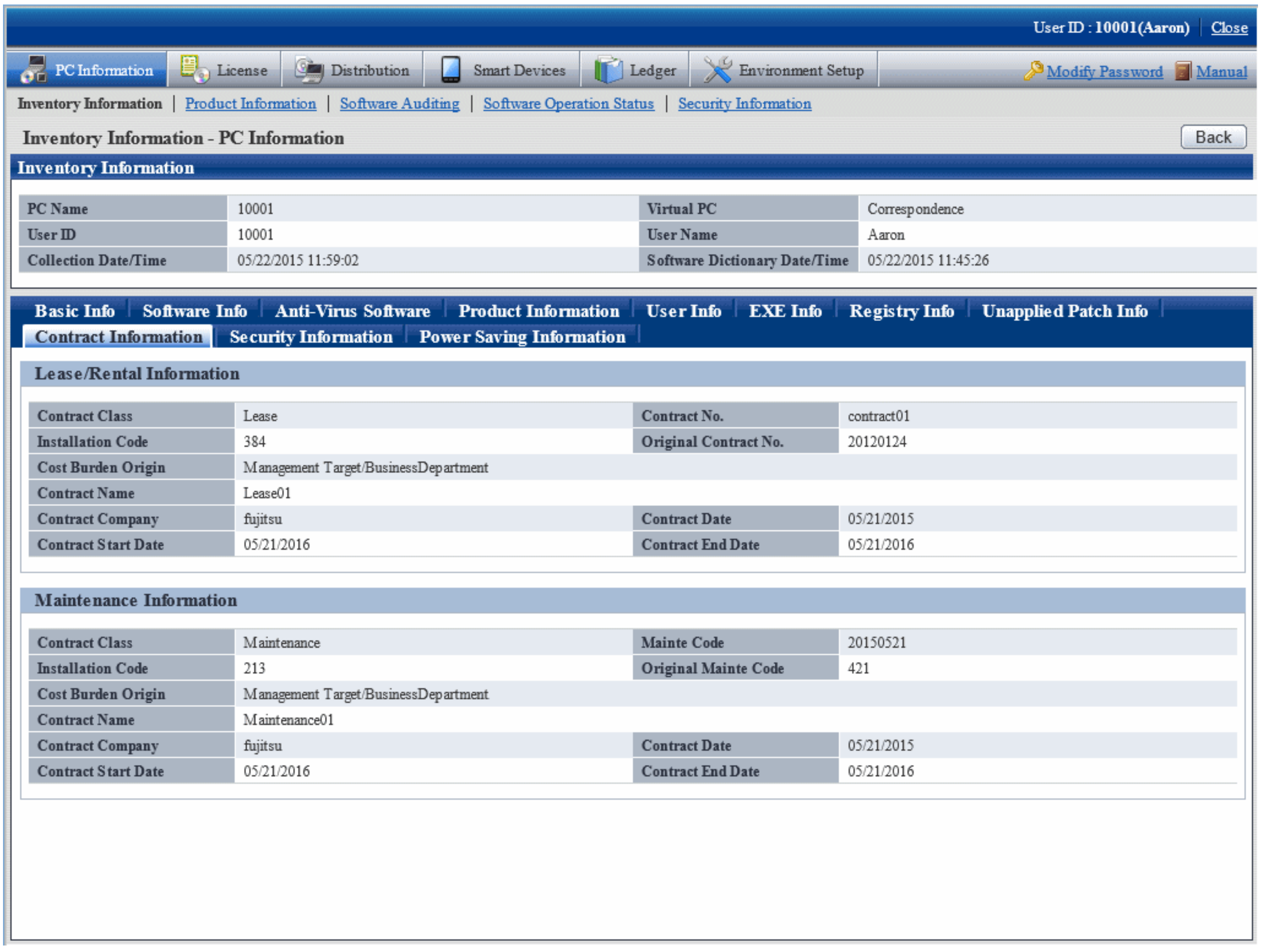
Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 10:38:42	Software Dictionary Date/Time	05/22/2015 09:56:34

Name
Install MS15-011C(3000483) to Windows2012R2

Contract information

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



Inventory Information - PC Information

Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/22/2015 11:59:02	Software Dictionary Date/Time	05/22/2015 11:45:26

Lease/Rental Information

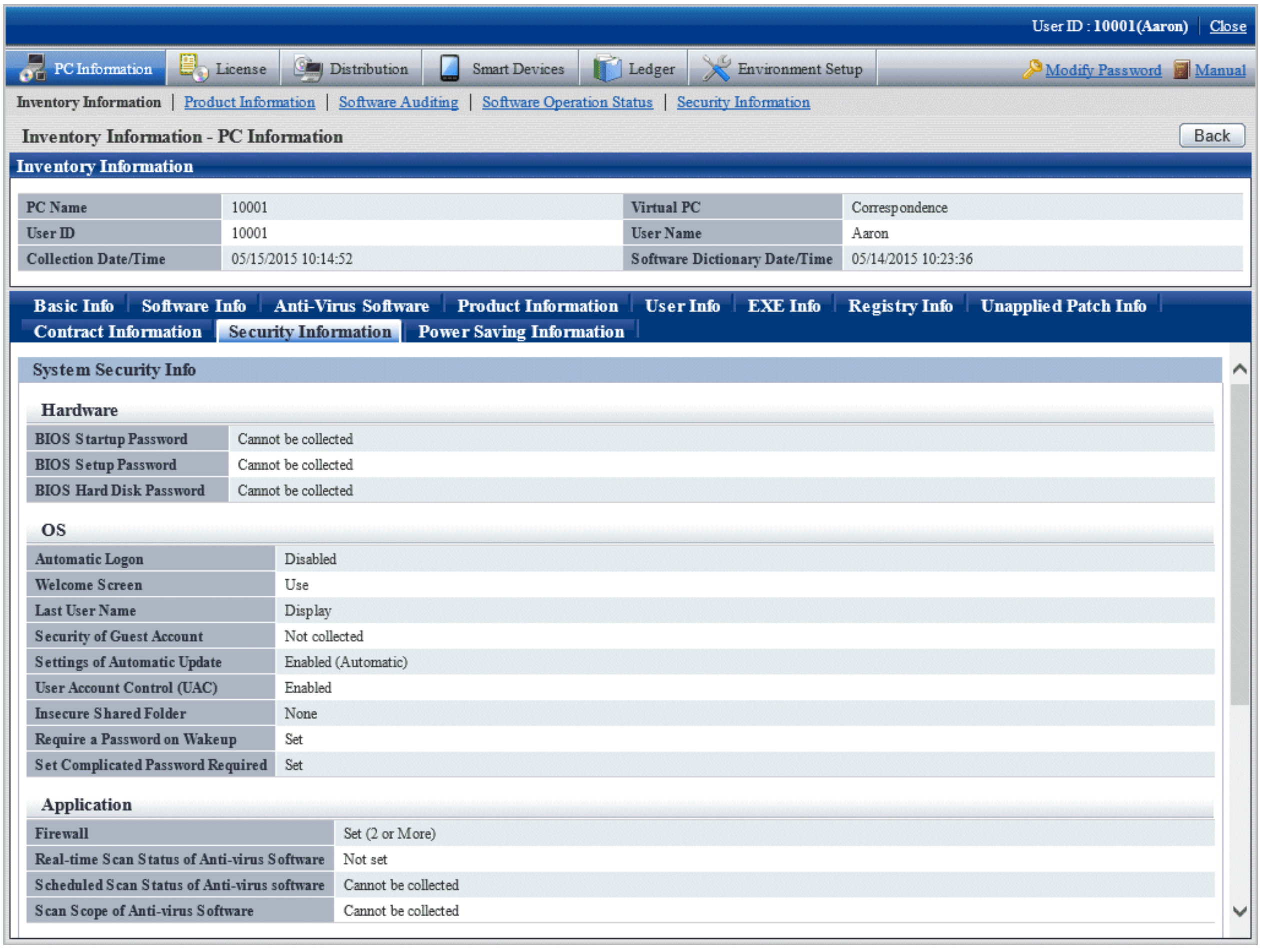
Contract Class	Lease	Contract No.	contract01
Installation Code	384	Original Contract No.	20120124
Cost Burden Origin	Management Target/BusinessDepartment		
Contract Name	Lease01		
Contract Company	fujitsu	Contract Date	05/21/2015
Contract Start Date	05/21/2016	Contract End Date	05/21/2016

Maintenance Information

Contract Class	Maintenance	Mainte Code	20150521
Installation Code	213	Original Mainte Code	421
Cost Burden Origin	Management Target/BusinessDepartment		
Contract Name	Maintenance01		
Contract Company	fujitsu	Contract Date	05/21/2015
Contract Start Date	05/21/2016	Contract End Date	05/21/2016

Security information

The user can browse the security information of the PC.



Inventory Information - PC Information

Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/15/2015 10:14:52	Software Dictionary Date/Time	05/14/2015 10:23:36

System Security Info

Hardware

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

OS

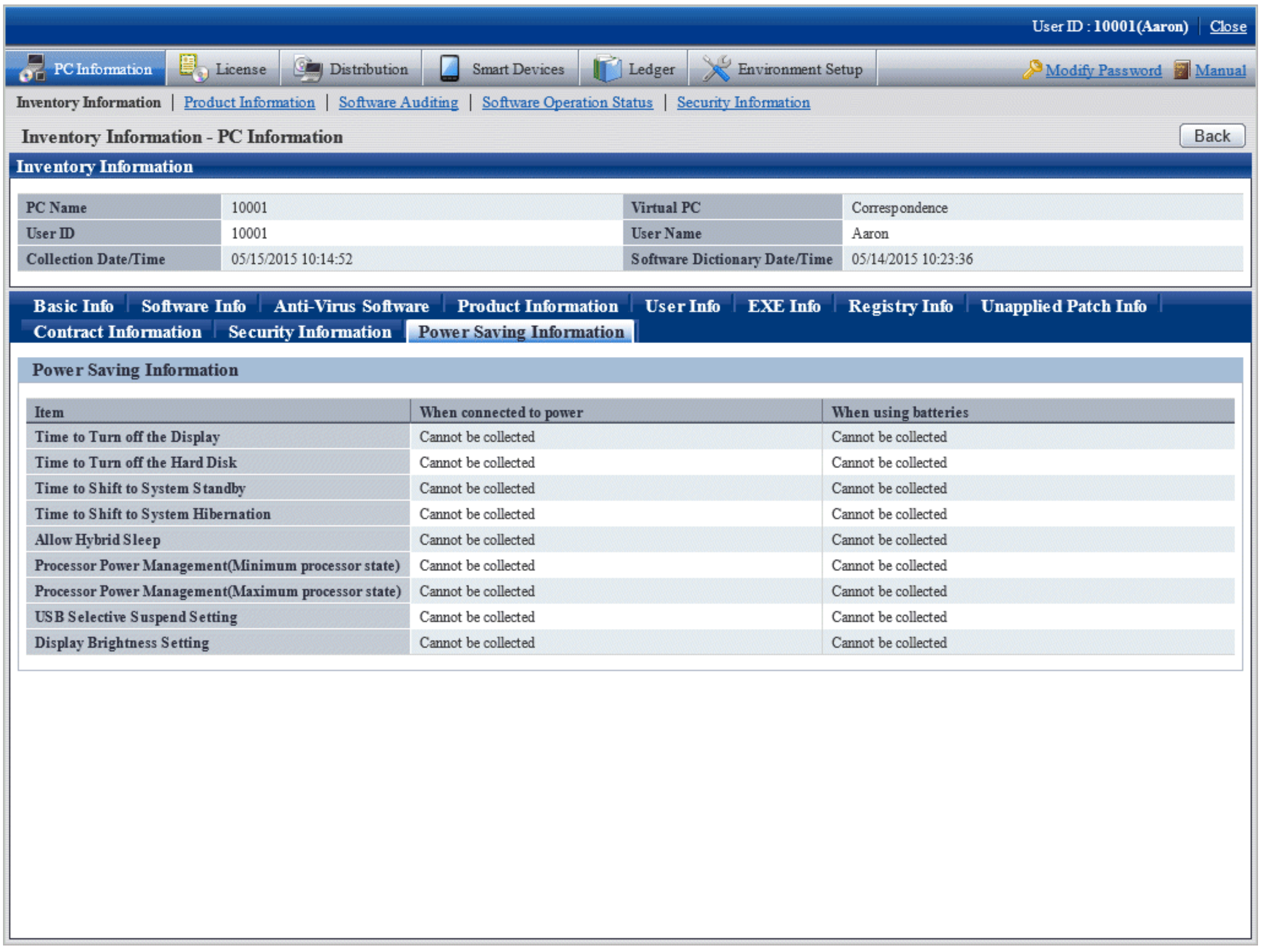
Automatic Logon	Disabled
Welcome Screen	Use
Last User Name	Display
Security of Guest Account	Not collected
Settings of Automatic Update	Enabled (Automatic)
User Account Control (UAC)	Enabled
Insecure Shared Folder	None
Require a Password on Wakeup	Set
Set Complicated Password Required	Set

Application

Firewall	Set (2 or More)
Real-time Scan Status of Anti-virus Software	Not set
Scheduled Scan Status of Anti-virus software	Cannot be collected
Scan Scope of Anti-virus Software	Cannot be collected

Power saving information

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



User ID : 10001(Aaron) | Close

Inventory Information - PC Information

Inventory Information

PC Name	10001	Virtual PC	Correspondence
User ID	10001	User Name	Aaron
Collection Date/Time	05/15/2015 10:14:52	Software Dictionary Date/Time	05/14/2015 10:23:36

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 Product Information

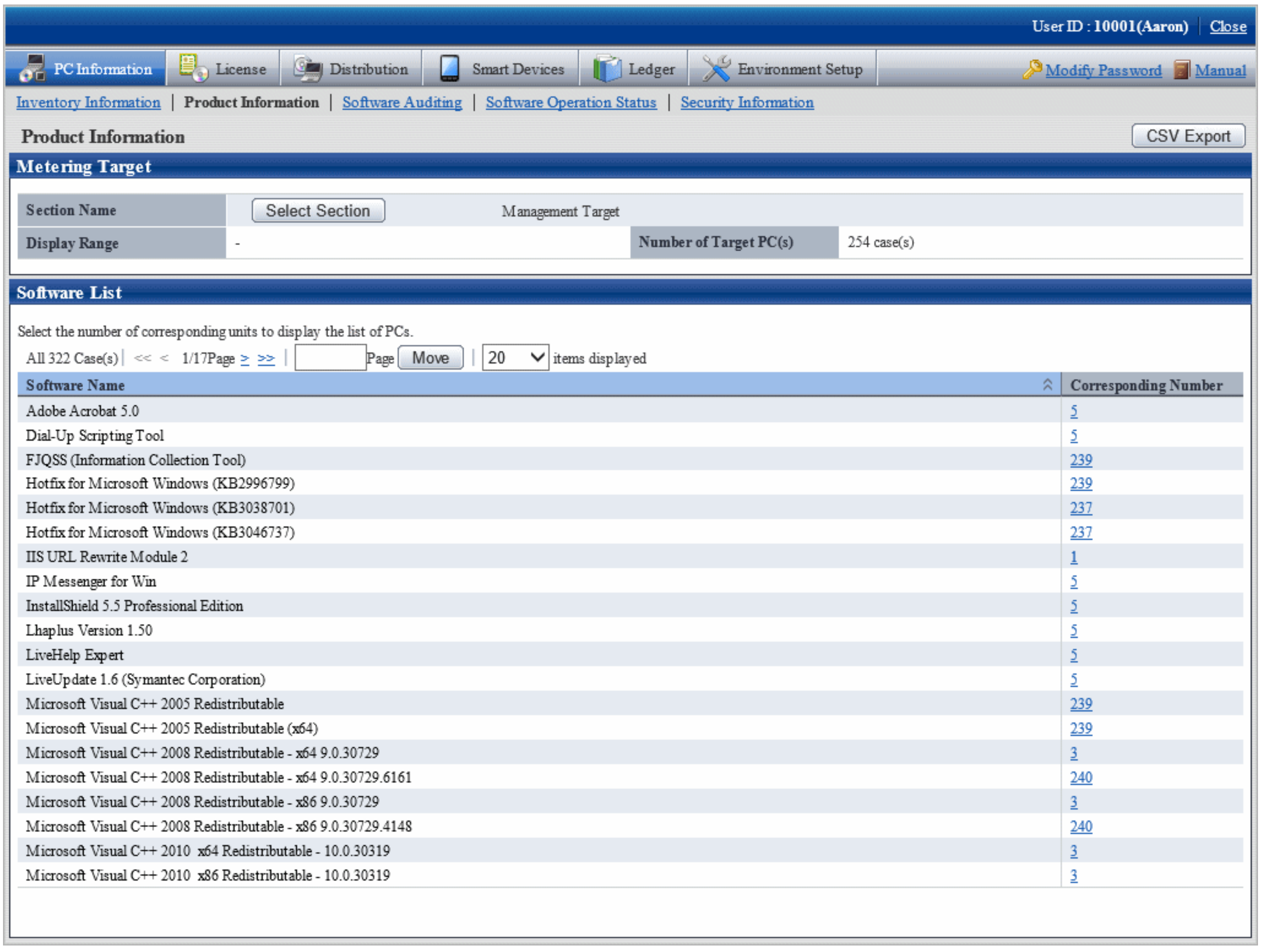
Automatically collect the list of the software displayed in **Uninstall a program** and **View installed updates** in **Add or Remove Programs** or **Programs and Features**.

The information will be used when performing license management.

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

The product information is displayed in the **PC Information** > **Product Information** window of main menu.

The display picture is shown below:



Product Information

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Target PC(s)	254 case(s)

Software List

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

All 322 Case(s) | << < 1/17Page > >> | Page Move | 20 items displayed

Software Name	Corresponding Number
Adobe Acrobat 5.0	5
Dial-Up Scripting Tool	5
FJQSS (Information Collection Tool)	239
Hotfix for Microsoft Windows (KB2996799)	239
Hotfix for Microsoft Windows (KB3038701)	237
Hotfix for Microsoft Windows (KB3046737)	237
IIS URL Rewrite Module 2	1
IP Messenger for Win	5
InstallShield 5.5 Professional Edition	5
Lhaplus Version 1.50	5
LiveHelp Expert	5
LiveUpdate 1.6 (Symantec Corporation)	5
Microsoft Visual C++ 2005 Redistributable	239
Microsoft Visual C++ 2005 Redistributable (x64)	239
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729	3
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	240
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729	3
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	240
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319	3
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	3

Note

If program information is not collected

If the version of Windows Installer 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 PCs on which security patches from Microsoft Corporation have not been installed are not applied can be found.

The PCs on which computer anti-virus software is not installed can be found.

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

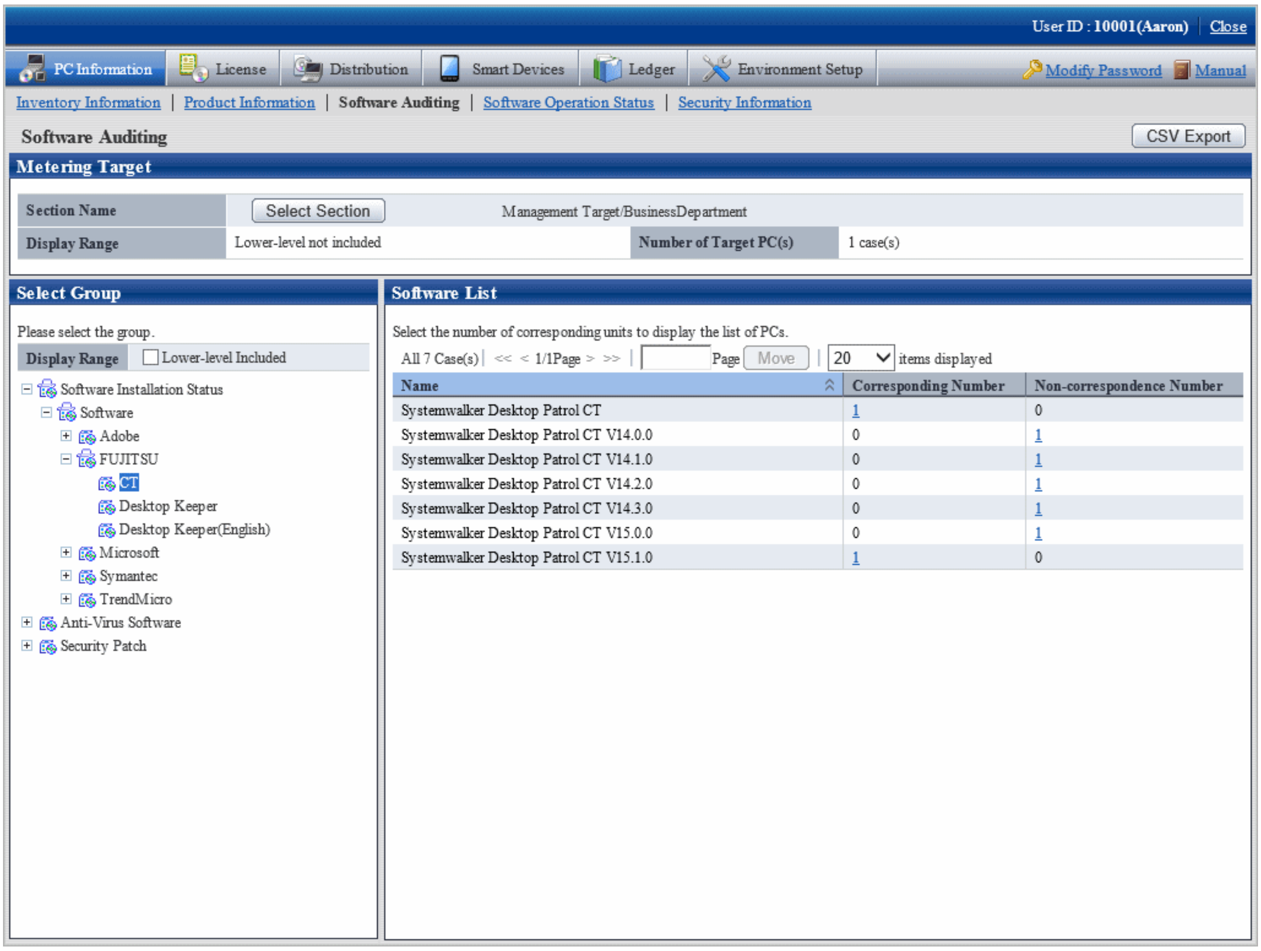
The administrator can find the PC in which potential computer virus and security breaches exist to improve the protective capability of the PC.

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.



Section Name	Select Section	Management Target/BusinessDepartment	
Display Range	Lower-level not included	Number of Target PC(s)	1 case(s)

Please select the group.

Display Range □ Lower-level Included

- Software Installation Status
  - Software
    - Adobe
    - FUJITSU
      - CT
      - Desktop Keeper
      - Desktop Keeper(English)
    - Microsoft
    - Symantec
    - TrendMicro
  - Anti-Virus Software
  - Security Patch

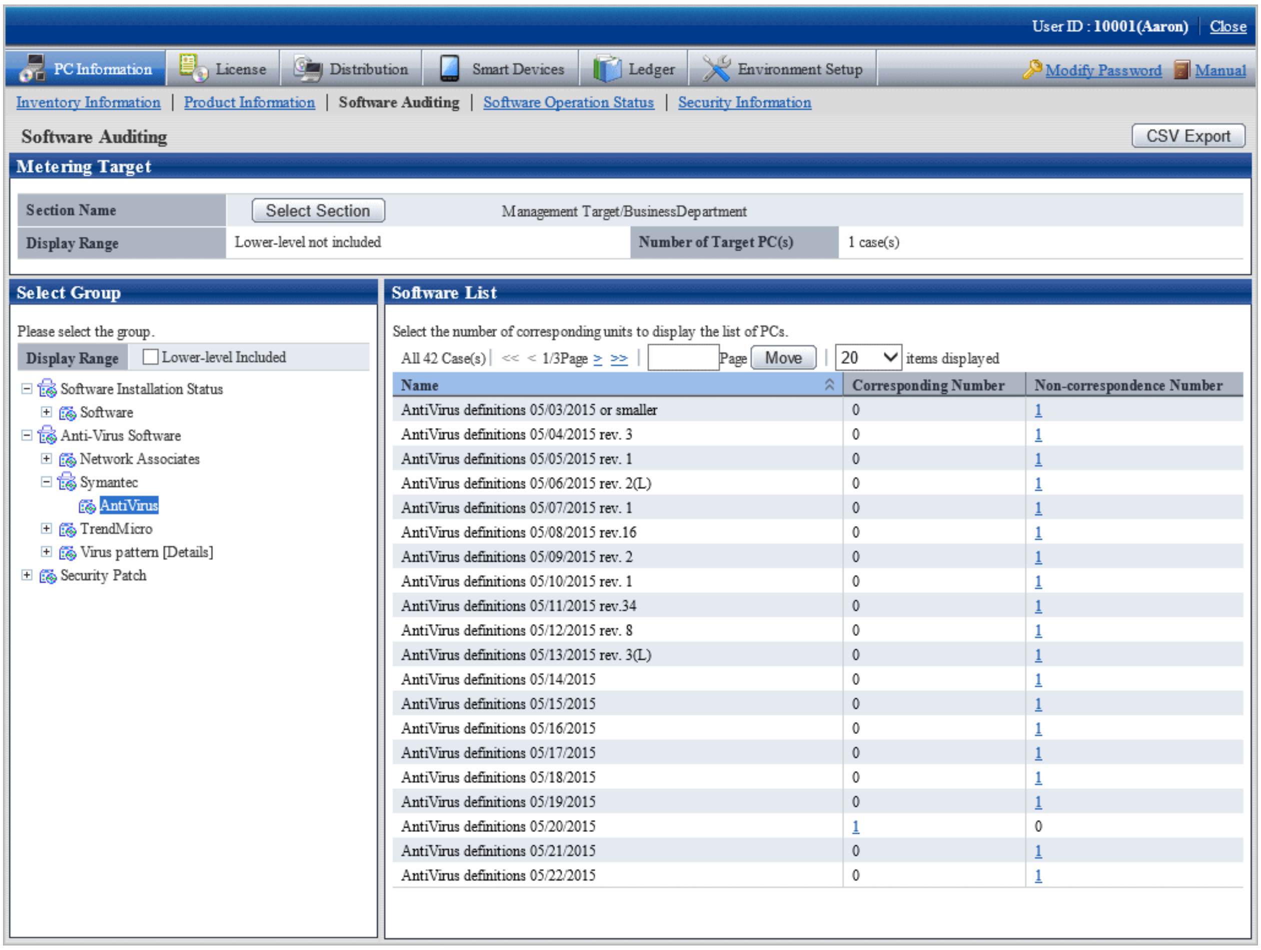
Select the number of corresponding units to display the list of PCs.

All 7 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Name	Corresponding Number	Non-correspondence Number
Systemwalker Desktop Patrol CT	1	0
Systemwalker Desktop Patrol CT V14.0.0	0	1
Systemwalker Desktop Patrol CT V14.1.0	0	1
Systemwalker Desktop Patrol CT V14.2.0	0	1
Systemwalker Desktop Patrol CT V14.3.0	0	1
Systemwalker Desktop Patrol CT V15.0.0	0	1
Systemwalker Desktop Patrol CT V15.1.0	1	0

Installation status of anti-virus software

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



User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Product Information | Software Auditing | Software Operation Status | Security Information
CSV Export
Select Section
Move

Software Auditing

Metering Target

Section Name	Select Section Management Target/BusinessDepartment		
Display Range	Lower-level not included	Number of Target PC(s)	1 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

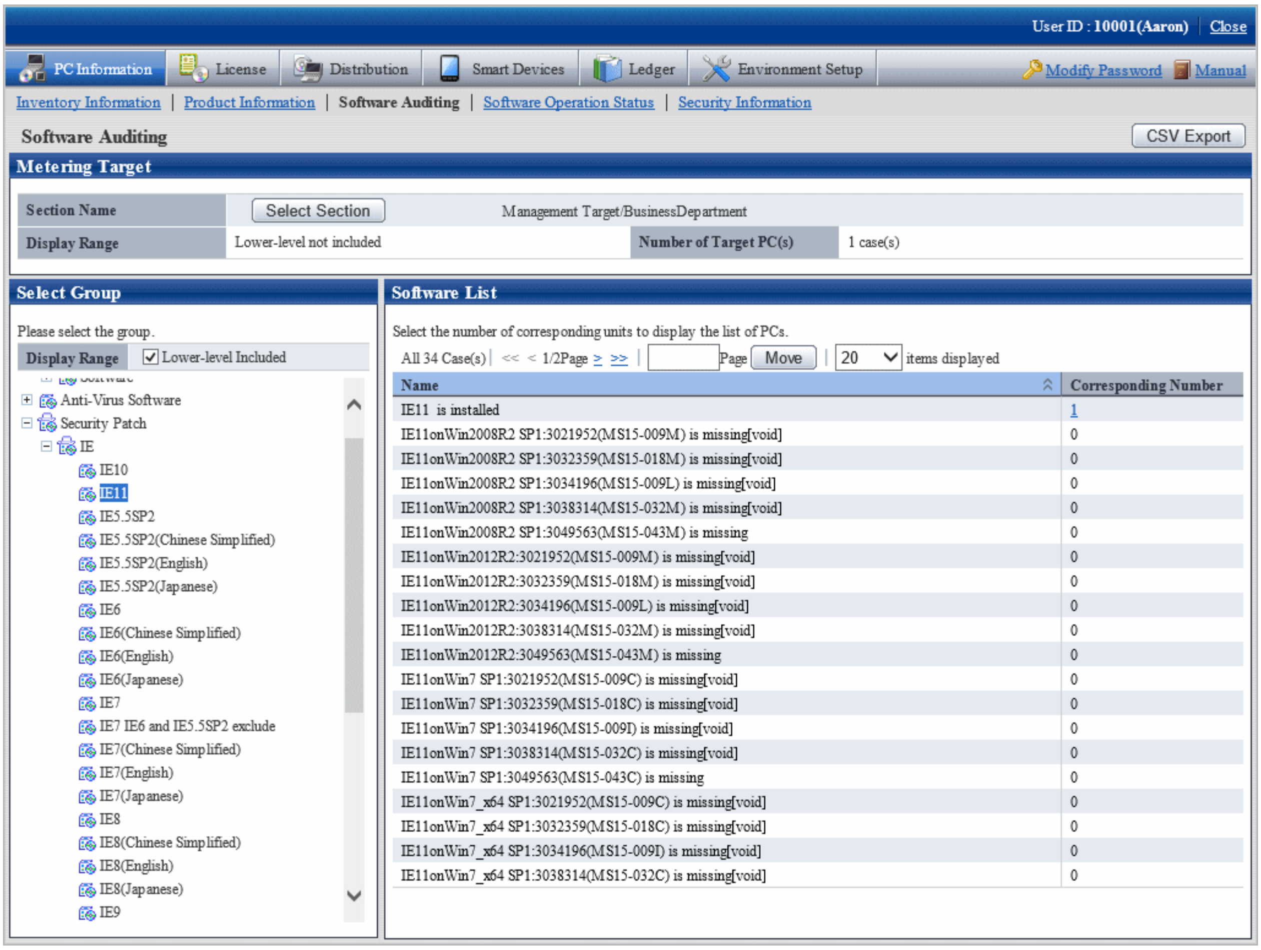
Select the number of corresponding units to display the list of PCs.

All 42 Case(s) | << < 1/3Page > >> | Page Move | 20 items displayed

Name	Corresponding Number	Non-correspondence Number
AntiVirus definitions 05/03/2015 or smaller	0	1
AntiVirus definitions 05/04/2015 rev. 3	0	1
AntiVirus definitions 05/05/2015 rev. 1	0	1
AntiVirus definitions 05/06/2015 rev. 2(L)	0	1
AntiVirus definitions 05/07/2015 rev. 1	0	1
AntiVirus definitions 05/08/2015 rev.16	0	1
AntiVirus definitions 05/09/2015 rev. 2	0	1
AntiVirus definitions 05/10/2015 rev. 1	0	1
AntiVirus definitions 05/11/2015 rev.34	0	1
AntiVirus definitions 05/12/2015 rev. 8	0	1
AntiVirus definitions 05/13/2015 rev. 3(L)	0	1
AntiVirus definitions 05/14/2015	0	1
AntiVirus definitions 05/15/2015	0	1
AntiVirus definitions 05/16/2015	0	1
AntiVirus definitions 05/17/2015	0	1
AntiVirus definitions 05/18/2015	0	1
AntiVirus definitions 05/19/2015	0	1
AntiVirus definitions 05/20/2015	1	0
AntiVirus definitions 05/21/2015	0	1
AntiVirus definitions 05/22/2015	0	1

Usage status of security patches

The usage status of security patches can be browsed.


User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
Inventory Information | Product Information | Software Auditing | Software Operation Status | Security Information
CSV Export
Select Section
Move

Software Auditing

Metering Target

Section Name	Select Section Management Target/BusinessDepartment		
Display Range	Lower-level not included	Number of Target PC(s)	1 case(s)

Select Group

Please select the group.

Display Range ☑ Lower-level Included

- Software
- Anti-Virus Software
- Security Patch
  - IE
    - IE10
    - IE11
    - IE5.5SP2
    - IE5.5SP2(Chinese Simplified)
    - IE5.5SP2(English)
    - IE5.5SP2(Japanese)
    - IE6
    - IE6(Chinese Simplified)
    - IE6(English)
    - IE6(Japanese)
    - IE7
    - IE7 IE6 and IE5.5SP2 exclude
    - IE7(Chinese Simplified)
    - IE7(English)
    - IE7(Japanese)
    - IE8
    - IE8(Chinese Simplified)
    - IE8(English)
    - IE8(Japanese)
    - IE9

Software List

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

All 34 Case(s) | << < 1/2Page > >> | Page Move | 20 items displayed

Name	Corresponding Number
IE11 is installed	1
IE11onWin2008R2 SP1:3021952(MS15-009M) is missing[void]	0
IE11onWin2008R2 SP1:3032359(MS15-018M) is missing[void]	0
IE11onWin2008R2 SP1:3034196(MS15-009L) is missing[void]	0
IE11onWin2008R2 SP1:3038314(MS15-032M) is missing[void]	0
IE11onWin2008R2 SP1:3049563(MS15-043M) is missing	0
IE11onWin2012R2:3021952(MS15-009M) is missing[void]	0
IE11onWin2012R2:3032359(MS15-018M) is missing[void]	0
IE11onWin2012R2:3034196(MS15-009L) is missing[void]	0
IE11onWin2012R2:3038314(MS15-032M) is missing[void]	0
IE11onWin2012R2:3049563(MS15-043M) is missing	0
IE11onWin7 SP1:3021952(MS15-009C) is missing[void]	0
IE11onWin7 SP1:3032359(MS15-018C) is missing[void]	0
IE11onWin7 SP1:3034196(MS15-009D) is missing[void]	0
IE11onWin7 SP1:3038314(MS15-032C) is missing[void]	0
IE11onWin7 SP1:3049563(MS15-043C) is missing	0
IE11onWin7_x64 SP1:3021952(MS15-009C) is missing[void]	0
IE11onWin7_x64 SP1:3032359(MS15-018C) is missing[void]	0
IE11onWin7_x64 SP1:3034196(MS15-009D) is missing[void]	0
IE11onWin7_x64 SP1:3038314(MS15-032C) is missing[void]	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".

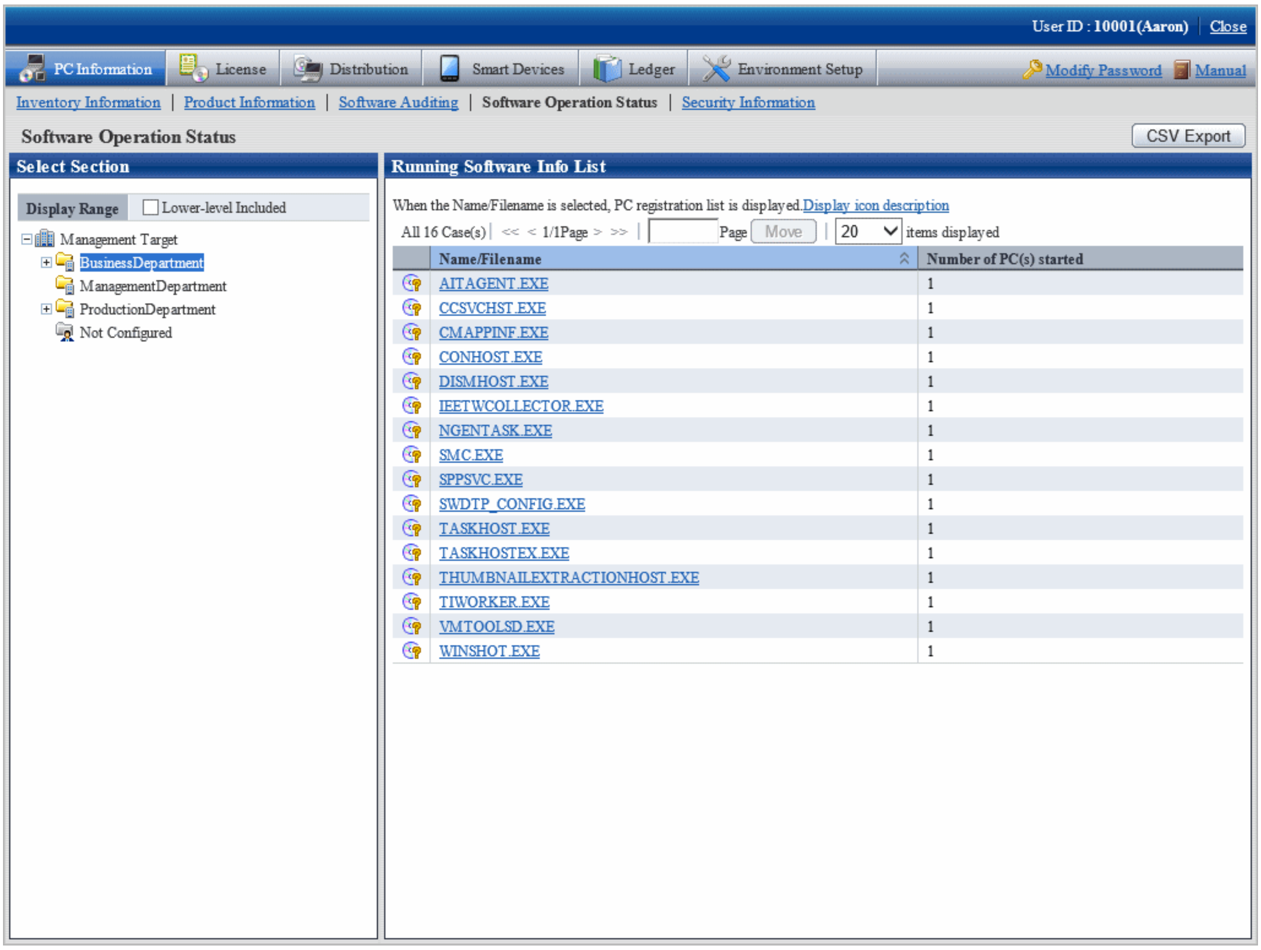
Effective utilization of assets can be realized through browsing the software operation status. For example, although license has been distributed and software has been installed, if software is not applied, dormant assets can be reduced by distributing the License to other users in need.

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

Software operation status cannot 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.

Name/Filename	Number of PC(s) started
AITAGENT.EXE	1
CCSVCHST.EXE	1
CMAPPINF.EXE	1
CONHOST.EXE	1
DISMHOST.EXE	1
IEETWCOLLECTOR.EXE	1
NGENTASK.EXE	1
SMC.EXE	1
SPPSVC.EXE	1
SWDTP_CONFIG.EXE	1
TASKHOST.EXE	1
TASKHOSTEX.EXE	1
THUMBNAILEXTRACTIONHOST.EXE	1
TIWORKER.EXE	1
VMTOOLSD.EXE	1
WINSHOT.EXE	1

Note

The following EXE files cannot 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 cannot be browsed.

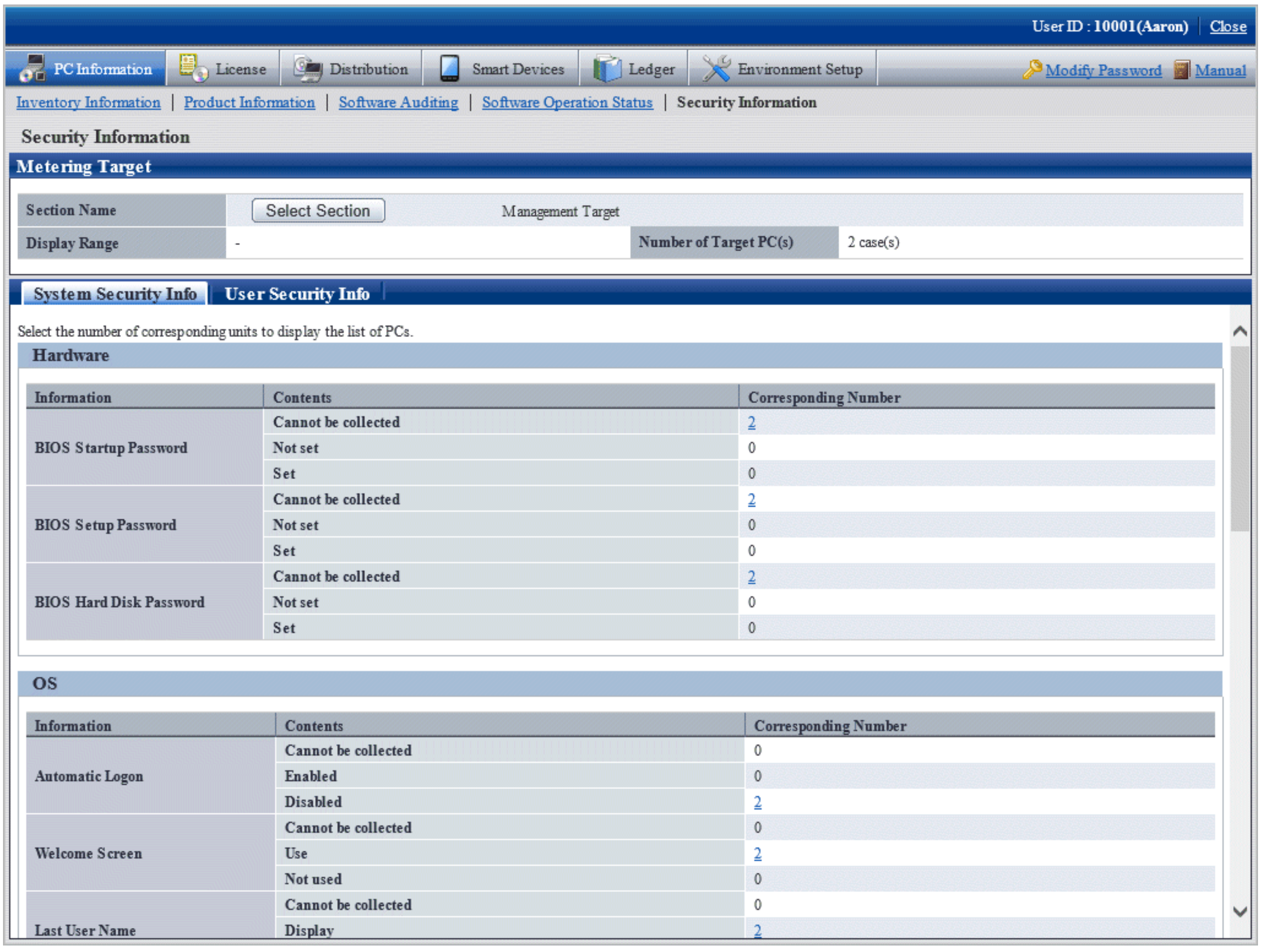
Collectable security information (system security information and user security information) and confirmable items may be variable with different OS.

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



User ID : 10001(Aaron) | Close

PC Information | License | Distribution | Smart Devices | Ledger | Environment Setup | Modify Password | Manual

Inventory Information | Product Information | Software Auditing | Software Operation Status | Security Information

Security Information

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Target PC(s)	2 case(s)

System Security Info | User Security Info

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

Hardware

Information	Contents	Corresponding Number
BIOS Startup Password	Cannot be collected	2
	Not set	0
	Set	0
BIOS Setup Password	Cannot be collected	2
	Not set	0
	Set	0
BIOS Hard Disk Password	Cannot be collected	2
	Not set	0
	Set	0

OS

Information	Contents	Corresponding Number
Automatic Logon	Cannot be collected	0
	Enabled	0
	Disabled	2
Welcome Screen	Cannot be collected	0
	Use	2
	Not used	0
Last User Name	Cannot be collected	0
	Display	2

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

Class	Information	Collectable						
		Vista	Vista 64bit	7/8	7 64bit/ 8 64bit	2008	2008 64bit/ 2012	Remarks
Hardware (Note 1)	**BIOS Startup password**	D	D	D	D	D	D	
	BIOS Setup Password	D	D	D	D	D	D	
	BIOS Hard Disk Password	D	D	D	D	D	D	

Class	Information	Collectable						
		Vista	Vista 64bit	7/8	7 64bit/ 8 64bit	2008	2008 64bit/ 2012	Remarks
OS	**Automatic Logon**	Y	Y	Y	Y	Y	Y	
	Welcome Screen	Y	Y	Y	Y	Y	Y	In operating systems other than Windows Server(R) 2008, it must be set as "Displayed".
	Last User Name	Y	Y	Y	Y	Y	Y	
	Security of Guest Account	Y	Y	Y	Y	Y	Y	
	Settings of Automatic Update	Y	Y	Y	Y	Y	Y	
	User Account Control (UAC)	Y	Y	Y	Y	Y	Y	
	Insecure Shared Folder	Y	Y	Y	Y	Y	Y	
	Require a Password on Wakeup	Y	Y	Y	Y	Y	Y	
	Set Complicated Password Required	Y	Y	Y	Y	Y	Y	
Applicatio n	**Firewall** (Note 2)	Y	Y	Y	Y	Y	Y	
	Real-time Scan Status of Anti-virus Software (Note 3)	Y	Y	Y	Y	Y	Y	
	Scheduled Scan Status of Anti-virus software (Note 4)	Y	Y	Y	Y	Y	Y	
	Scan Scope of Anti-virus Software (Note 5)	Y	Y	Y	Y	Y	Y	

Y: Collectable

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

U: Uncollected or no corresponding information

Vista: Windows Vista(R)

Vista 64bit: Windows Vista(R) x64 Edition

7: Windows(R) 7

7 64bit: Windows(R) 7 x64 Edition

8: Windows(R) 8

8 64bit: Windows(R) 8 x64 Edition

2008: Windows Server(R) 2008

2008 64bit: Windows Server(R) 2008 x64 Edition

2012: Windows Server(R) 2012

Refer to "3.2.1 Operating System" for details on each Service Pack of the operating systems above that are supported in Systemwalker Desktop Patrol.

Note 1:

Information collection may be impossible due to different types of devices. If information cannot be collected, it shall be set as "Cannot be collected".

Also, the BIOS hard disk password will be "Cannot be collected" if the command mode CT is not executed with the administrator privileges.

Note 2:

The notation for each product's firewall function is shown below, but in this document, they are collectively referred to as "Firewall".

- Microsoft Windows: "Windows Firewall"
- Trend Micro Virus Buster: "Personal Firewall"
- McAfee VirusScan: "Port Blocking"

Note 3:

The notation for each anti-virus software's real-time scan feature is shown below, but in this document, they are all referred to as "real-time inspection".

- Trend Micro Virus Buster: "Real-Time Scan"
- McAfee VirusScan: "On Access Scanner"

Note 4:

The notation for each anti-virus software's scheduled scan feature is shown below, but in this document, they are all referred to as "timing scan status".

- Trend Micro Virus Buster: "Scheduled Scans"
- McAfee VirusScan: "On-Demand Scan"

Note 5:

The notation for each anti-virus software's scan target range is shown below, but in this document, they are all referred to as "scan object range".

- Trend Micro Virus Buster: "Files scanned"
- McAfee VirusScan: "Scan items"

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

February, 2015

Manufacturer	Product Name	Version	Auditable			
			Firewall	Real-time Inspection	Timing scan status	Scan Object Range
Microsoft(R)	Windows Vista(R)	Without, SP1, SP2	Y	N	N	N
	Windows(R) 7	Without, SP1	Y	N	N	N
	Windows(R) 8	Without	Y	N	N	N
	Windows(R) 8.1	Without	Y	N	N	N
	Windows Server(R) 2008	Without, SP1, SP2	Y	N	N	N
	Windows Server(R) 2008 R2	Without, SP1	Y	N	N	N
	Windows Server(R) 2012	Without	Y	N	N	N
	Windows Server(R) 2012 R2	Without	Y	N	N	N
TrendMicro	Virus Buster Corporate Edition	Ver10.0, 10.5, 10.6	Y(Note 1)	Y	N	Y
Symantec	Endpoint Protection	12.1 (Note 2)	Y	Y	Y	Y
McAfee	VirusScan Enterprise	8.7i, 8.8	Y	Y	Y	Y

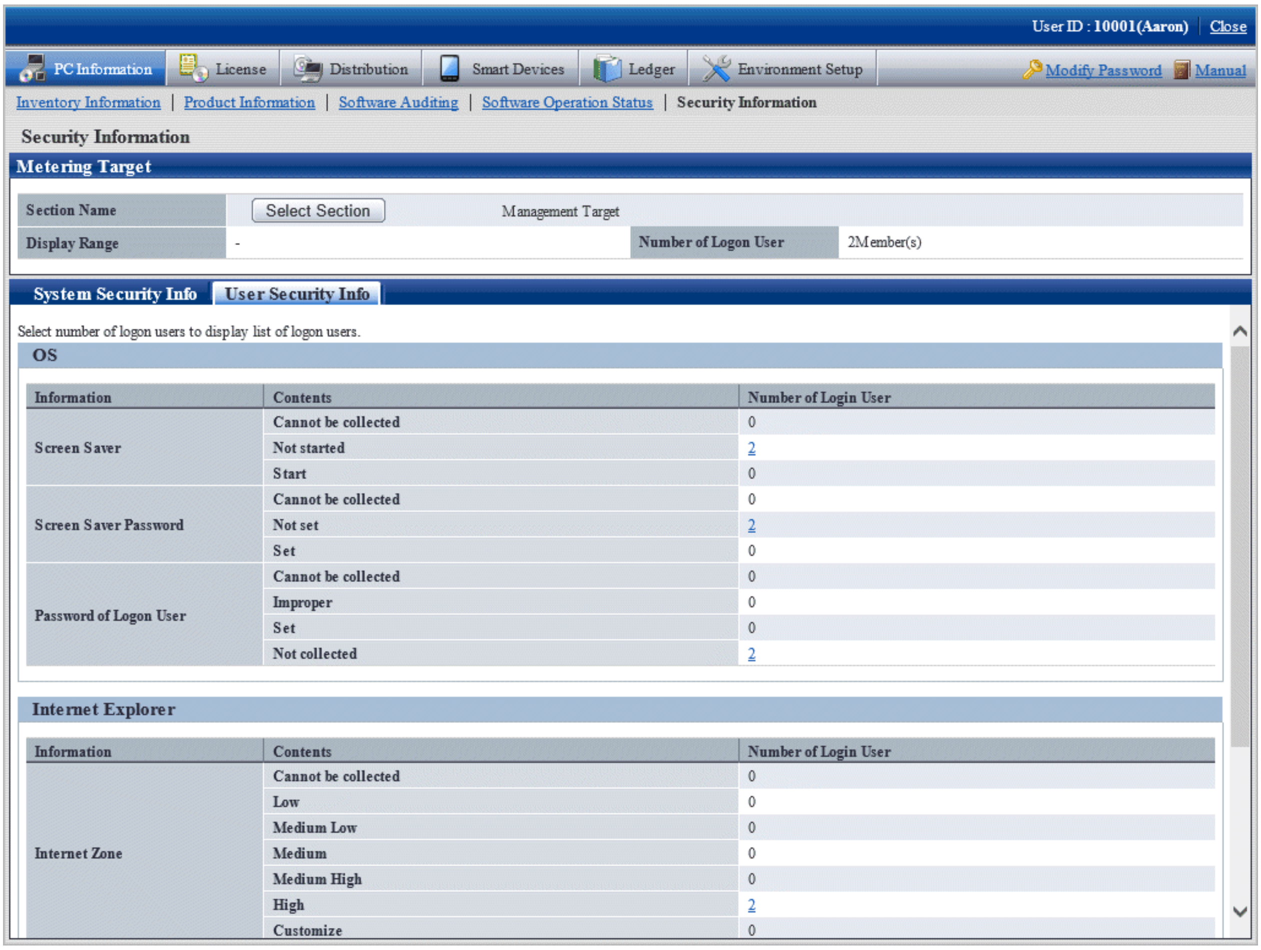
Y: Auditable

N: Not audited or no corresponding function

Note 1: When enabled with a product such as Client/Server Suite Premium(TM) that has a firewall function.

Note 2: Symantec Endpoint Protection 12.1 supports RU1 MP1(12.1.1100) or later.

User security information



Security Information

Metering Target

Section Name	Select Section	Management Target	
Display Range	-	Number of Logon User	2Member(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	2
	Start	0
Screen Saver Password	Cannot be collected	0
	Not set	2
	Set	0
Password of Logon User	Cannot be collected	0
	Improper	0
	Set	0
	Not collected	2

Internet Explorer

Information	Contents	Number of Login User
Internet Zone	Cannot be collected	0
	Low	0
	Medium Low	0
	Medium	0
	Medium High	0
	High	2
	Customize	0

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

Class	Information	Collectable						
		Vista	Vista 64bit	7/8	7 64bit/ 8 64bit	2008	2008 64bit/ 2012	Note
OS	**Screen Saver**	Y	Y	Y	Y	Y	Y	
	Time until the screen saver starts up	Y	Y	Y	Y	Y	Y	
	Screen Saver Password	Y	Y	Y	Y	Y	Y	
	Password of Logon User	Y	Y	Y	Y	Y	Y	
Internet Explorer	**Internet Zone**	Y	Y	Y	Y	Y	Y	
Applicatio n	**Google Desktop [Search Across Computers]**	Y	Y	Y	Y	Y	Y	

Vista: Windows Vista(R)

Vista 64bit: Windows Vista(R) x64 Edition

7: Windows(R) 7

7 64bit: Windows(R) 7 x64 Edition

8: Windows(R) 8

8 64bit: Windows(R) 8 x64 Edition

2008: Windows Server(R) 2008

2008 64bit: Windows Server(R) 2008 x64 Edition

2012: Windows Server(R) 2012

2.1.7 PC Operation Management

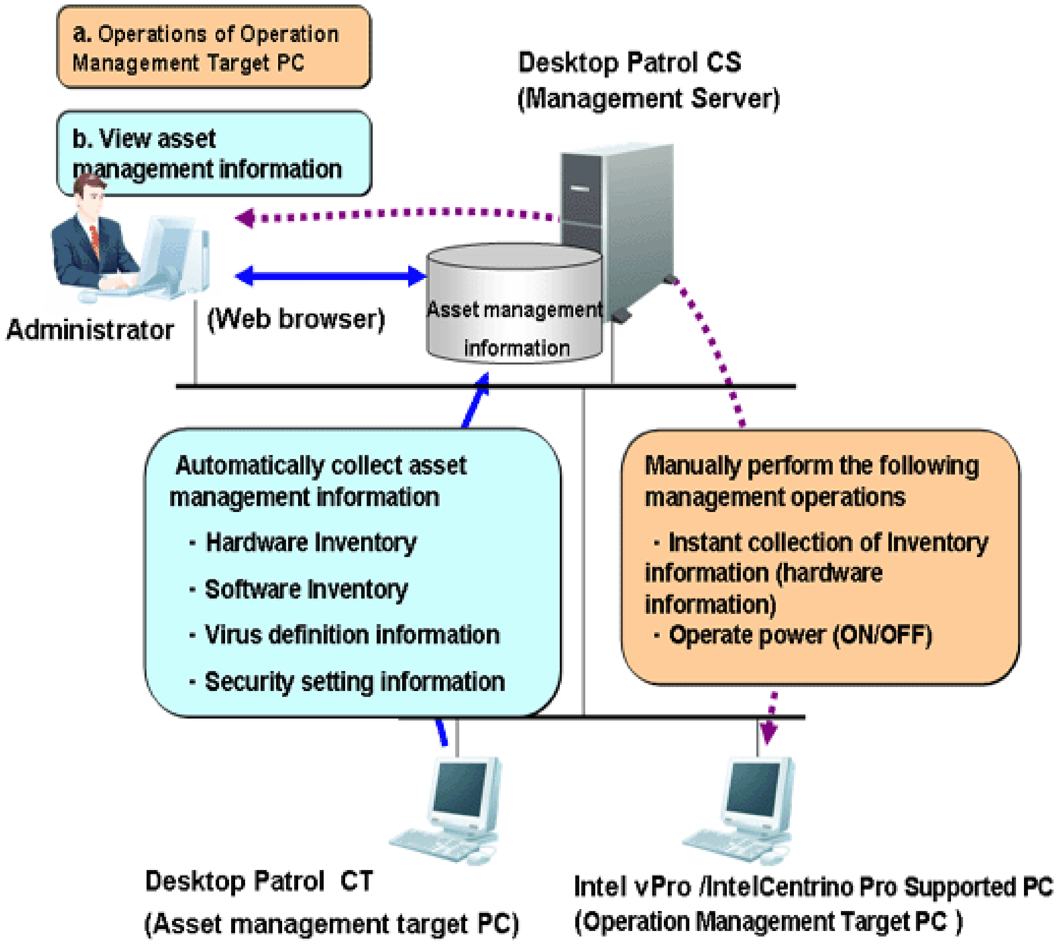
PC operation management function refers to the function to realize the remote control over the PC via Intel(R) AMT (CT, management, technology) in Intel(R) vPro(TM) and Intel(R) Centrino(R) Pro technology even though the PC is powered off.

PC operation management functions include:

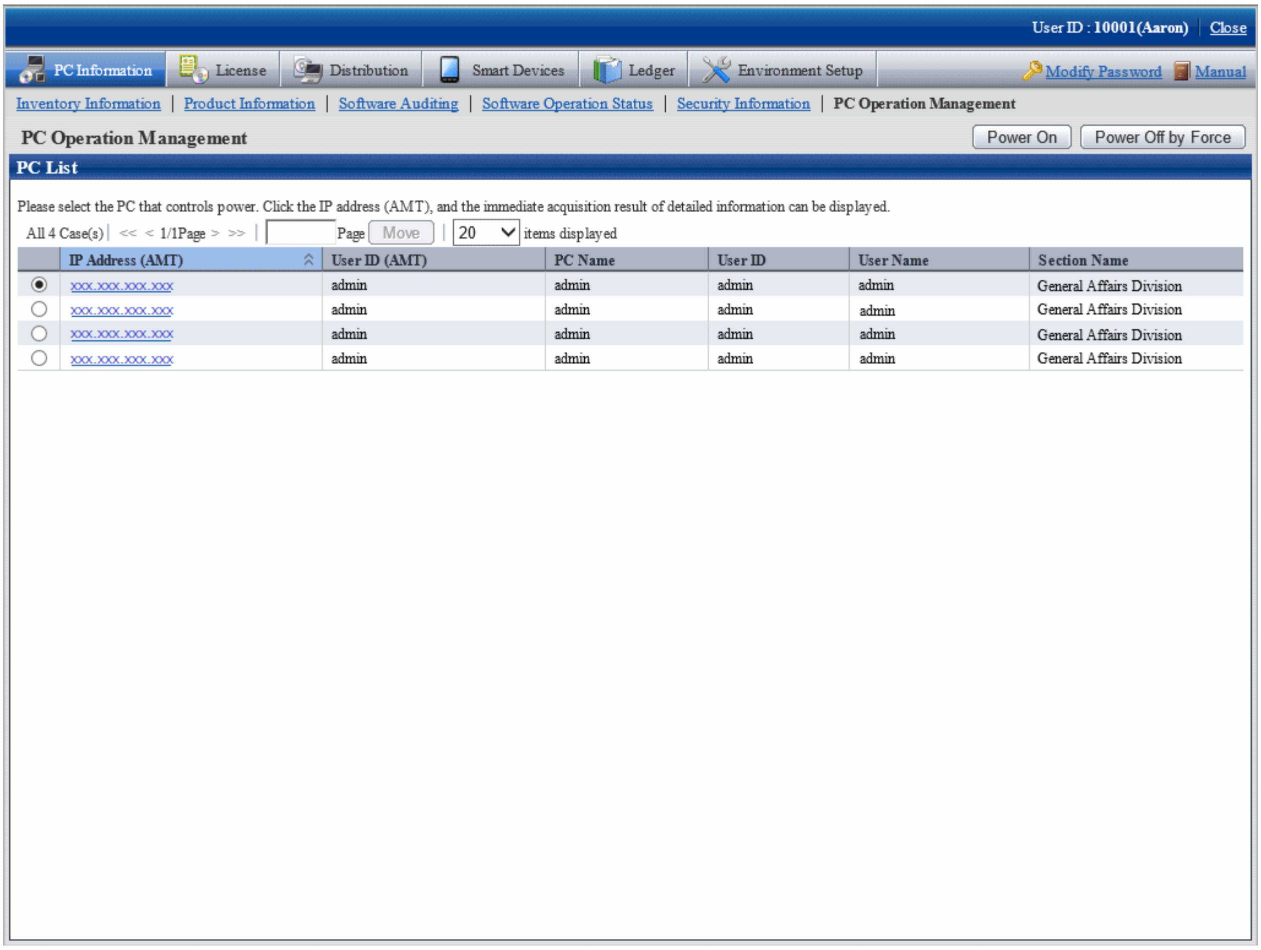
- Immediate collection of inventory information (hardware information) (Note)
- Operation on power supply (ON, OFF)

Note: The inventory collection via this function must need to use Intel(R) 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 is displayed in the **PC Information** window of main menu.



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

All 4 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

	IP Address (AMT)	User ID (AMT)	PC Name	User ID	User Name	Section Name
●	xxx.xxx.xxx.xxx	admin	admin	admin	admin	General Affairs Division
○	xxx.xxx.xxx.xxx	admin	admin	admin	admin	General Affairs Division
○	xxx.xxx.xxx.xxx	admin	admin	admin	admin	General Affairs Division
○	xxx.xxx.xxx.xxx	admin	admin	admin	admin	General Affairs Division

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, confirm the setting value first.

For information on how to modify, refer to "Command Reference" of the *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 in the main menu homepage.

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

1. Easily master business status only through browsing the **Status** window.

2. Master the status of statistical items from multiple points of view to quickly judge the problems existing in service execution.

   Statistical items:

   - PCs for which inventory information has not been collected
   - PCs on which security patches have not been installed
   - PCs violating security policy
   - PCs violating power saving policy
   - PCs on which unlicensed software is installed
   - Expired contracts
   - Contracts about to expire
   - Devices for which stocktaking is not yet complete
   - Devices detected as unregistered devices

3. Display detailed information according to statistical items to easily screen out problems related to the items.

   Detailed Information:

   - Aggregate by section
   - Aggregate by item

4. Save the time for screening out corresponding PCs/devices/contracts to quickly processing them because the PCs/devices/contracts 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, confirmation can be made in the **Status** window according to the point of view to every product.

Application processing

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

The following application processing can be performed in the **Status** window:

1. Message sending

   - Send messages to the problematic PC/device/contract to make the user of the PC/device/contract aware of the problems in the application method.
   - Although the operation on the set diagnosis result window is allowed, the PC/device/contract 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/devices/contracts.

   - 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.

7. Furthermore, other actions can be taken for each item.

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.

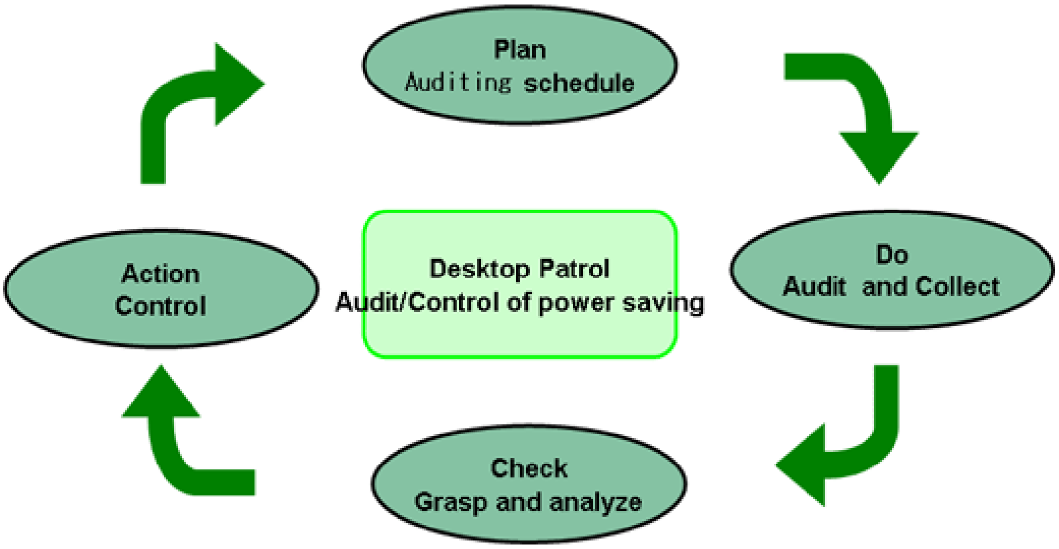
The following functions can be used for security auditing/control.

- 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.

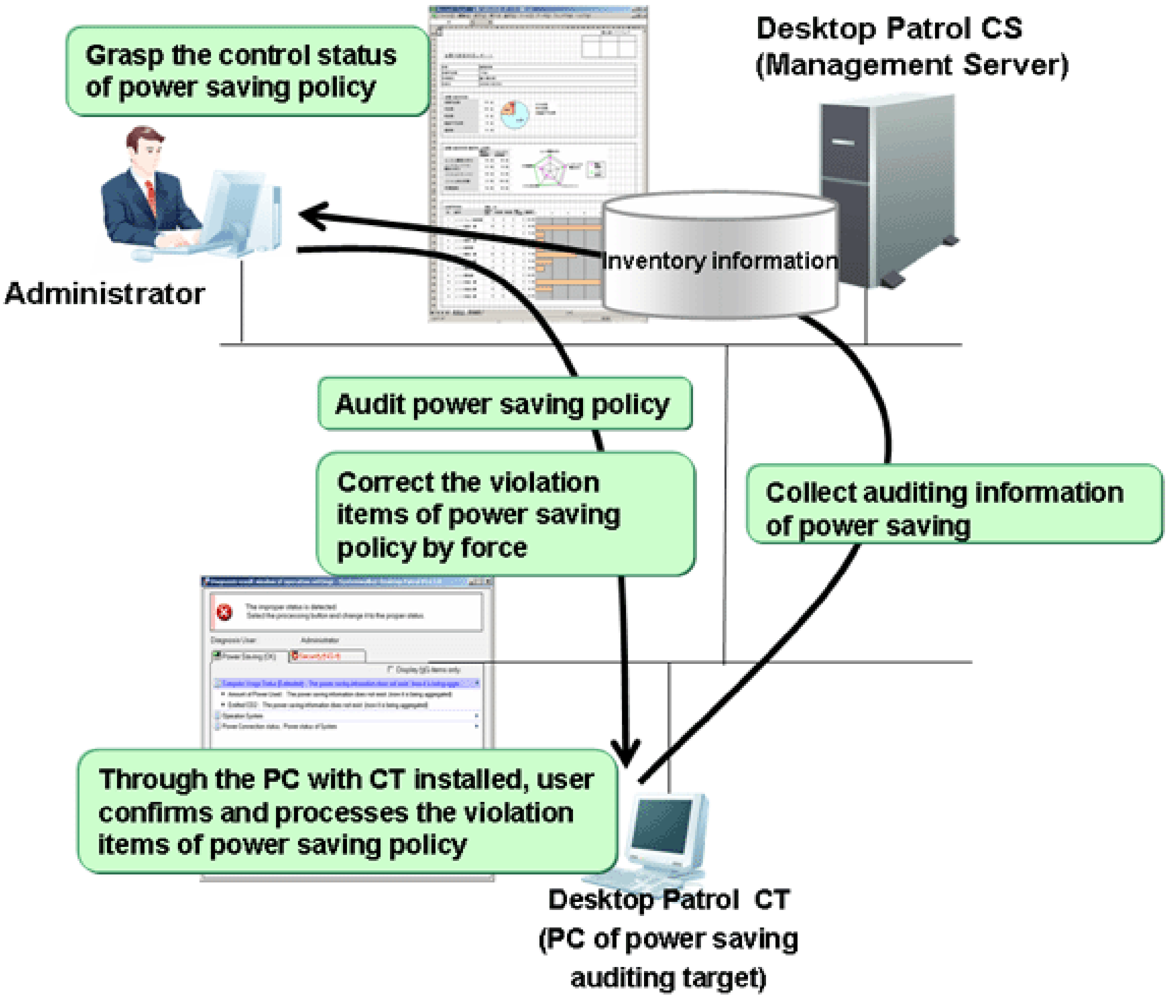
- Auditing plan: Execute power saving auditing plan of operating system.
- Audit and collect: Collect the information about power saving setup status of the PC.
- Master and analyze: Confirm and analyze the power saving setup status of the PC.
- Control: Control the PC needing treatment according to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



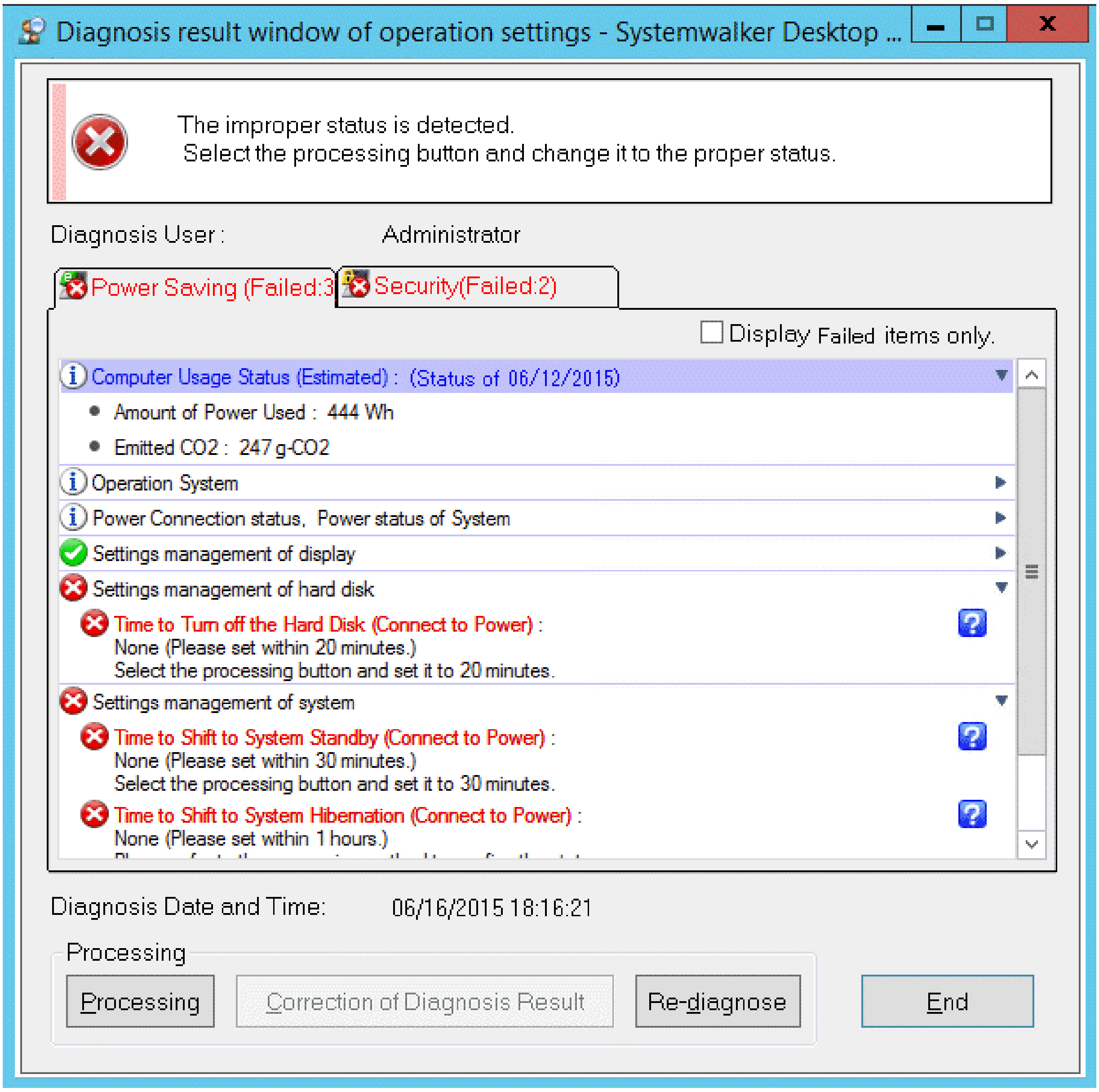
Power saving auditing and control status realized via Systemwalker Desktop Patrol during the PDCA period is summarily shown below:

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 ...

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

Diagnosis User : Administrator

Computer Usage Status (Estimated) : (Status of 06/12/2015)

- Amount of Power Used : 444 Wh
- Emitted CO2 : 247 g-CO2

Operation System

Power Connection status, Power status of System

✓ Settings management of display

☒ Settings management of hard disk

☒ Time to Turn off the Hard Disk (Connect to Power) :
None (Please set within 20 minutes.)
Select the processing button and set it to 20 minutes.

☒ Settings management of system

☒ Time to Shift to System Standby (Connect to Power) :
None (Please set within 30 minutes.)
Select the processing button and set it to 30 minutes.

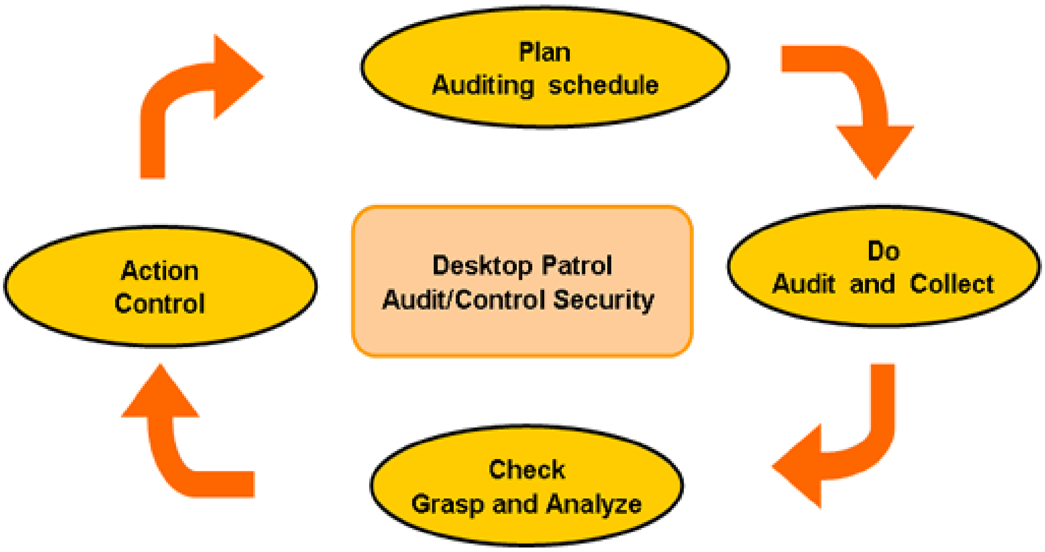
☒ Time to Shift to System Hibernation (Connect to Power) :
None (Please set within 1 hours.)

Diagnosis Date and Time: 06/16/2015 18:16:21

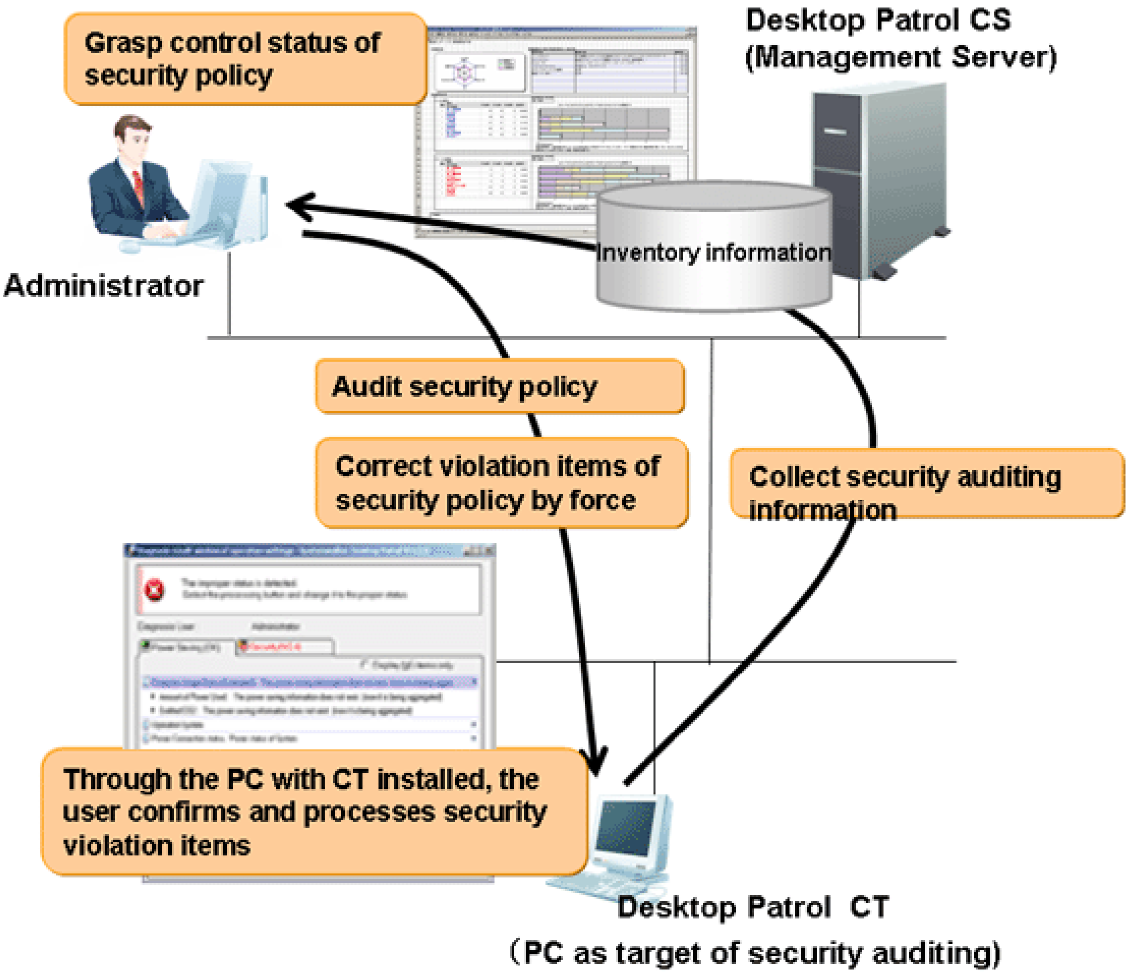
2.2.2 Auditing/Control of Security Setup

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

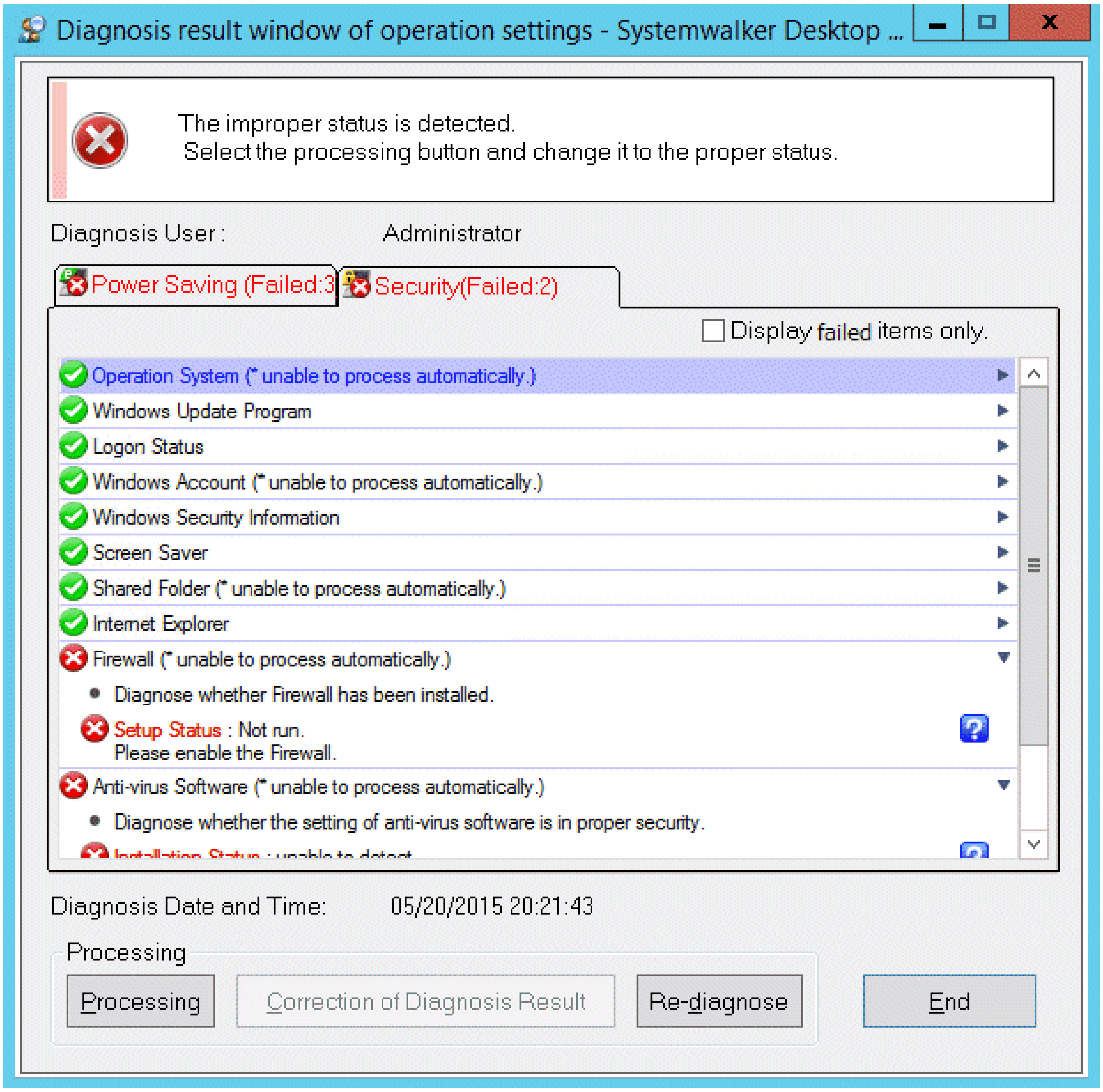
- Auditing plan: Execute the security auditing plan of the operating system.
- Audit and collect: Collect the information about security setup status of the PC.
- Master and analyze: Confirm and analyze the security setup status of the PC.
- Control: Control the PC needing treatment according to analysis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

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

Diagnosis User : Administrator

- ✓ Operation System (* unable to process automatically.)
- ✓ Windows Update Program
- ✓ Logon Status
- ✓ Windows Account (* unable to process automatically.)
- ✓ Windows Security Information
- ✓ Screen Saver
- ✓ Shared Folder (* unable to process automatically.)
- ✓ Internet Explorer
- ✗ Firewall (* unable to process automatically.)
  - ● Diagnose whether Firewall has been installed.
  - ✗ Setup Status : Not run.
    Please enable the Firewall.
- ✗ Anti-virus Software (* unable to process automatically.)
  - ● Diagnose whether the setting of anti-virus software is in proper security.
  - ✗ Installation Status : unable to detect

Diagnosis Date and Time: 05/20/2015 20:21:43

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.

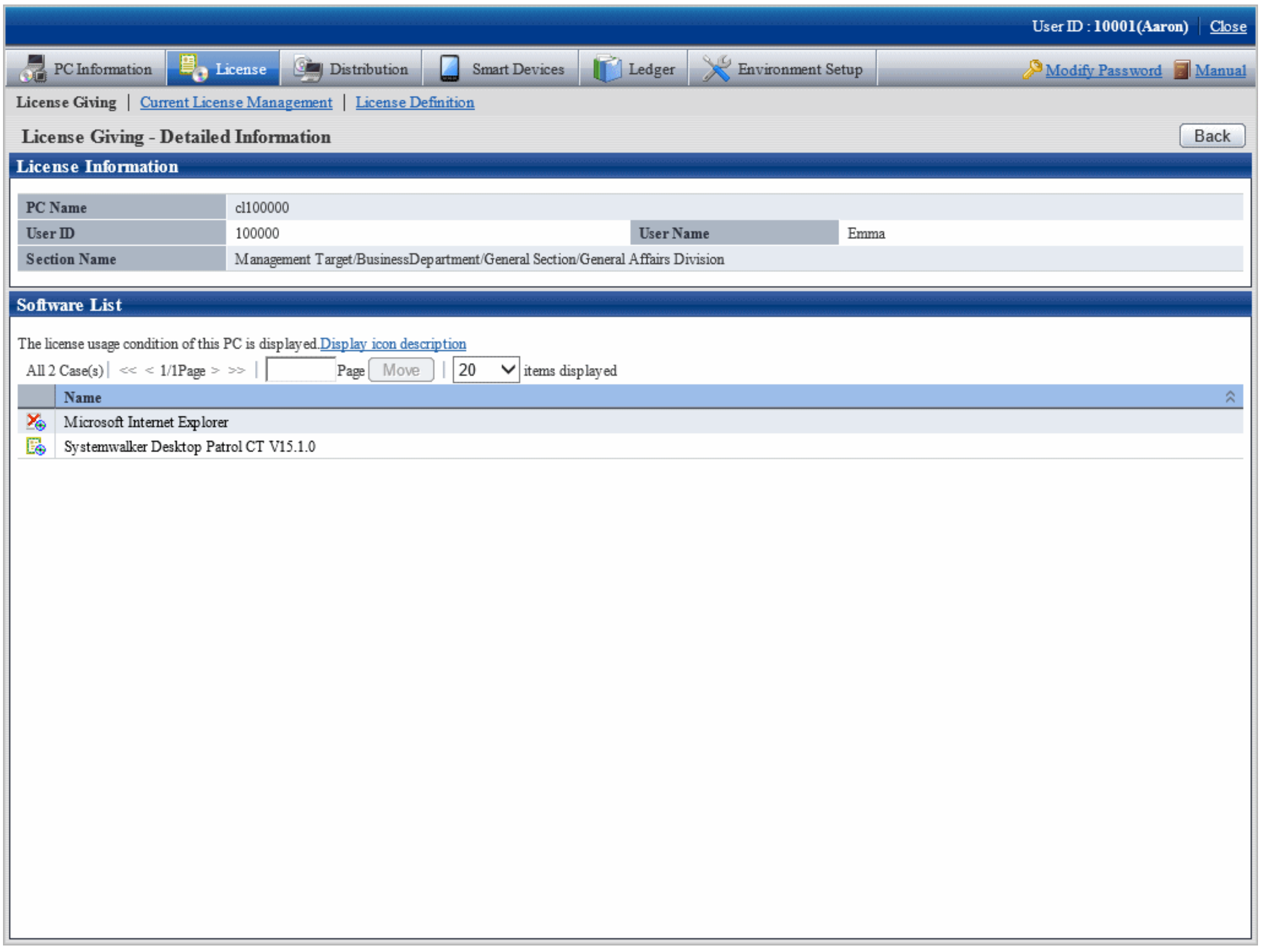
- "Software Dictionary" has been registered
- The relation between License and software (Dictionary Code) has been defined in the **License** > **License Definition** window of the main menu.
- The number of Licenses for each section has been set in the **License** > **Current License Management** window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

Distribute the license to software used in the PC in the **License** > **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** > **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** > **License Giving** window of main menu, the usage status of License will be displayed as below.


User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
License Giving | Current License Management | License Definition
Back

License Giving - Detailed Information

License Information

PC Name	cl100000		
User ID	100000	User Name	Emma
Section Name	Management Target/BusinessDepartment/General Section/General Affairs Division		

Software List

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

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

Name
Microsoft Internet Explorer
Systemwalker Desktop Patrol CT V15.1.0

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 "Product 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 ICT assets and shortage of software license.

Importing the SAMAC software dictionary

The association of SAM Assessment & Certification (SAMAC) Software Dictionary can be imported and used in Systemwalker Desktop Patrol.

The imported SAMAC Software Dictionary data is used as a user definition.

By selecting the software to be audited, software installation status detection and license management can be performed.

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.

2.4 File Distribution Function

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

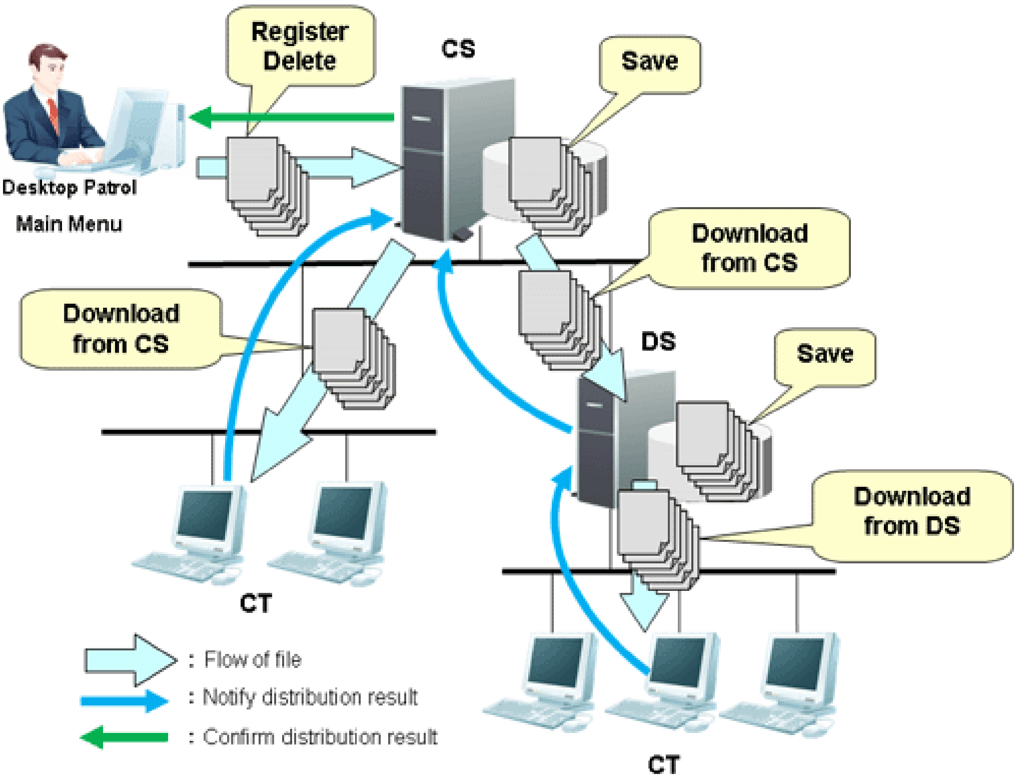
File distribution function is a function of distributing multiple files from CS to multiple CTs only through operation on the CS. In addition, the distribution result can be confirmed on the CS.

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, use the "2.5 Software Distribution Function". In addition, if it is required to apply security patches, use "2.6 Security Patches Distribution /Application Function"

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

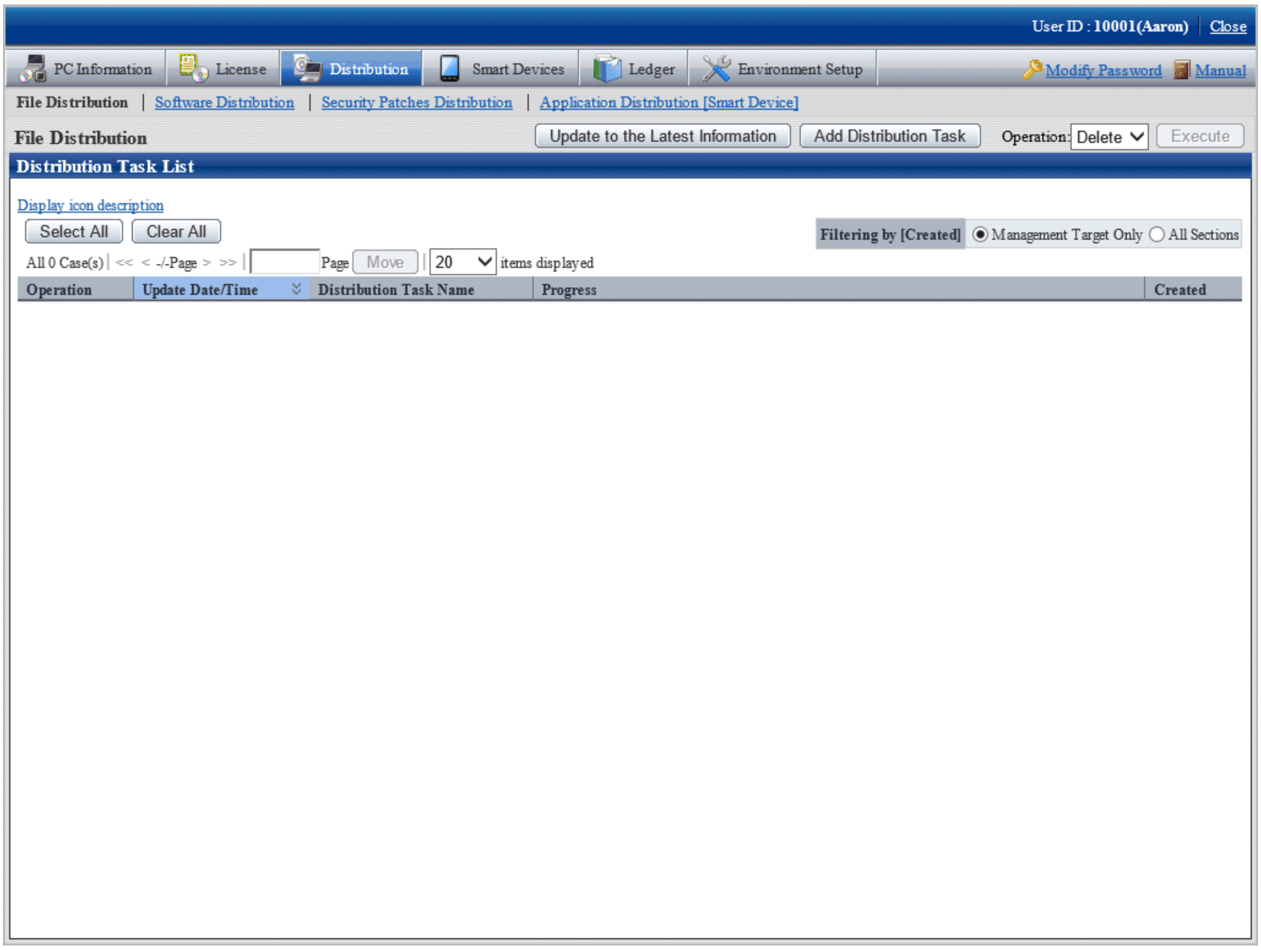
- Distribution Settings of file and distribution target
- File download
- Distribution result confirmation



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.



Operation: Delete

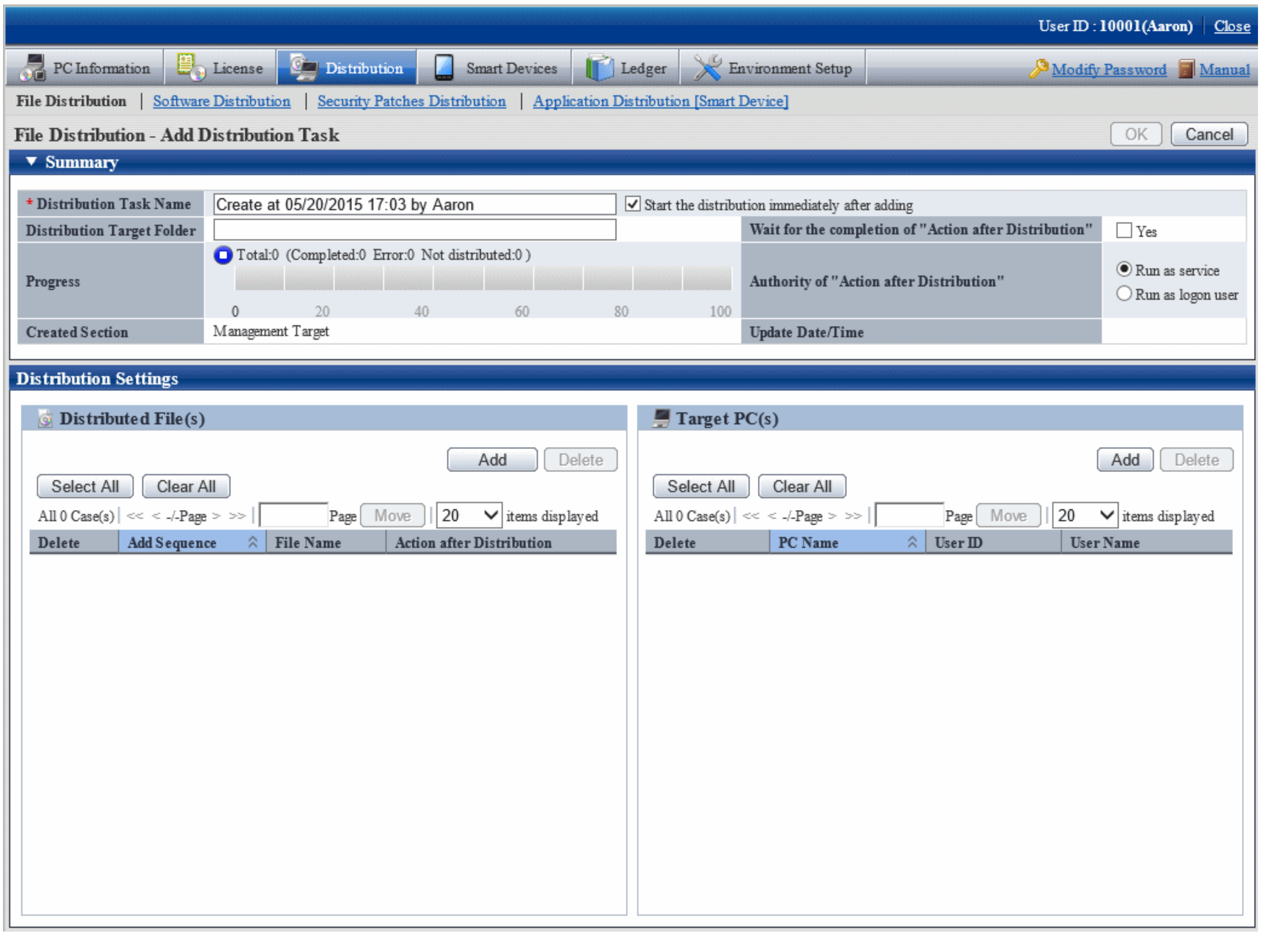
Filtering by [Created]: ● Management Target Only ○ All Sections

20 items displayed

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.



User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
File Distribution | Software Distribution | Security Patches Distribution | Application Distribution [Smart Device]

File Distribution - Add Distribution Task

▼ Summary

* Distribution Task Name	Create at 05/20/2015 17:03 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) 0 20 40 60 80 100	Authority of "Action after Distribution"	● Run as service ○ Run as logon user
Created Section	Management Target	Update Date/Time	

Distribution Settings

Distributed File(s)

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

Delete	Add Sequence	File Name	Action after Distribution

Target PC(s)

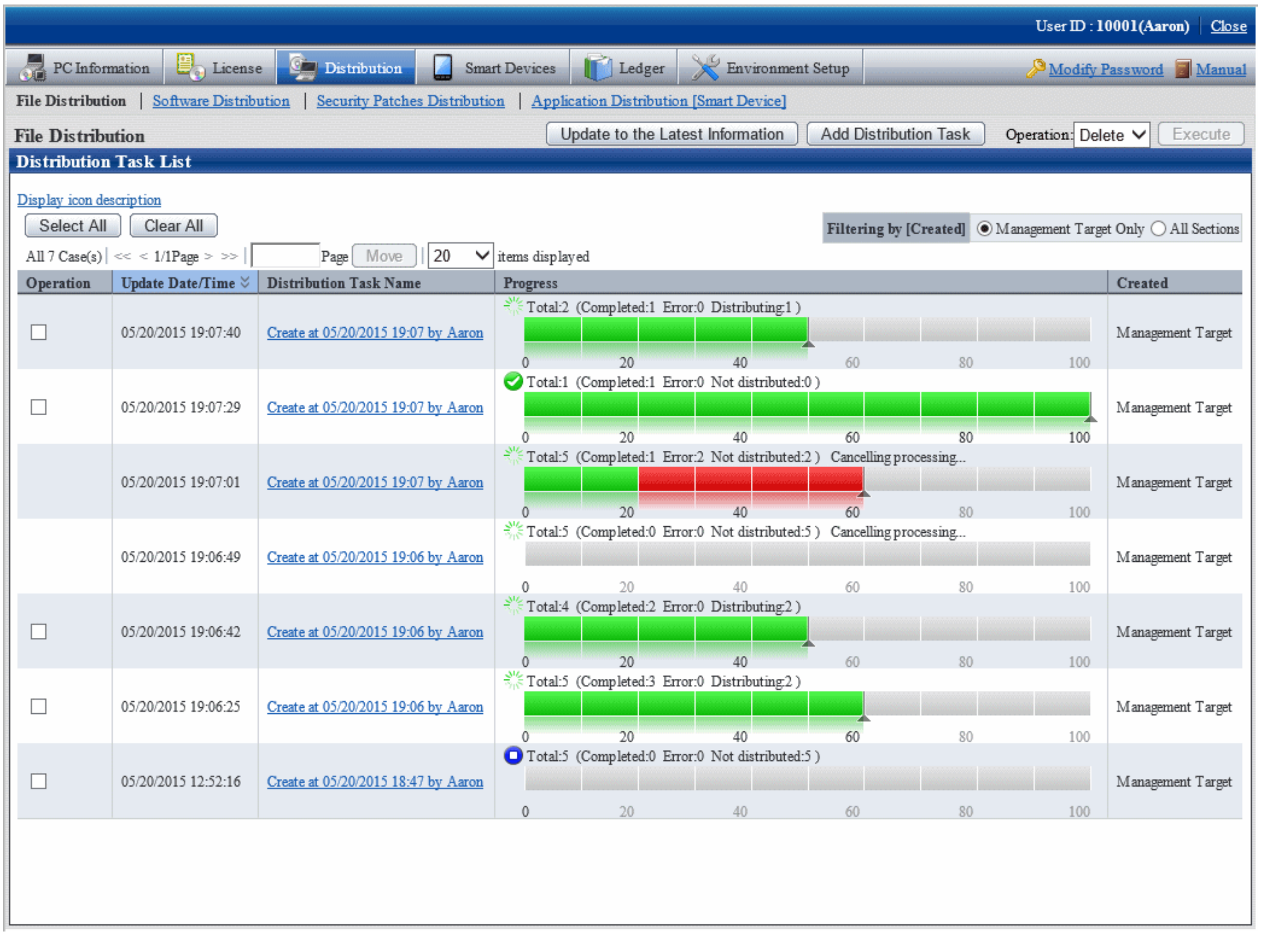
Add
Delete
Select All
Clear All
All 0 Case(s) | << < -/-Page > >> | Page Move | 20 items displayed

Delete	PC Name	User ID	User Name

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.



File Distribution

Operation: Delete

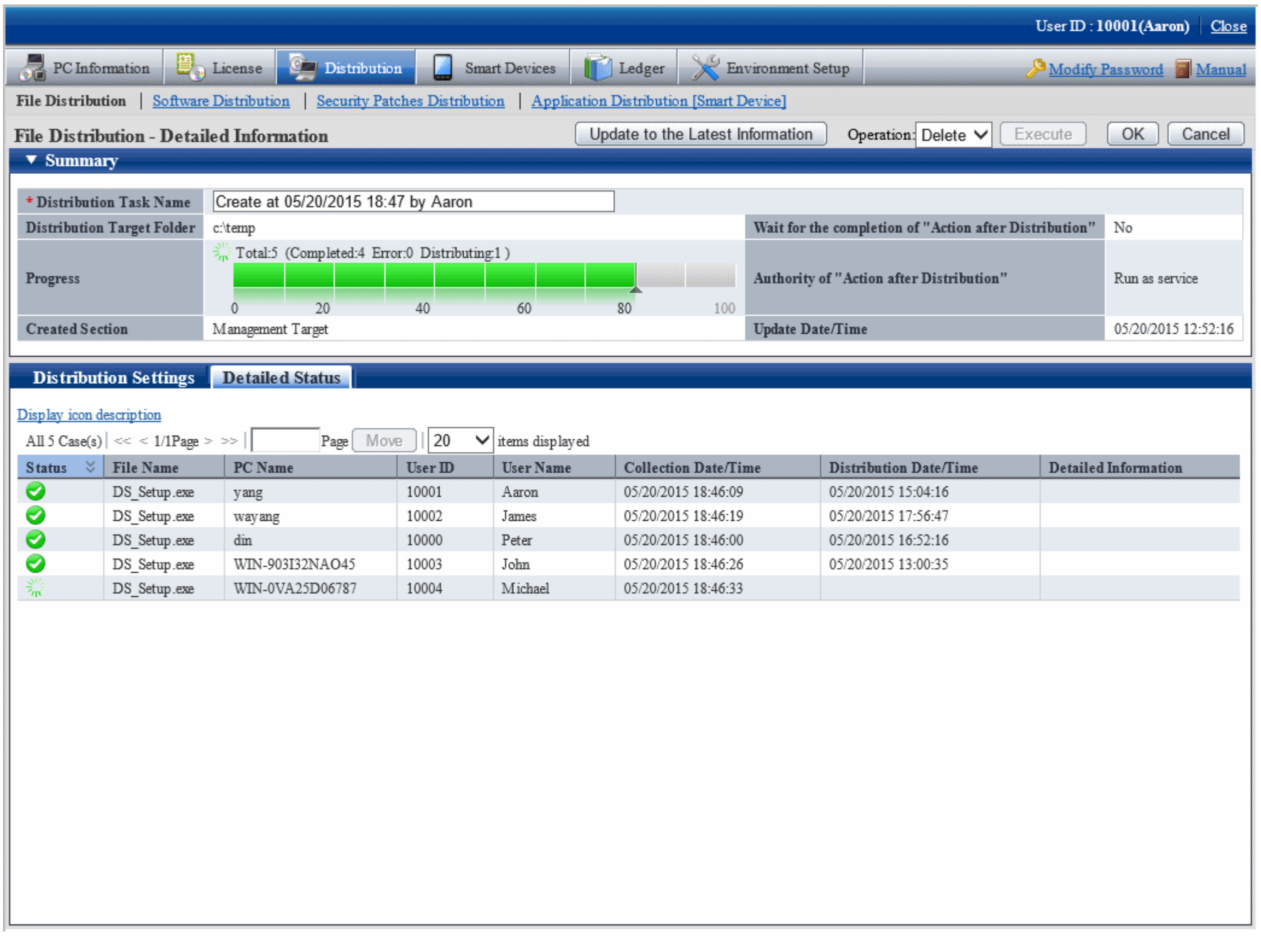
Distribution Task List

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

All 7 Case(s) << < 1/1Page > >> Page 20 items displayed

Operation	Update Date/Time	Distribution Task Name	Progress	Created
□	05/20/2015 19:07:40	Create at 05/20/2015 19:07 by Aaron	Total:2 (Completed:1 Error:0 Distributing:1)	Management Target
□	05/20/2015 19:07:29	Create at 05/20/2015 19:07 by Aaron	✓ Total:1 (Completed:1 Error:0 Not distributed:0)	Management Target
	05/20/2015 19:07:01	Create at 05/20/2015 19:07 by Aaron	Total:5 (Completed:1 Error:2 Not distributed:2) Cancelling processing...	Management Target
	05/20/2015 19:06:49	Create at 05/20/2015 19:06 by Aaron	Total:5 (Completed:0 Error:0 Not distributed:5) Cancelling processing...	Management Target
□	05/20/2015 19:06:42	Create at 05/20/2015 19:06 by Aaron	Total:4 (Completed:2 Error:0 Distributing:2)	Management Target
□	05/20/2015 19:06:25	Create at 05/20/2015 19:06 by Aaron	Total:5 (Completed:3 Error:0 Distributing:2)	Management Target
□	05/20/2015 12:52:16	Create at 05/20/2015 18:47 by Aaron	Total:5 (Completed:0 Error: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.



File Distribution - Detailed Information

* Distribution Task Name	Create at 05/20/2015 18:47 by Aaron		
Distribution Target Folder	c:\temp	Wait for the completion of "Action after Distribution"	No
Progress	Total:5 (Completed:4 Error:0 Distributing:1) 0 20 40 60 80 100	Authority of "Action after Distribution"	Run as service
Created Section	Management Target	Update Date/Time	05/20/2015 12:52:16

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

Status	File Name	PC Name	User ID	User Name	Collection Date/Time	Distribution Date/Time	Detailed Information
✓	DS_Setup.exe	yang	10001	Aaron	05/20/2015 18:46:09	05/20/2015 15:04:16	
✓	DS_Setup.exe	wayang	10002	James	05/20/2015 18:46:19	05/20/2015 17:56:47	
✓	DS_Setup.exe	din	10000	Peter	05/20/2015 18:46:00	05/20/2015 16:52:16	
✓	DS_Setup.exe	WIN-903I32NAO45	10003	John	05/20/2015 18:46:26	05/20/2015 13:00:35	
⟳	DS_Setup.exe	WIN-0VA25D06787	10004	Michael	05/20/2015 18:46:33		

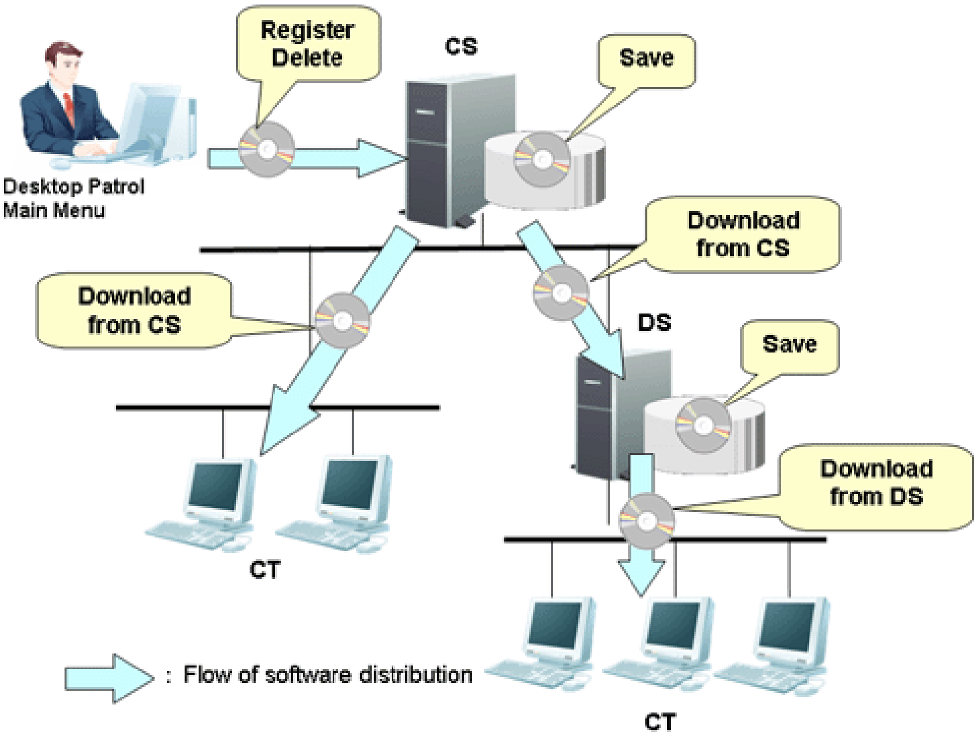
2.5 Software Distribution Function

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

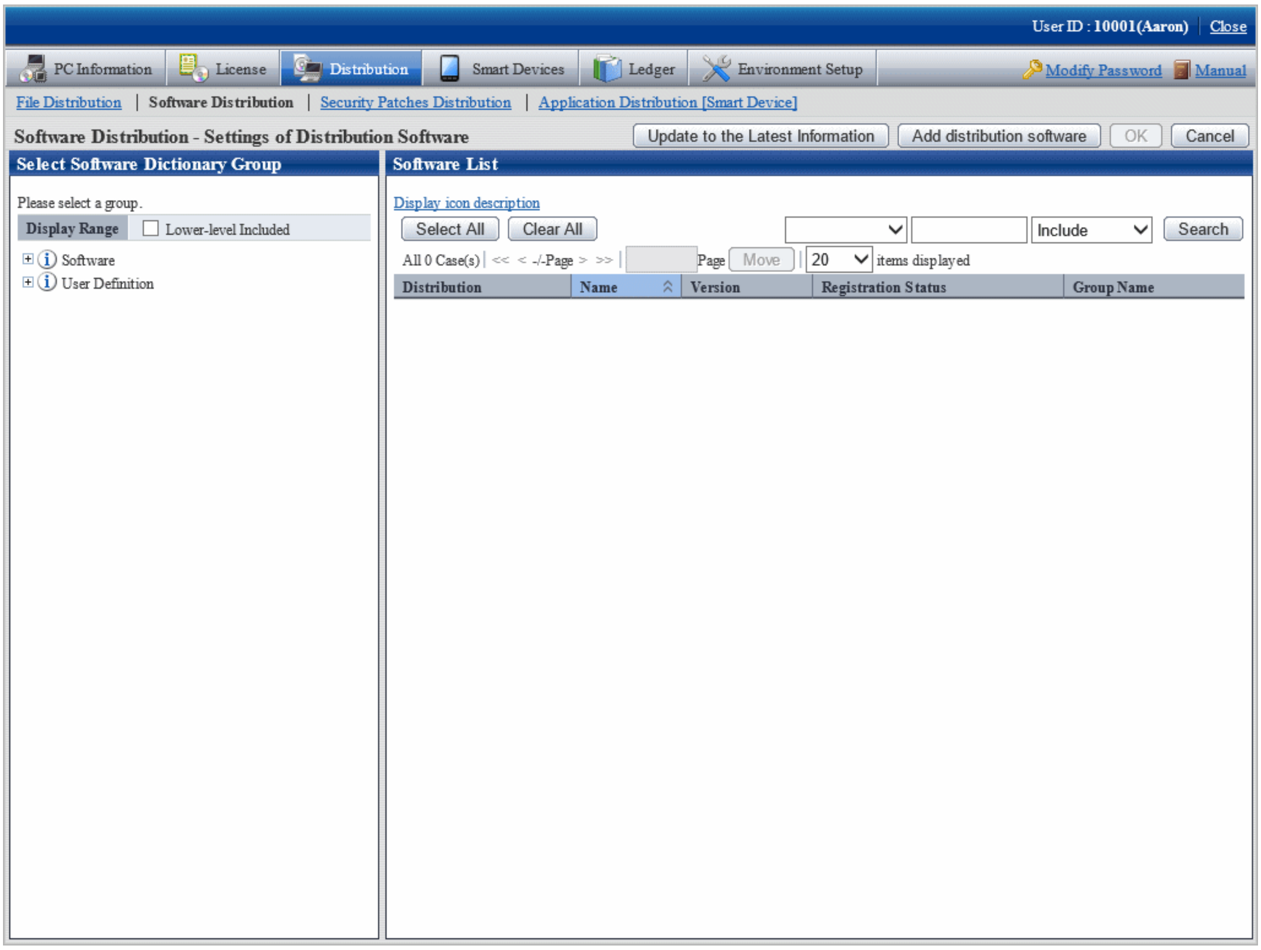


2.5.1 Management on Software Distribution

Management on Software Distribution includes:

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

Manage the Software Distribution in the **Distribution** > **Software Distribution** > **Add Software Group for 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 higher server and CT can download Software Distribution from the higher 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.

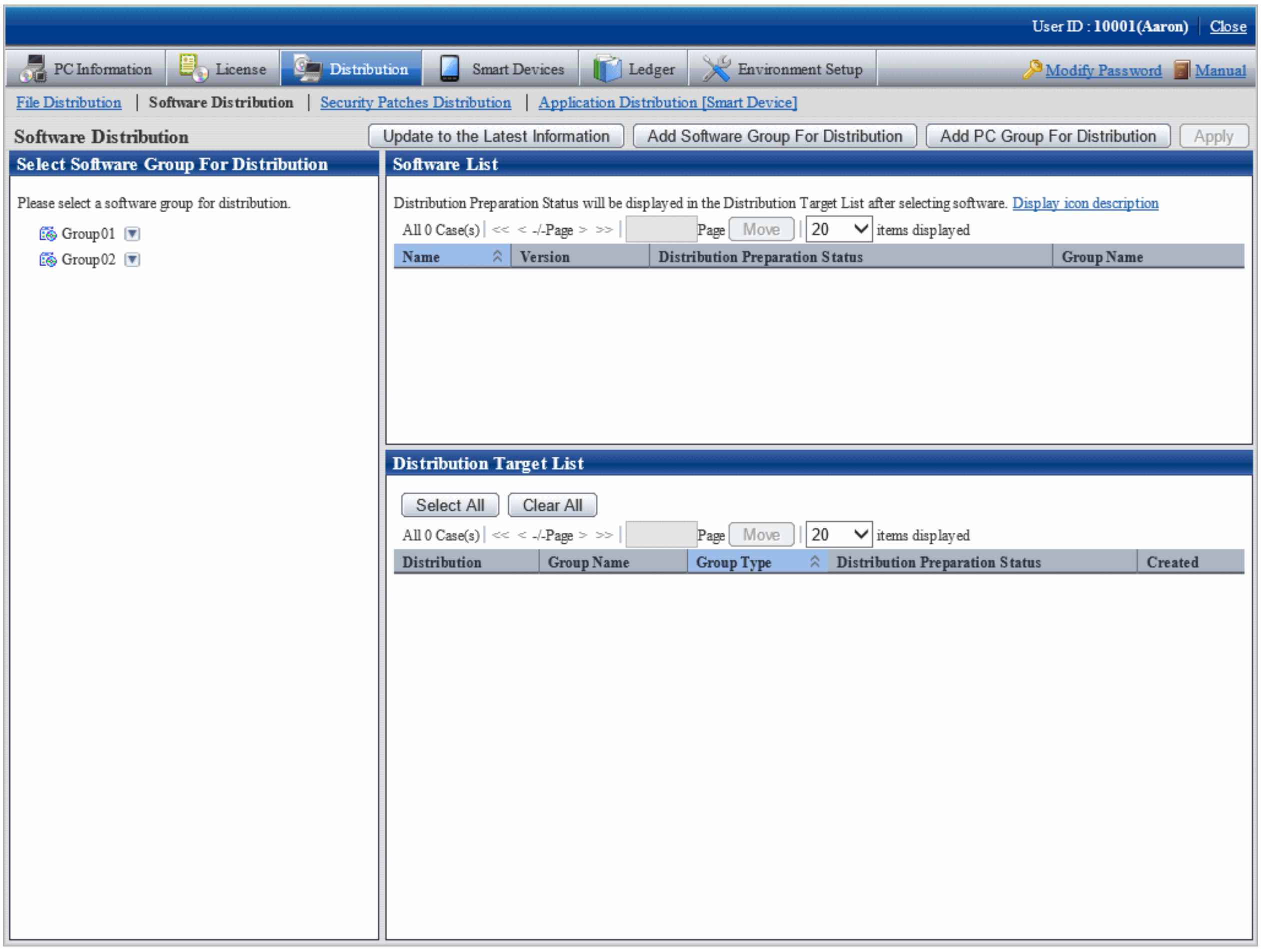
- Policy group

  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 **Distribution** > **Software Distribution** window of main menu.



Please select a software group for distribution.

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

Name	Version	Distribution Preparation Status	Group Name

Distribution	Group Name	Group Type	Distribution Preparation Status	Created

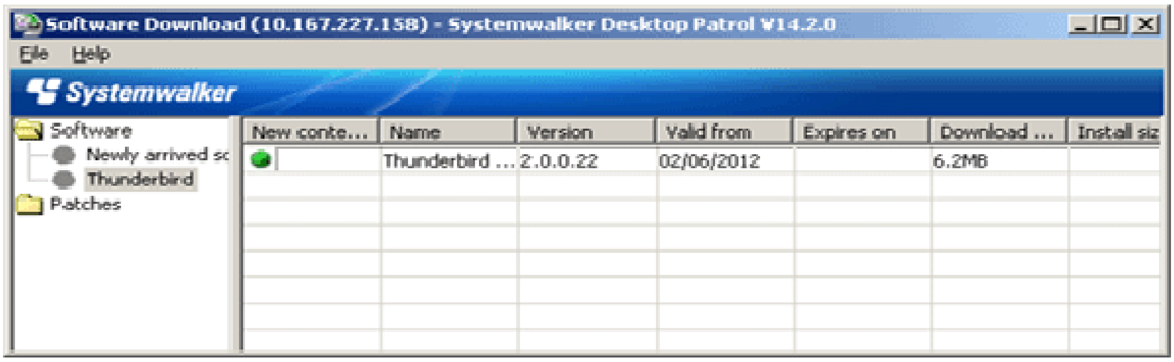
2.5.3 Download of Software Distribution

Download of Software Distribution is a function to download Software Distribution from the higher 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	

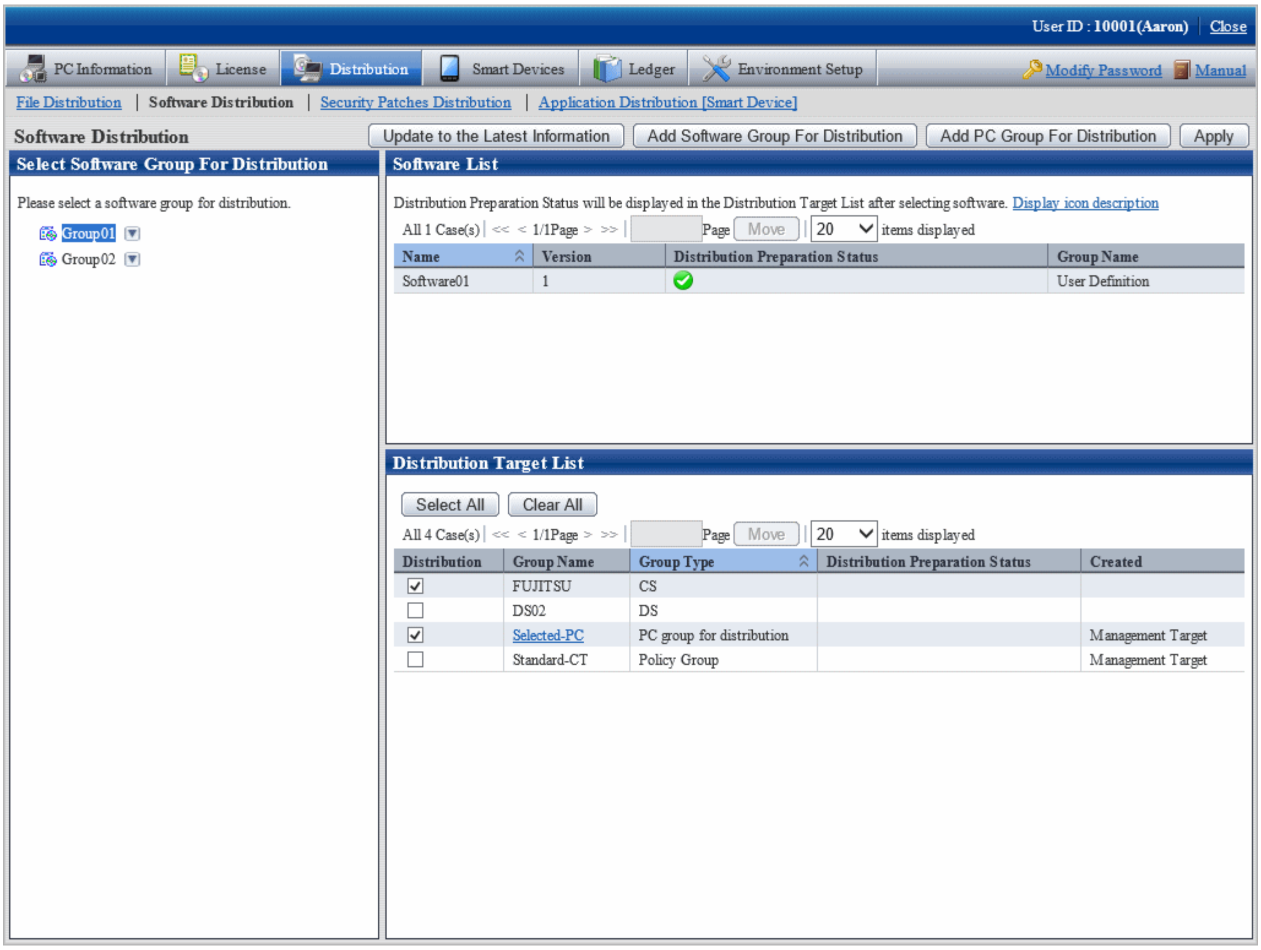
Refer to *Systemwalker Desktop Patrol Operation Guide: for Clients* for how to download Software Distribution to CTs.

Download software distribution to DS

DS can download Software Distribution from the higher 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 1 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Name	Version	Distribution Preparation Status	Group Name
Software01	1	✓	User Definition

All 4 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Distribution	Group Name	Group Type	Distribution Preparation Status	Created
☑	FUJITSU	CS		
□	DS02	DS		
☑	Selected-PC	PC group for distribution		Management Target
□	Standard-CT	Policy Group		Management Target

2.6 Security Patches Distribution /Application Function

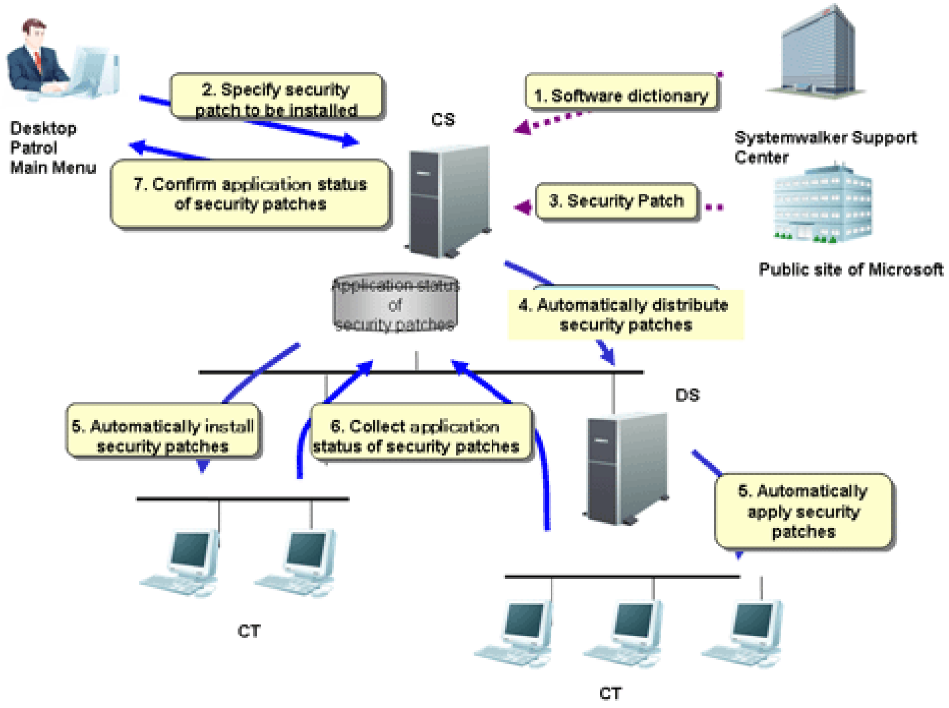
This section describes the security patches distribution and application function of Systemwalker Desktop Patrol.

2.6.1 Automatic Application of Security Patches

Systemwalker Desktop Patrol can automatically distribute the security patches provided by Microsoft Corporation from the higher 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
CS
1. Software dictionary
Systemwalker Support Center
7. Confirm application status of security patches
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", 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 higher 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 higher server, select **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Patch Application** or select **Apps** > **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.

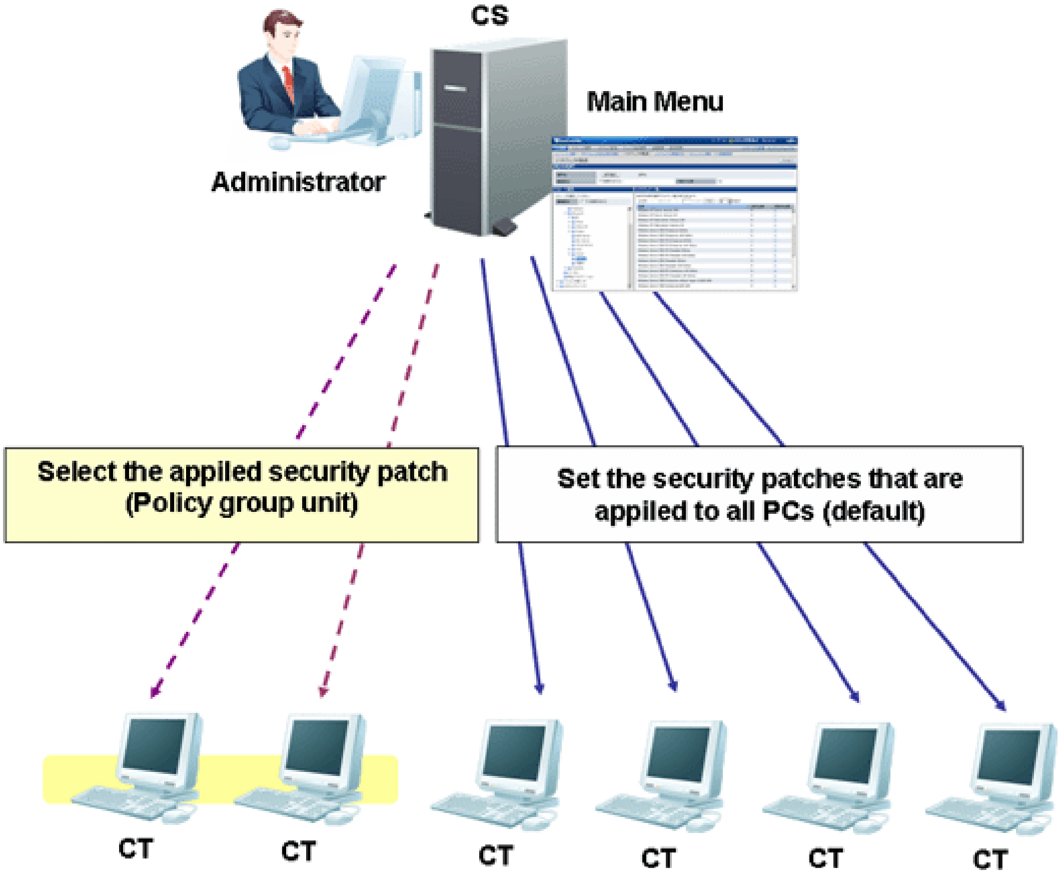
The following setups shall be applied to the selected security patches.

- 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
Administrator
Main Menu
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 **Distribution** > **Security Patches Distribution** 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 Groups** > **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 Smart Device Management Function

This section explains the smart device management function of Systemwalker Desktop Patrol.

The smart device management function manages your smart devices (Android devices and iOS devices).

By installing the smart device CT in smart devices, the inventory information of the smart devices can be collected before the information is sent to the CS via the Systemwalker Desktop Patrol SS (hereafter referred to as "SS").

The inventory information of the smart devices sent to the CS is displayed in the main menu so it can be viewed and managed.

The collected inventory information can also be imported to the management ledger where the information can be displayed, edited, and output as report, just like the PC information and network device information.

Systemwalker Desktop Patrol SS

An SS is a Smart Device Relay Server, and is installed between smart devices and a CS in order to send the inventory information collected from the smart devices to the CS.

Note that an SS can be operated regardless of whether it coexists with a CS or not.

Smart device CT

Use the smart device CT that is installed in smart devices to collect the inventory information of the smart devices.

2.7.1 Managing an Individually Owned Smart Device (Android Device Only)

The ownership type of a smart device becomes individually owned when the device owner clear **Company owned device** in the smart device CT. For individually owned smart devices, the system administrator would decide whether to collect the inventory information (phone number, account information, etc).

2.8 Application Distribution Function (to Smart Devices)

With this function, applications can be distributed to smart devices (Android devices and iOS devices).

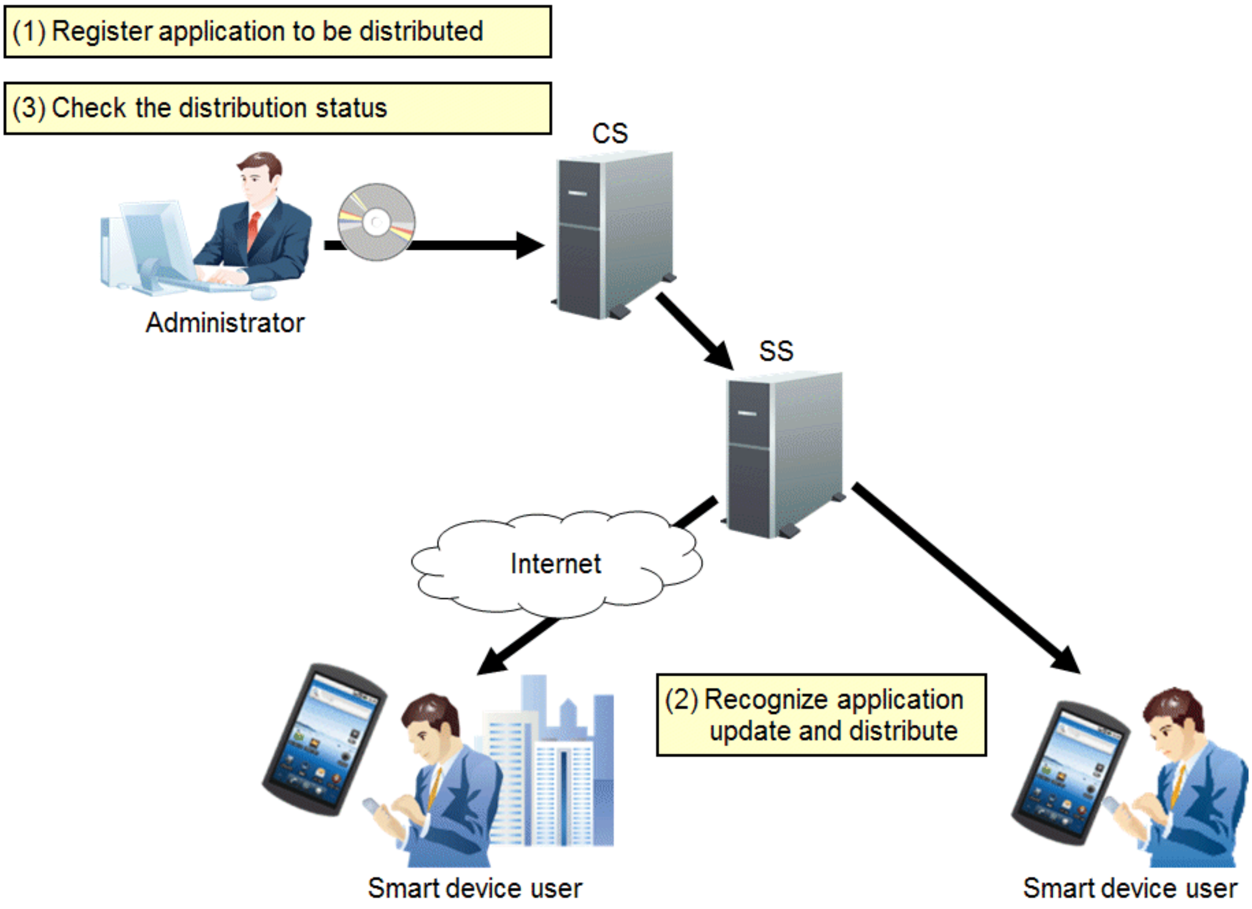
Note

The Android(TM) native application (apk file) or the iOS native application (ipa file and manifest file) can be distributed.

The administrator can perform the following management tasks in the main menu.

- Distribute a specific application to the smart device.
- Check the installation status of application on the smart device.

The smart device user, however, must approve of the installation of the distributed application.


(1) Register application to be distributed
(3) Check the distribution status
CS
Administrator
SS
Internet
(2) Recognize application update and distribute
Smart device user
Smart device user

2.9 Management Ledger Function

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

2.9.1 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 **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

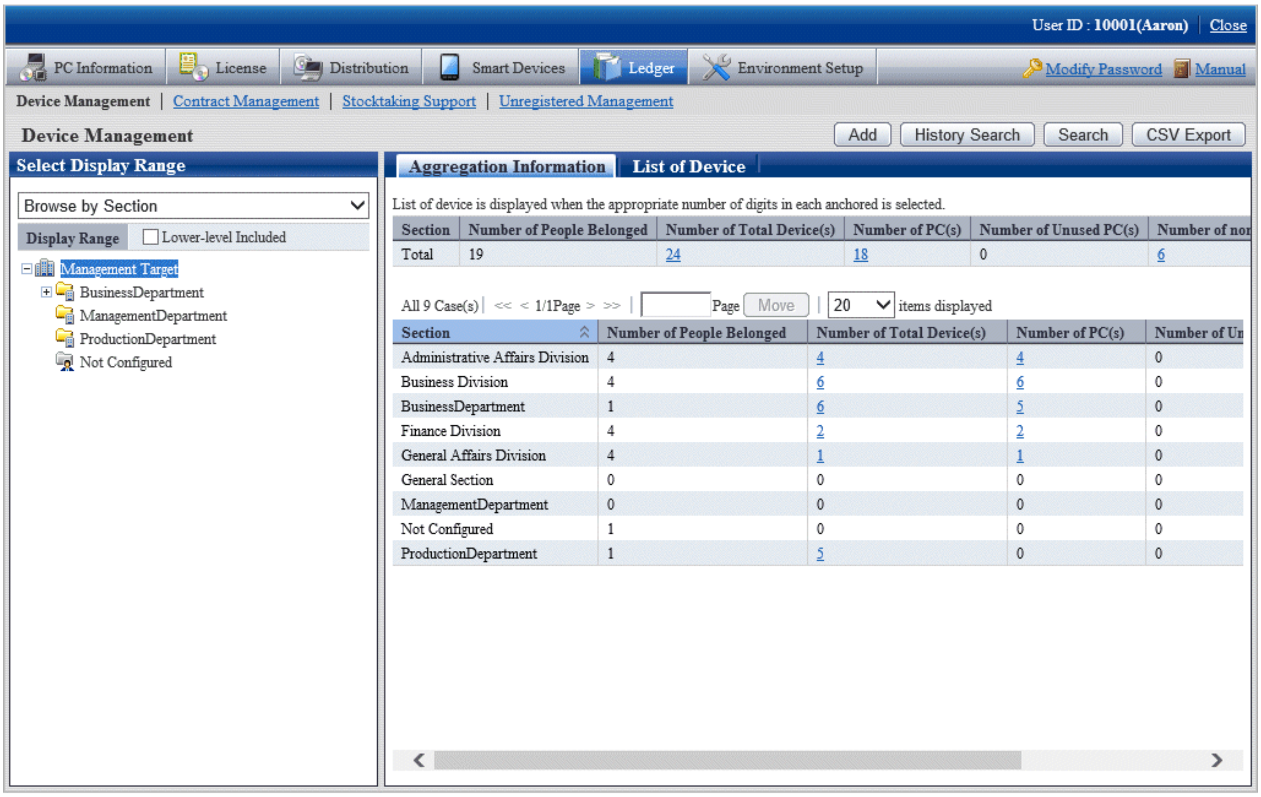
Display the information of devices meeting the requirements of user operation.

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.

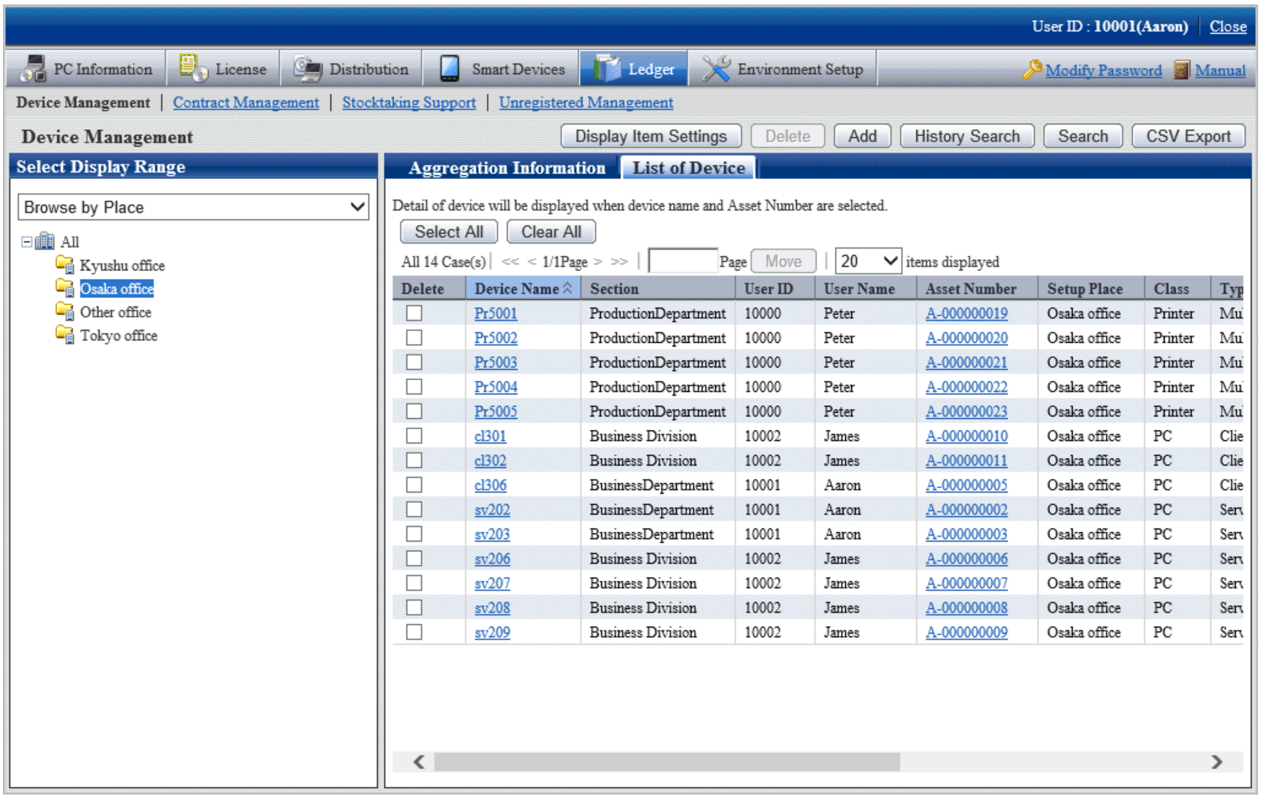
Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Unused PC(s)	Number of nor
Total	19	24	18	0	6

Section	Number of People Belonged	Number of Total Device(s)	Number of PC(s)	Number of Un
Administrative Affairs Division	4	4	4	0
Business Division	4	6	6	0
BusinessDepartment	1	6	5	0
Finance Division	4	2	2	0
General Affairs Division	4	1	1	0
General Section	0	0	0	0
ManagementDepartment	0	0	0	0
Not Configured	1	0	0	0
ProductionDepartment	1	5	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:



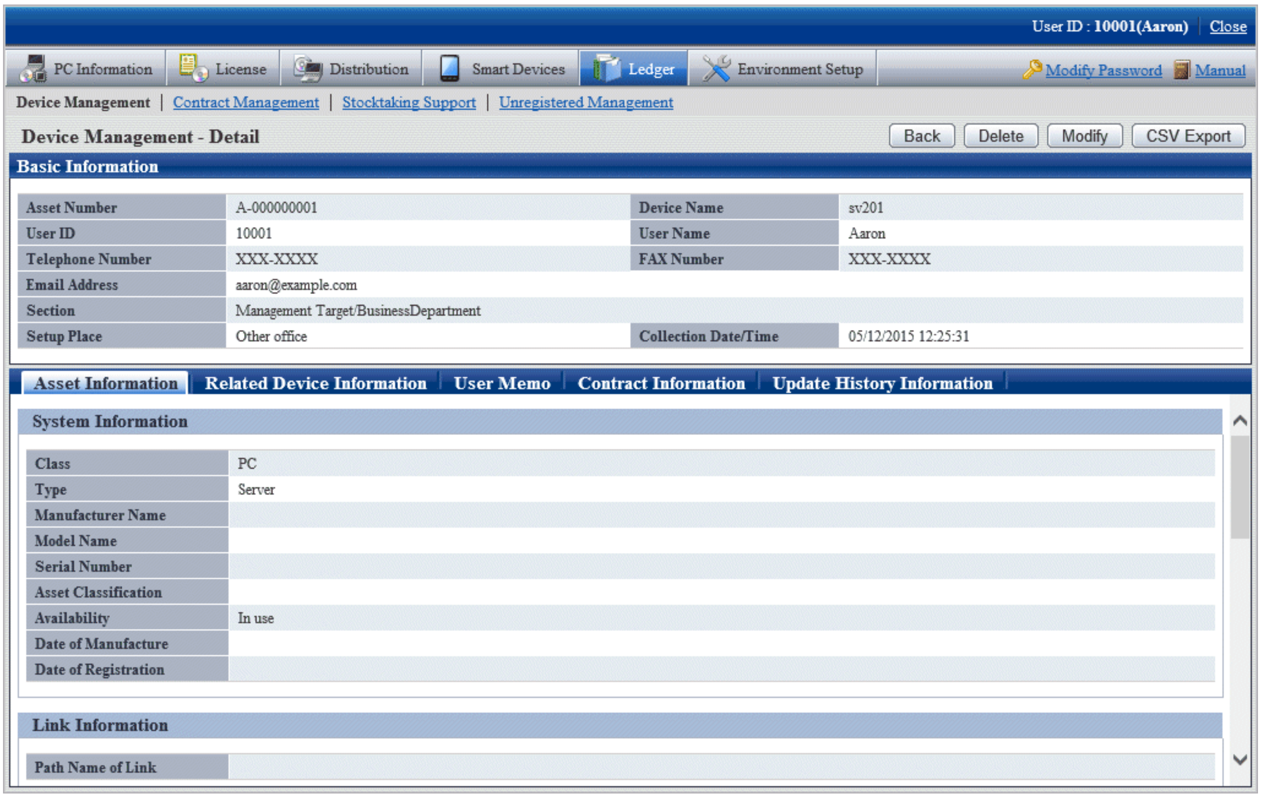
Detail of device will be displayed when device name and Asset Number are selected.

Delete	Device Name	Section	User ID	User Name	Asset Number	Setup Place	Class	Typ
□	Pr5001	ProductionDepartment	10000	Peter	A-000000019	Osaka office	Printer	Mu
□	Pr5002	ProductionDepartment	10000	Peter	A-000000020	Osaka office	Printer	Mu
□	Pr5003	ProductionDepartment	10000	Peter	A-000000021	Osaka office	Printer	Mu
□	Pr5004	ProductionDepartment	10000	Peter	A-000000022	Osaka office	Printer	Mu
□	Pr5005	ProductionDepartment	10000	Peter	A-000000023	Osaka office	Printer	Mu
□	cl301	Business Division	10002	James	A-000000010	Osaka office	PC	Clie
□	cl302	Business Division	10002	James	A-000000011	Osaka office	PC	Clie
□	cl306	BusinessDepartment	10001	Aaron	A-000000005	Osaka office	PC	Clie
□	sv202	BusinessDepartment	10001	Aaron	A-000000002	Osaka office	PC	Serv
□	sv203	BusinessDepartment	10001	Aaron	A-000000003	Osaka office	PC	Serv
□	sv206	Business Division	10002	James	A-000000006	Osaka office	PC	Serv
□	sv207	Business Division	10002	James	A-000000007	Osaka office	PC	Serv
□	sv208	Business Division	10002	James	A-000000008	Osaka office	PC	Serv
□	sv209	Business Division	10002	James	A-000000009	Osaka office	PC	Serv

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:



Device Management - Detail

Basic Information

Asset Number	A-000000001	Device Name	sv201
User ID	10001	User Name	Aaron
Telephone Number	XXX-XXXX	FAX Number	XXX-XXXX
Email Address	aaron@example.com		
Section	Management Target/BusinessDepartment		
Setup Place	Other office	Collection Date/Time	05/12/2015 12:25:31

System Information

Class	PC
Type	Server
Manufacturer Name	
Model Name	
Serial Number	
Asset Classification	
Availability	In use
Date of Manufacture	
Date of Registration	

Link Information

Path Name of Link	

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 note "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 status 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.

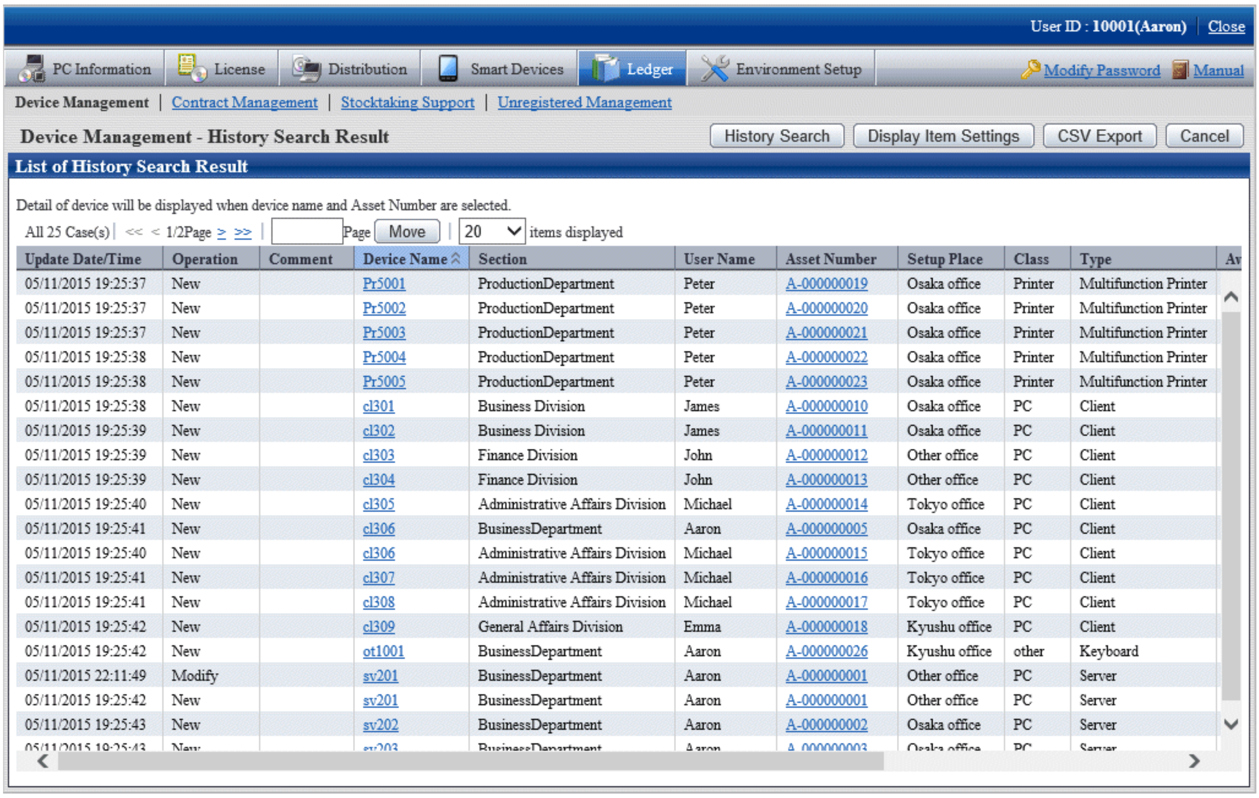
  According to the device Asset Number of new device, search the device history information to confirm the previous user and Setup Place of the device.

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

Update Date/Time	Operation	Comment	Device Name	Section	User Name	Asset Number	Setup Place	Class	Type	Av
05/11/2015 19:25:37	New		Pr5001	ProductionDepartment	Peter	A-000000019	Osaka office	Printer	Multifunction Printer	
05/11/2015 19:25:37	New		Pr5002	ProductionDepartment	Peter	A-000000020	Osaka office	Printer	Multifunction Printer	
05/11/2015 19:25:37	New		Pr5003	ProductionDepartment	Peter	A-000000021	Osaka office	Printer	Multifunction Printer	
05/11/2015 19:25:38	New		Pr5004	ProductionDepartment	Peter	A-000000022	Osaka office	Printer	Multifunction Printer	
05/11/2015 19:25:38	New		Pr5005	ProductionDepartment	Peter	A-000000023	Osaka office	Printer	Multifunction Printer	
05/11/2015 19:25:38	New		cl301	Business Division	James	A-000000010	Osaka office	PC	Client	
05/11/2015 19:25:39	New		cl302	Business Division	James	A-000000011	Osaka office	PC	Client	
05/11/2015 19:25:39	New		cl303	Finance Division	John	A-000000012	Other office	PC	Client	
05/11/2015 19:25:39	New		cl304	Finance Division	John	A-000000013	Other office	PC	Client	
05/11/2015 19:25:40	New		cl305	Administrative Affairs Division	Michael	A-000000014	Tokyo office	PC	Client	
05/11/2015 19:25:41	New		cl306	BusinessDepartment	Aaron	A-000000005	Osaka office	PC	Client	
05/11/2015 19:25:40	New		cl306	Administrative Affairs Division	Michael	A-000000015	Tokyo office	PC	Client	
05/11/2015 19:25:41	New		cl307	Administrative Affairs Division	Michael	A-000000016	Tokyo office	PC	Client	
05/11/2015 19:25:41	New		cl308	Administrative Affairs Division	Michael	A-000000017	Tokyo office	PC	Client	
05/11/2015 19:25:42	New		cl309	General Affairs Division	Emma	A-000000018	Kyushu office	PC	Client	
05/11/2015 19:25:42	New		ot1001	BusinessDepartment	Aaron	A-000000026	Kyushu office	other	Keyboard	
05/11/2015 22:11:49	Modify		sv201	BusinessDepartment	Aaron	A-000000001	Other office	PC	Server	
05/11/2015 19:25:42	New		sv201	BusinessDepartment	Aaron	A-000000001	Other office	PC	Server	
05/11/2015 19:25:43	New		sv202	BusinessDepartment	Aaron	A-000000002	Osaka office	PC	Server	
05/11/2015 19:25:43	New		sv203	BusinessDepartment	Aaron	A-000000003	Osaka office	PC	Server	

2.9.2 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

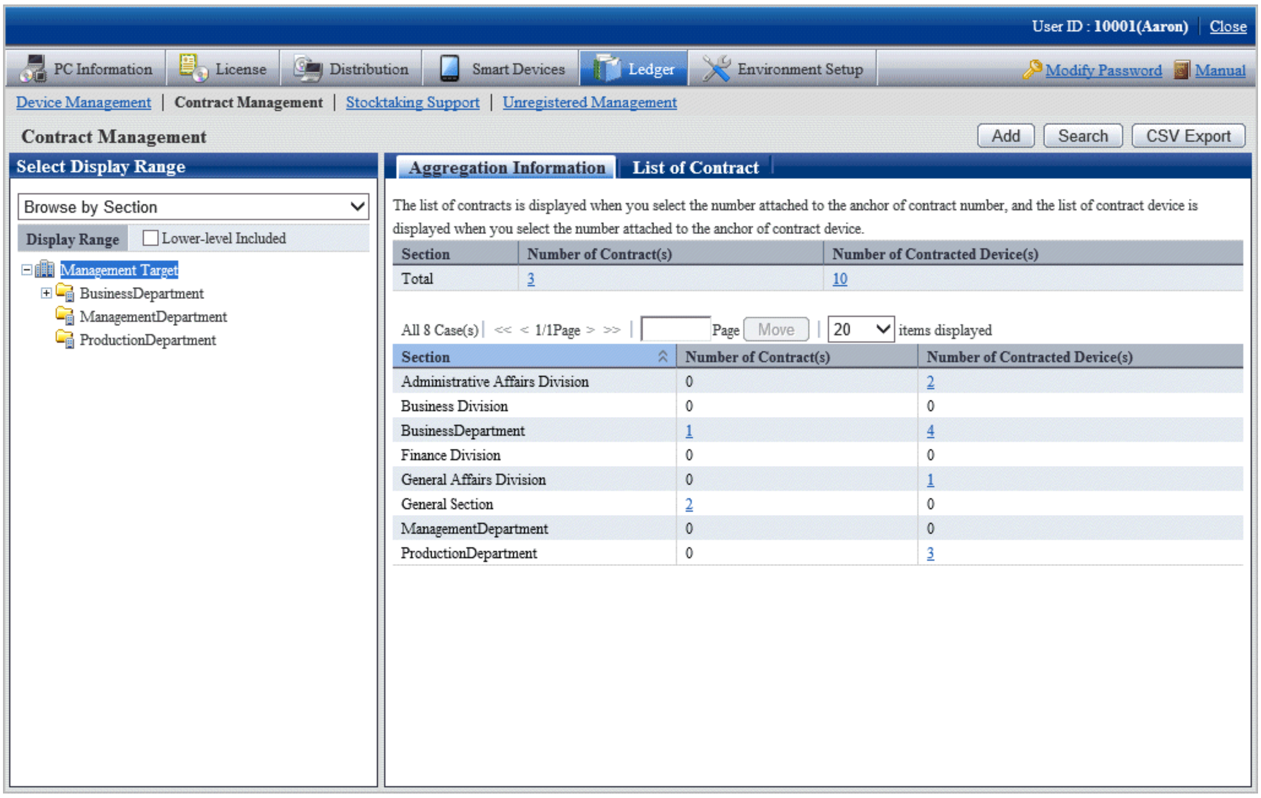
Display contract information meeting the requirements of user operation.

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:



The list of contracts is displayed when you select the number attached to the anchor of contract number, and the list of contract device is displayed when you select the number attached to the anchor of contract device.

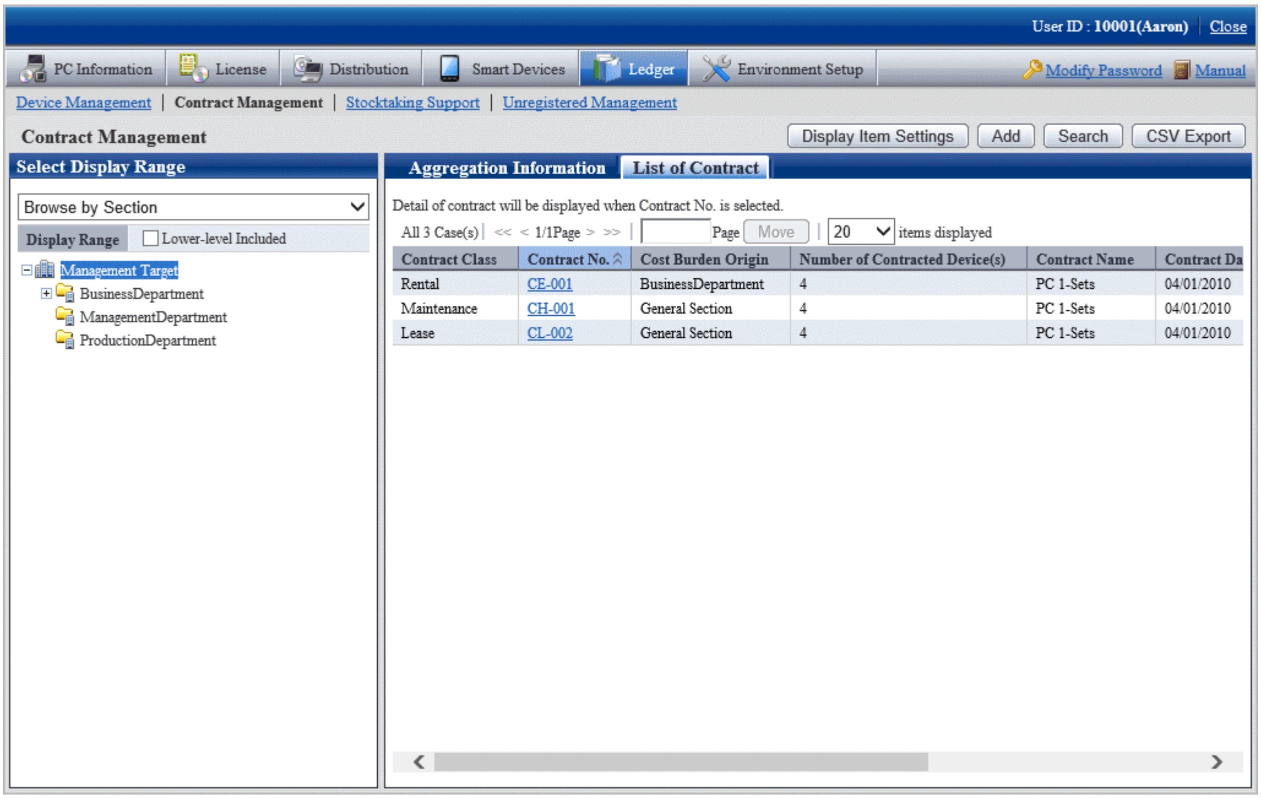
Section	Number of Contract(s)	Number of Contracted Device(s)
Total	3	10

Section	Number of Contract(s)	Number of Contracted Device(s)
Administrative Affairs Division	0	2
Business Division	0	0
BusinessDepartment	1	4
Finance Division	0	0
General Affairs Division	0	1
General Section	2	0
ManagementDepartment	0	0
ProductionDepartment	0	3

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:



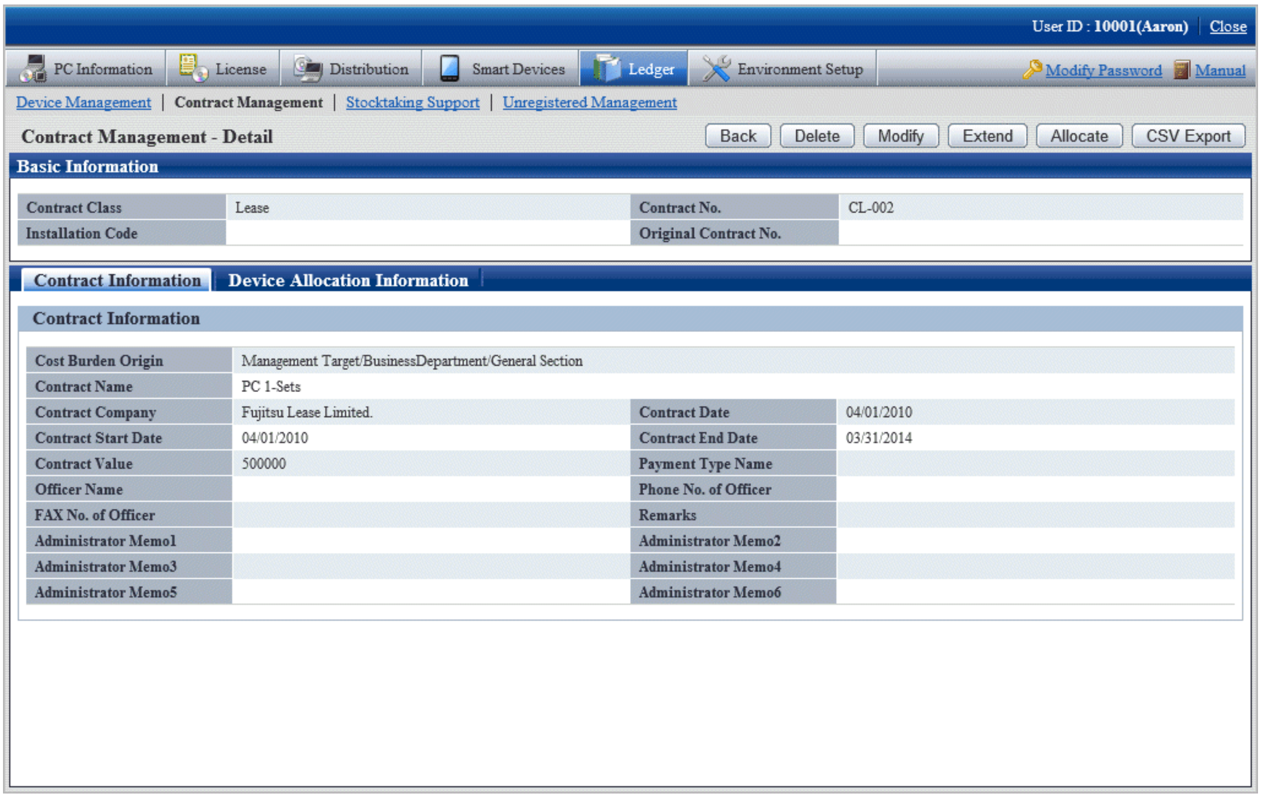
Detail of contract will be displayed when Contract No. is selected.

Contract Class	Contract No.	Cost Burden Origin	Number of Contracted Device(s)	Contract Name	Contract Da
Rental	CE-001	BusinessDepartment	4	PC 1-Sets	04/01/2010
Maintenance	CH-001	General Section	4	PC 1-Sets	04/01/2010
Lease	CL-002	General Section	4	PC 1-Sets	04/01/2010

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.	CL-002
Installation Code		Original Contract No.	

Contract Information

Cost Burden Origin	Management Target/BusinessDepartment/General Section		
Contract Name	PC 1-Sets		
Contract Company	Fujitsu Lease Limited.	Contract Date	04/01/2010
Contract Start Date	04/01/2010	Contract End Date	03/31/2014
Contract Value	500000	Payment Type Name	
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.

2.9.3 Stocktaking Support

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

- Confirm stocktaking status by section, type or location
- Change stocktaking state
- Stocktaking Operational Configuration
- Save device account of stocktaking status
- Correction of Place

Confirm stocktaking status by section, type or locating

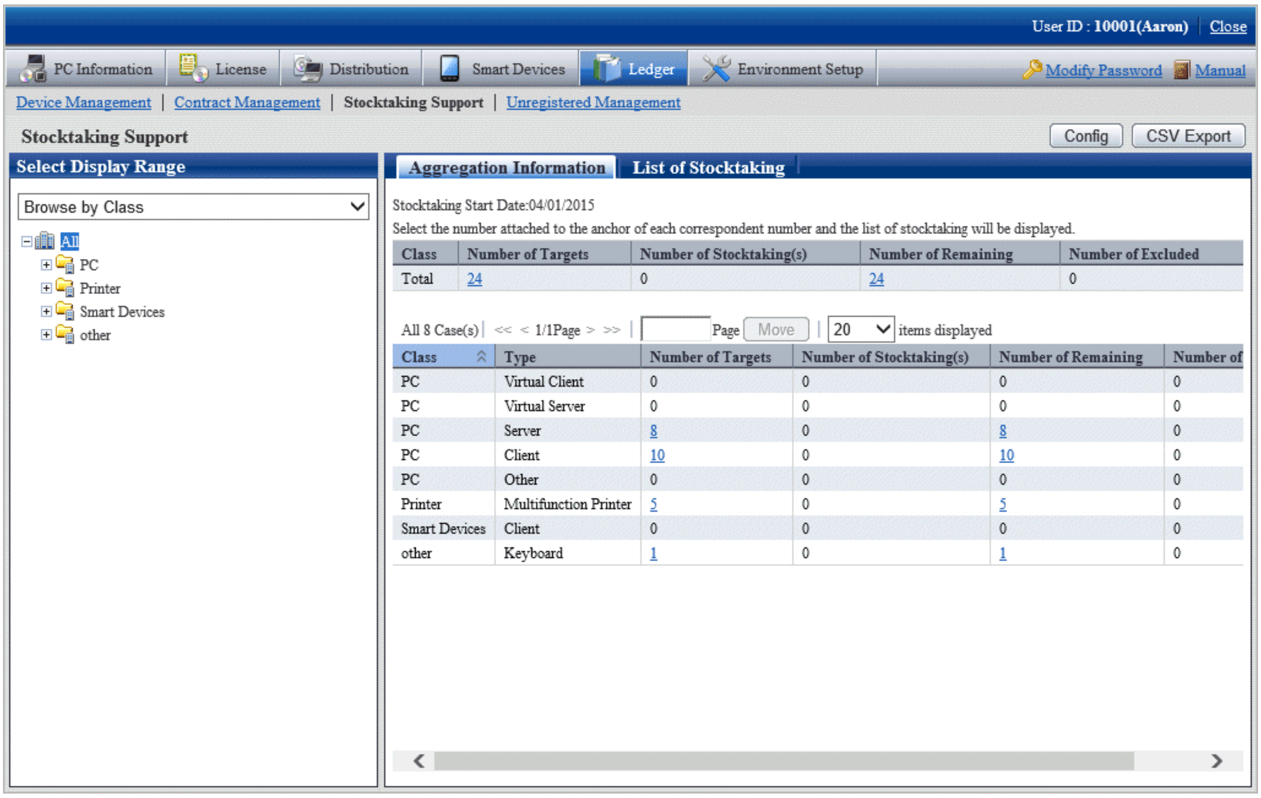
Display stocktaking status meeting the requirements of user operation.

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

Aggregation Information

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

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



Stocktaking Start Date:04/01/2015

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

Class	Number of Targets	Number of Stocktaking(s)	Number of Remaining	Number of Excluded
Total	24	0	24	0

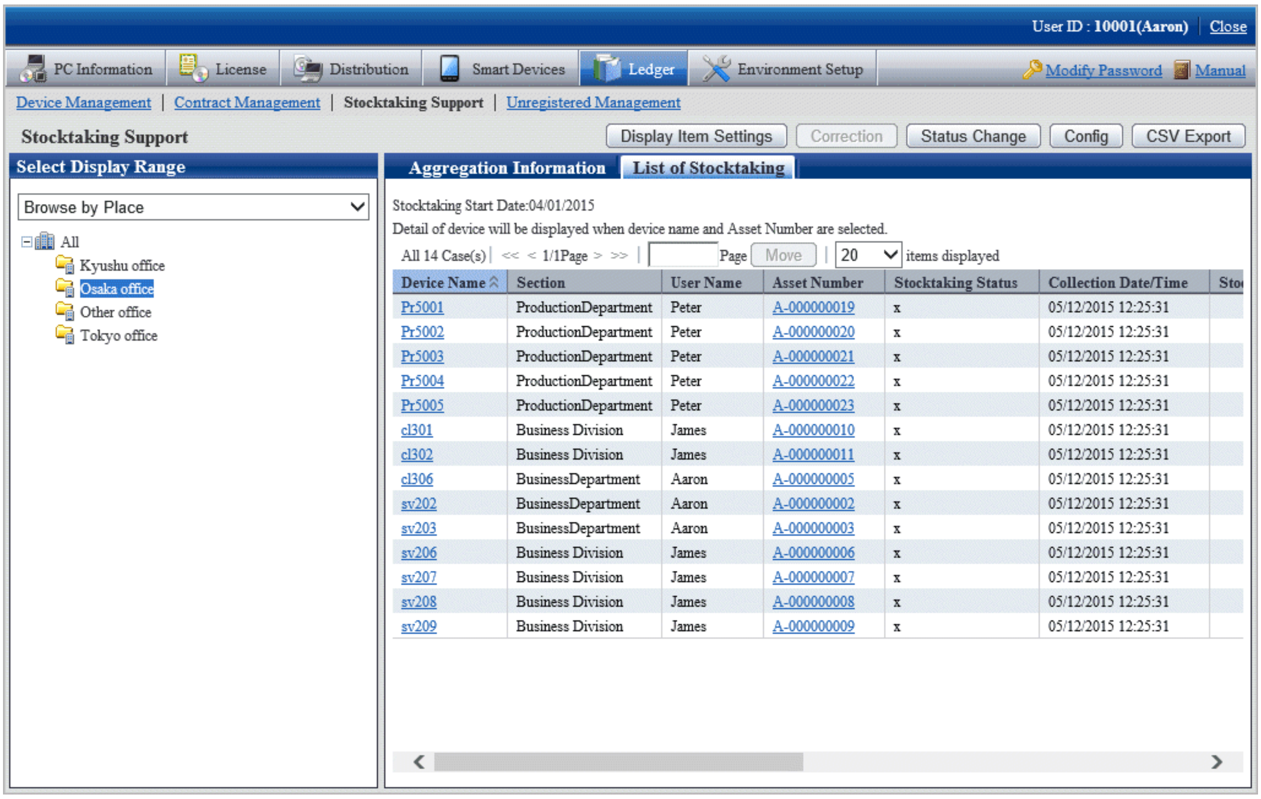
All 8 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Class	Type	Number of Targets	Number of Stocktaking(s)	Number of Remaining	Number of
PC	Virtual Client	0	0	0	0
PC	Virtual Server	0	0	0	0
PC	Server	8	0	8	0
PC	Client	10	0	10	0
PC	Other	0	0	0	0
Printer	Multifunction Printer	5	0	5	0
Smart Devices	Client	0	0	0	0
other	Keyboard	1	0	1	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:04/01/2015

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

All 14 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

Device Name	Section	User Name	Asset Number	Stocktaking Status	Collection Date/Time	Sto
Pr5001	ProductionDepartment	Peter	A-000000019	x	05/12/2015 12:25:31	
Pr5002	ProductionDepartment	Peter	A-000000020	x	05/12/2015 12:25:31	
Pr5003	ProductionDepartment	Peter	A-000000021	x	05/12/2015 12:25:31	
Pr5004	ProductionDepartment	Peter	A-000000022	x	05/12/2015 12:25:31	
Pr5005	ProductionDepartment	Peter	A-000000023	x	05/12/2015 12:25:31	
cl301	Business Division	James	A-000000010	x	05/12/2015 12:25:31	
cl302	Business Division	James	A-000000011	x	05/12/2015 12:25:31	
cl306	BusinessDepartment	Aaron	A-000000005	x	05/12/2015 12:25:31	
sv202	BusinessDepartment	Aaron	A-000000002	x	05/12/2015 12:25:31	
sv203	BusinessDepartment	Aaron	A-000000003	x	05/12/2015 12:25:31	
sv206	Business Division	James	A-000000006	x	05/12/2015 12:25:31	
sv207	Business Division	James	A-000000007	x	05/12/2015 12:25:31	
sv208	Business Division	James	A-000000008	x	05/12/2015 12:25:31	
sv209	Business Division	James	A-000000009	x	05/12/2015 12:25:31	

Change stocktaking status

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

- Set to **Stocktaking Completed**
- Set to **Stocktaking Uncompleted**
- Set to **Excluded Stocktaking**

Except **Stocktaking Completed** and **Stocktaking Uncompleted**, the devices not considered as stocktaking objects can be set as Set to **Excluded Stocktaking**.

Stocktaking operational configuration

Operational Configuration of stocktaking 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 **Stocktaking Completed** automatically. For example, when Systemwalker Desktop Patrol collects inventory information for inventory verification, the setup of the stocktaking object devices will turn into **Stocktaking Completed**.

After the stocktaking start date is set, the system administrator can confirm stocktaking status of the PC according to the inventory information collected in Systemwalker Desktop Patrol, or confirm stocktaking 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 stocktaking objects are remote devices, the system administrator can set the object devices as **Stocktaking Completed** in the stocktaking status display window when it is impossible to carry out stocktaking according to the inventory information collected in Systemwalker Desktop Patrol. On the contrary, the devices set as **Stocktaking Completed** shall be restored to **Stocktaking Uncompleted**.

The system administrator can change the setups (**Stocktaking Completed**/**Stocktaking Uncompleted**) to support various applications.

Save device account of stocktaking status

Save stocktaking status (aggregation information, stocktaking 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 stocktaking, and reflect the Setup Place to the assets device account simply and correctly.

2.9.4 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.

Note

This function automatically detects devices with IPv4 addresses only, and devices with IPv6 addresses are not subject to its detection.

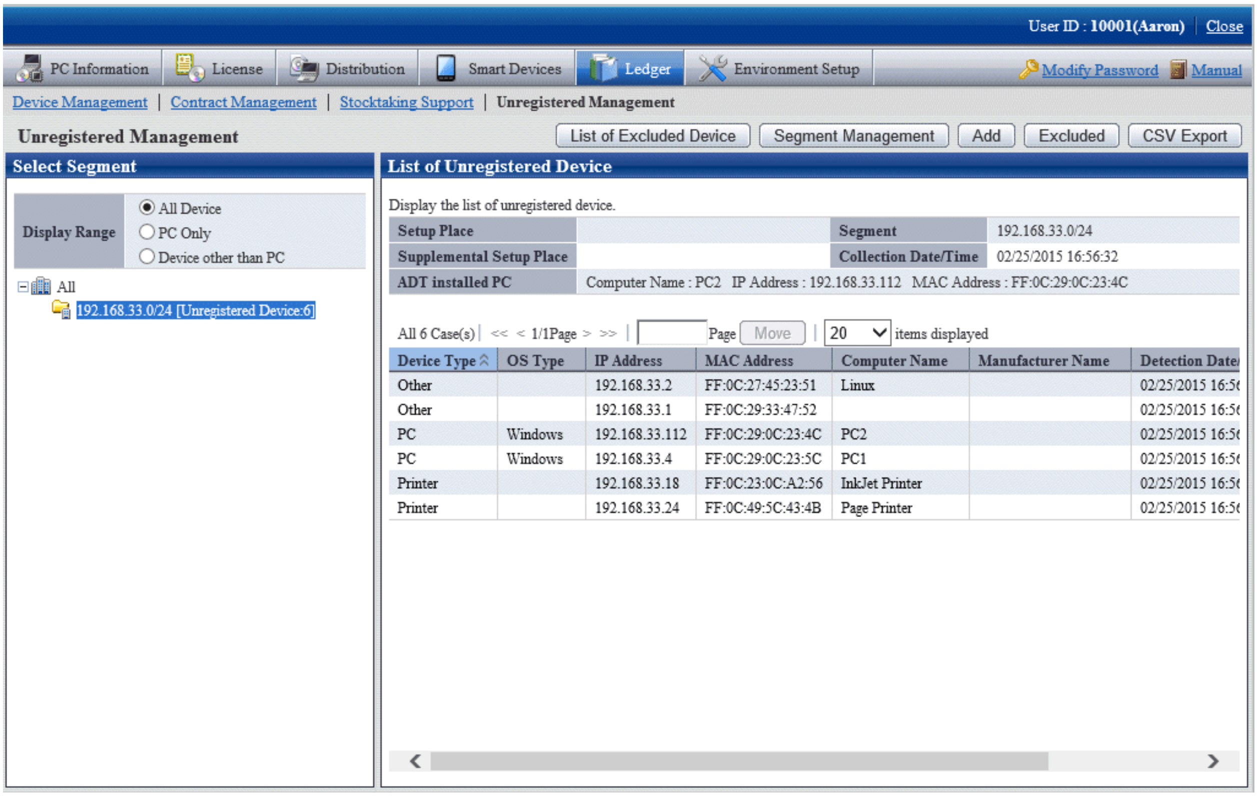
Register the unregistered devices in the unregistered device management window. Alternatively, the administrator can also export the unregistered devices to a file for registration at one time.

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.



User ID : 10001(Aaron) | Close
PC Information
License
Distribution
Smart Devices
Ledger
Environment Setup
Modify Password
Manual
Device Management | Contract Management | Stocktaking Support | Unregistered Management
Unregistered Management
List of Excluded Device
Segment Management
Add
Excluded
CSV Export
Select Segment
All
192.168.33.0/24 [Unregistered Device:6]
List of Unregistered Device
All 6 Case(s) | << < 1/1Page > >> | Page Move | 20 items displayed

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

Display the list of unregistered device.

Setup Place		Segment	192.168.33.0/24
Supplemental Setup Place		Collection Date/Time	02/25/2015 16:56:32
ADT installed PC	Computer Name : PC2 IP Address : 192.168.33.112 MAC Address : FF:0C:29:0C:23:4C		

Device Type	OS Type	IP Address	MAC Address	Computer Name	Manufacturer Name	Detection Date
Other		192.168.33.2	FF:0C:27:45:23:51	Linux		02/25/2015 16:5
Other		192.168.33.1	FF:0C:29:33:47:52			02/25/2015 16:5
PC	Windows	192.168.33.112	FF:0C:29:0C:23:4C	PC2		02/25/2015 16:5
PC	Windows	192.168.33.4	FF:0C:29:0C:23:5C	PC1		02/25/2015 16:5
Printer		192.168.33.18	FF:0C:23:0C:A2:56	InkJet Printer		02/25/2015 16:5
Printer		192.168.33.24	FF:0C:49:5C:43:4B	Page Printer		02/25/2015 16:5

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.

2.10 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

2.10.1 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(R) 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(R) 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. stocktaking) 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)

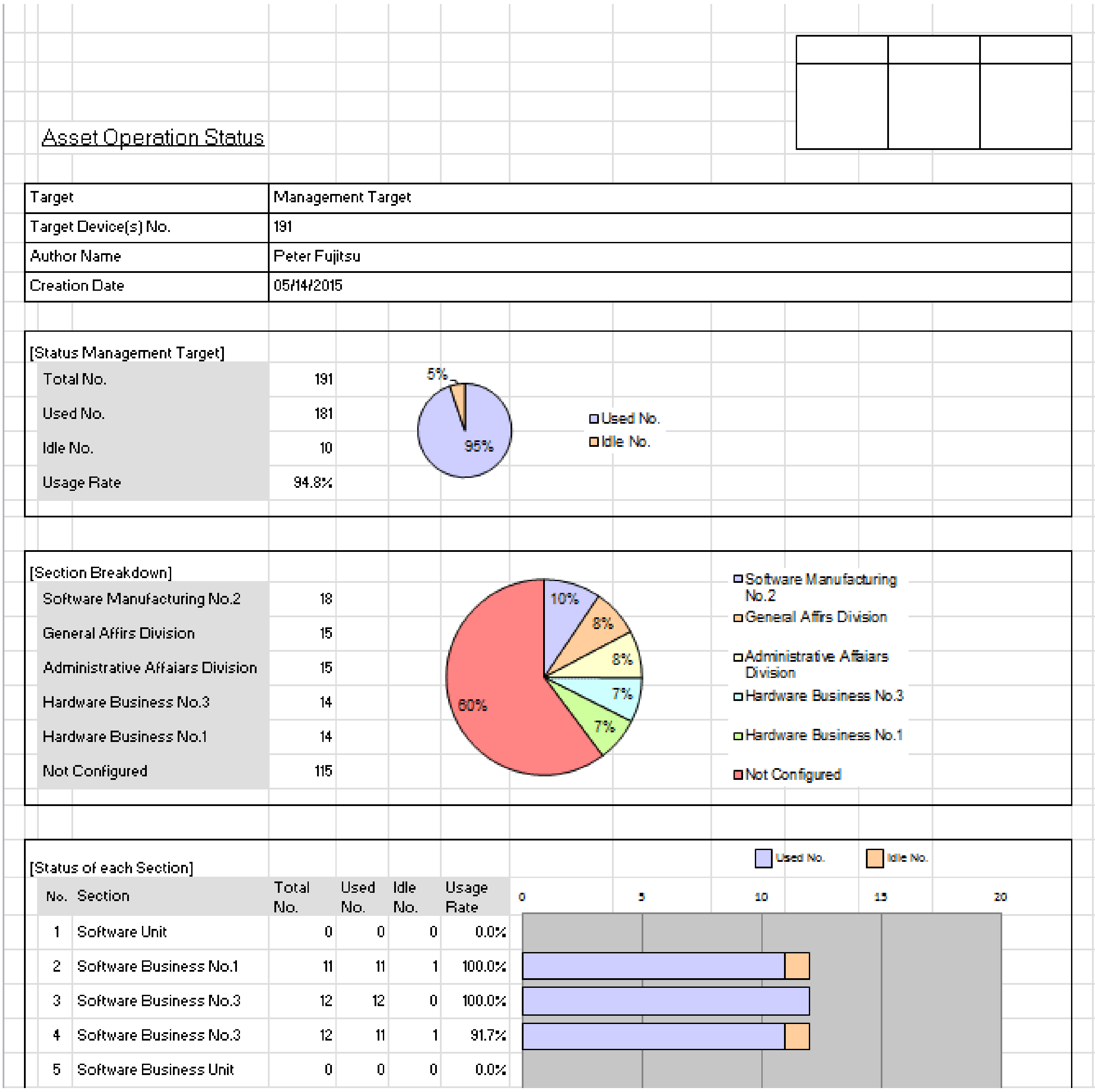
- stocktaking status

  Output the stocktaking 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:



Asset Operation Status

Target	Management Target
Target Device(s) No.	191
Author Name	Peter Fujitsu
Creation Date	05/14/2015

[Status Management Target]

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

[Section Breakdown]

Software Manufacturing No.2	18
General Affirs Division	15
Administrative Affaiars Division	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 No.1	11	11	1	100.0%
3	Software Business No.3	12	12	0	100.0%
4	Software Business No.3	12	11	1	91.7%
5	Software Business Unit	0	0	0	0.0%

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(R) Excel after the output data is saved in the form of report (Microsoft(R) Excel format).

2.10.2 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 Period is 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.

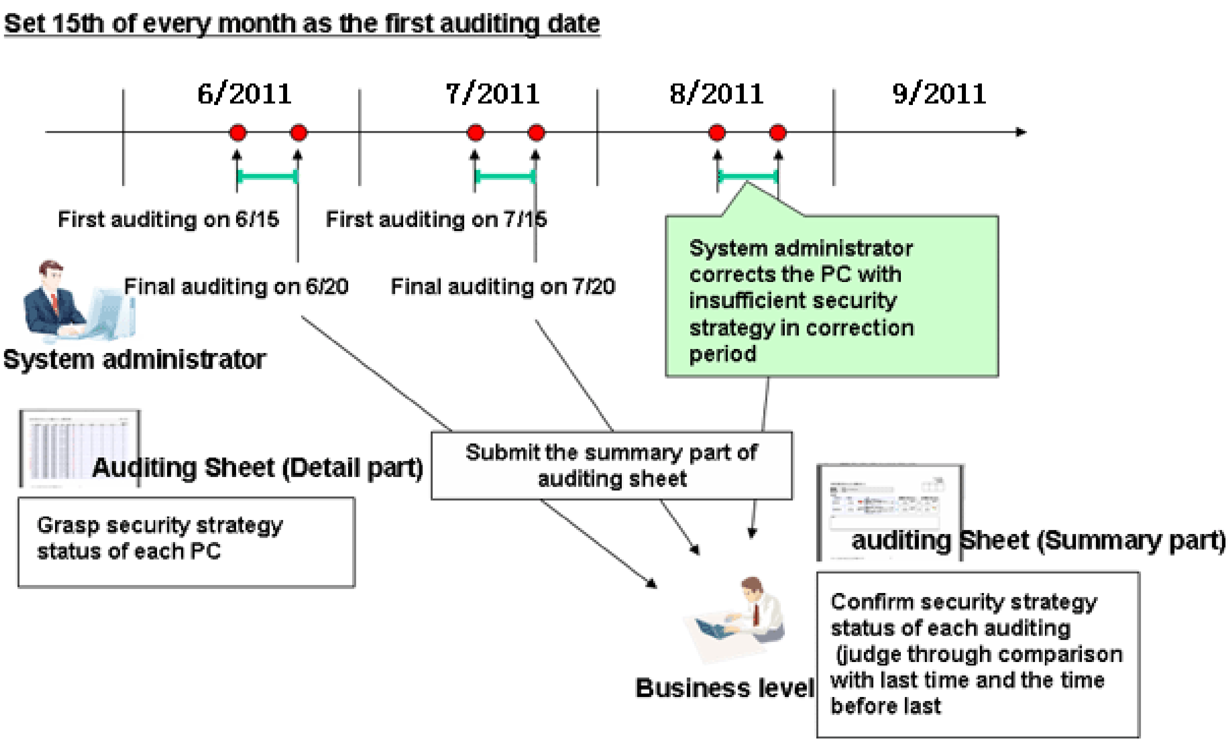
It is recommended that security auditing date and correction date should be set in Systemwalker Desktop Patrol so as to carry out periodic security auditing.

Security auditing can be carried out by schedule at night.

Application pattern

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
System administrator corrects the PC with insufficient security strategy in correction period
Auditing Sheet (Detail part)
Submit the summary part of auditing sheet
Grasp security strategy status of each PC
auditing Sheet (Summary part)
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 every day during the rectification period, and security countermeasure shall be taken if the auditing result shows that the PC is not secure enough.

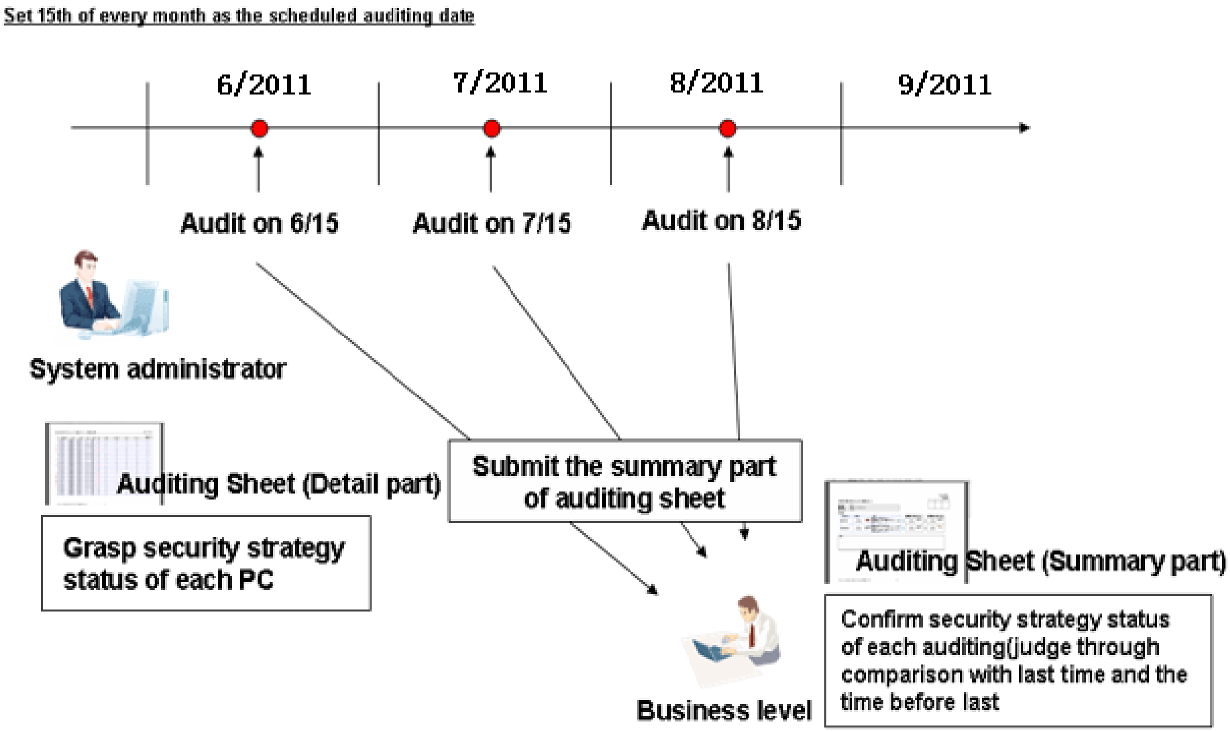
   After taking security countermeasures collect the inventory information from the PC and confirm no any problem exists according to the security auditing report.
3. On the last auditing date, output the final security auditing data as a security auditing report.

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.

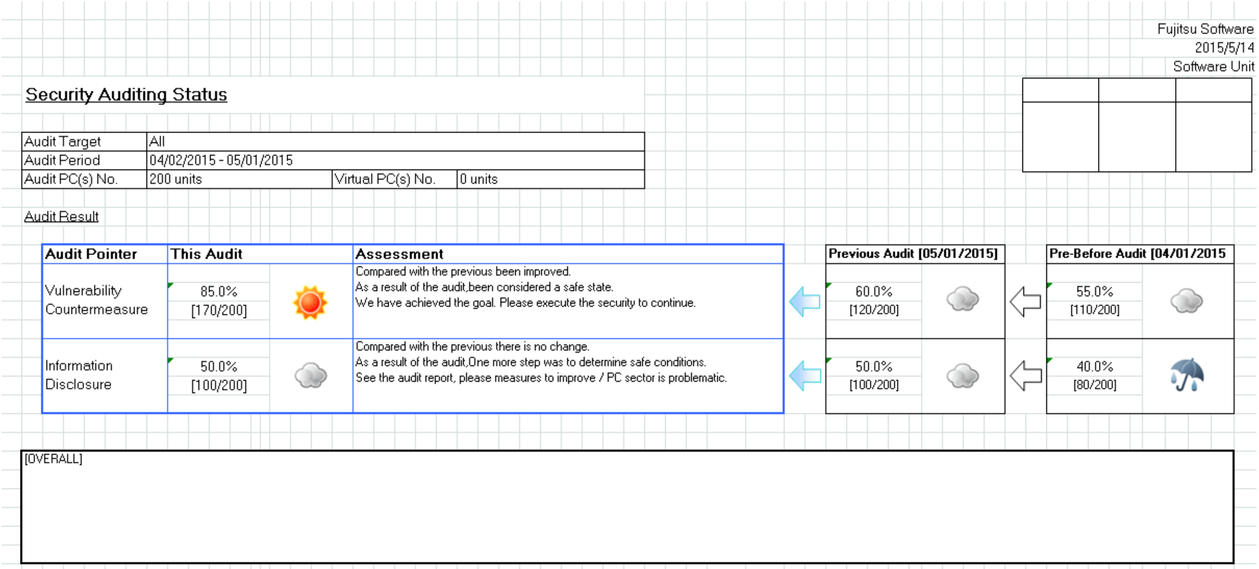

Set 15th of every month as the scheduled auditing date
6/2011
7/2011
8/2011
9/2011
Audit on 6/15
Audit on 7/15
Audit on 8/15
System administrator
Auditing Sheet (Detail part)
Grasp security strategy status of each PC
Submit the summary part of auditing sheet
Auditing Sheet (Summary part)
Confirm security 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 an 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
2015/5/14
Software Unit

Security Auditing Status

Audit Target	All		
Audit Period	04/02/2015 - 05/01/2015		
Audit PC(s) No.	200 units	Virtual PC(s) No.	0 units

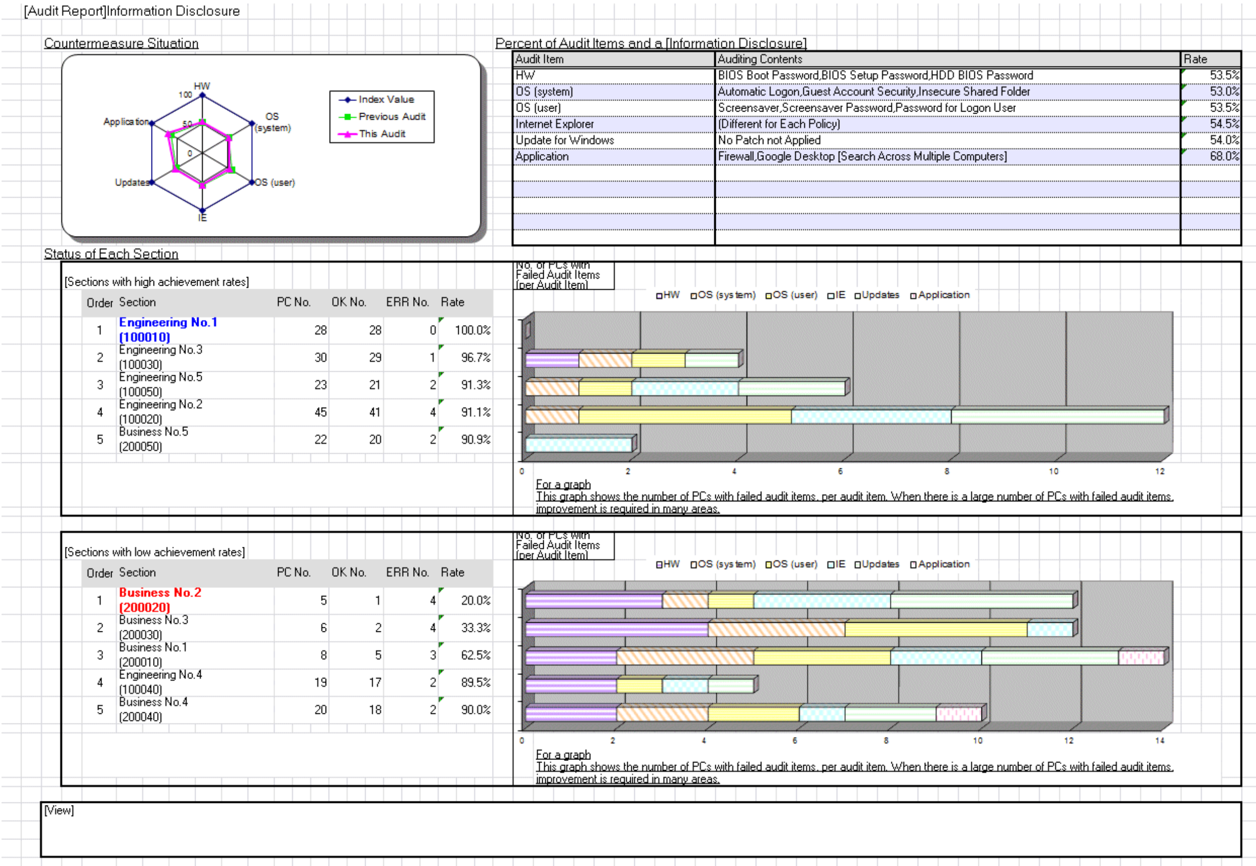
Audit Result

Audit Pointer	This Audit		Assessment		Previous Audit [05/01/2015]			Pre-Before Audit [04/01/2015	
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 group with high achievement rate having a higher percentage of OK events and the group with low achievement rate having a higher percentage of ERR events, to urge the group taking insufficient security countermeasures to correct security countermeasures.



[Audit Report]Information Disclosure

Countermeasure Situation

Percent of Audit Items and a [Information Disclosure]

Audit Item	Auditing Contents	Rate
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

[Sections with high achievement rates]

Order	Section	PC No.	OK No.	ERR No.	Rate
1	**Engineering No.1 (100010)**	28	28	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%

No. of PCs with Failed Audit Items (per Audit Item)

For a graph
This graph shows the number of PCs with failed audit items, per audit item. When there is a large number of PCs with failed audit items, improvement is required in many areas.

[Sections with low achievement rates]

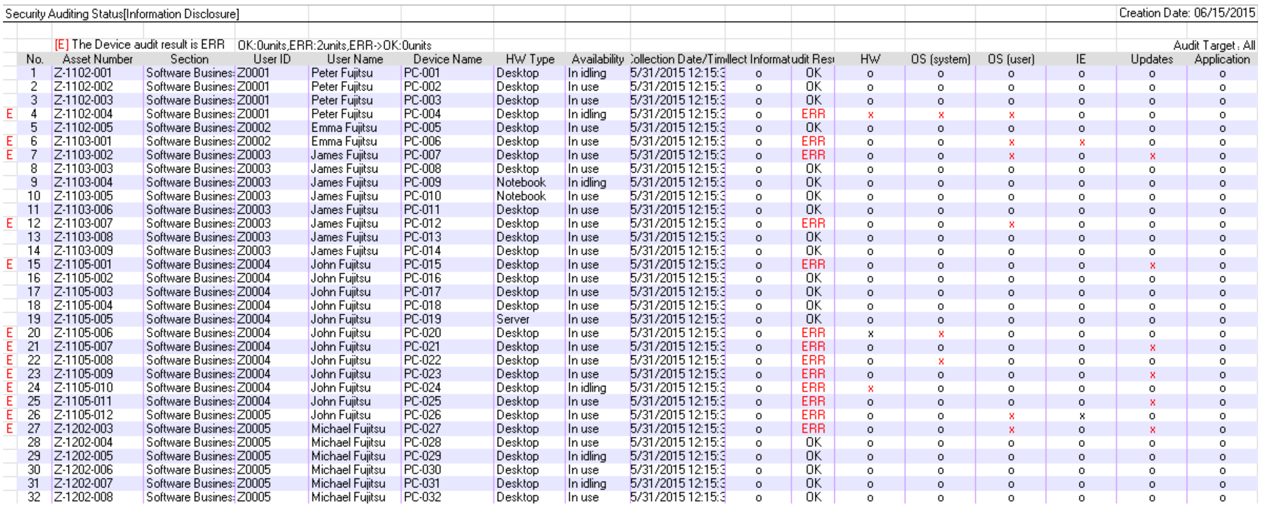
Order	Section	PC No.	OK No.	ERR No.	Rate
1	**Business No.2 (200020)**	5	1	4	20.0%
2	Business No.3 (200030)	6	2	4	33.3%
3	Business No.1 (200010)	8	5	3	62.5%
4	Engineering No.4 (100040)	19	17	2	89.5%
5	Business No.4 (200040)	20	18	2	90.0%

No. of PCs with Failed Audit Items (per Audit Item)

For a graph
This graph shows the number of PCs with failed audit items, per audit item. When there is a large number of PCs with failed audit items, improvement is required in many areas.

[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.



Security Auditing Status[Information Disclosure]

Creation Date: 06/15/2015

[E] The Device audit result is ERR OK:0units,ERR:2units,ERR->OK:0units

Audit Target : All

	No.	Asset Number	Section	User ID	User Name	Device Name	HW Type	Availability	:ollection Date/Tim	llect Informat	udit Resı	HW	OS (system)	OS (user)	IE	Updates	Application
	1	Z-1102-001	Software Busines	Z0001	Peter Fujitsu	PC-001	Desktop	In idling	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	2	Z-1102-002	Software Busines	Z0001	Peter Fujitsu	PC-002	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	3	Z-1102-003	Software Busines	Z0001	Peter Fujitsu	PC-003	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
E	4	Z-1102-004	Software Busines	Z0001	Peter Fujitsu	PC-004	Desktop	In idling	5/31/2015 12:15:3	o	ERR	x	x	x	o	o	o
	5	Z-1102-005	Software Busines	Z0002	Emma Fujitsu	PC-005	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
E	6	Z-1103-001	Software Busines	Z0002	Emma Fujitsu	PC-006	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	x	x	o	o
E	7	Z-1103-002	Software Busines	Z0003	James Fujitsu	PC-007	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	x	o	x	o
	8	Z-1103-003	Software Busines	Z0003	James Fujitsu	PC-008	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	9	Z-1103-004	Software Busines	Z0003	James Fujitsu	PC-009	Notebook	In idling	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	10	Z-1103-005	Software Busines	Z0003	James Fujitsu	PC-010	Notebook	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	11	Z-1103-006	Software Busines	Z0003	James Fujitsu	PC-011	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
E	12	Z-1103-007	Software Busines	Z0003	James Fujitsu	PC-012	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	x	o	o	o
	13	Z-1103-008	Software Busines	Z0003	James Fujitsu	PC-013	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	14	Z-1103-009	Software Busines	Z0003	James Fujitsu	PC-014	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
E	15	Z-1105-001	Software Busines	Z0004	John Fujitsu	PC-015	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	o	o	x	o
	16	Z-1105-002	Software Busines	Z0004	John Fujitsu	PC-016	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	17	Z-1105-003	Software Busines	Z0004	John Fujitsu	PC-017	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	18	Z-1105-004	Software Busines	Z0004	John Fujitsu	PC-018	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	19	Z-1105-005	Software Busines	Z0004	John Fujitsu	PC-019	Server	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
E	20	Z-1105-006	Software Busines	Z0004	John Fujitsu	PC-020	Desktop	In use	5/31/2015 12:15:3	o	ERR	x	x	o	o	o	o
E	21	Z-1105-007	Software Busines	Z0004	John Fujitsu	PC-021	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	o	o	x	o
E	22	Z-1105-008	Software Busines	Z0004	John Fujitsu	PC-022	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	x	o	o	o	o
E	23	Z-1105-009	Software Busines	Z0004	John Fujitsu	PC-023	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	o	o	x	o
E	24	Z-1105-010	Software Busines	Z0004	John Fujitsu	PC-024	Desktop	In idling	5/31/2015 12:15:3	o	ERR	x	o	o	o	o	o
E	25	Z-1105-011	Software Busines	Z0004	John Fujitsu	PC-025	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	o	o	x	o
E	26	Z-1105-012	Software Busines	Z0005	John Fujitsu	PC-026	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	x	x	o	o
E	27	Z-1202-003	Software Busines	Z0005	Michael Fujitsu	PC-027	Desktop	In use	5/31/2015 12:15:3	o	ERR	o	o	x	o	x	o
	28	Z-1202-004	Software Busines	Z0005	Michael Fujitsu	PC-028	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	29	Z-1202-005	Software Busines	Z0005	Michael Fujitsu	PC-029	Desktop	In idling	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	30	Z-1202-006	Software Busines	Z0005	Michael Fujitsu	PC-030	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	31	Z-1202-007	Software Busines	Z0005	Michael Fujitsu	PC-031	Desktop	In idling	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o
	32	Z-1202-008	Software Busines	Z0005	Michael Fujitsu	PC-032	Desktop	In use	5/31/2015 12:15:3	o	OK	o	o	o	o	o	o

2.10.3 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 ICT countermeasures.

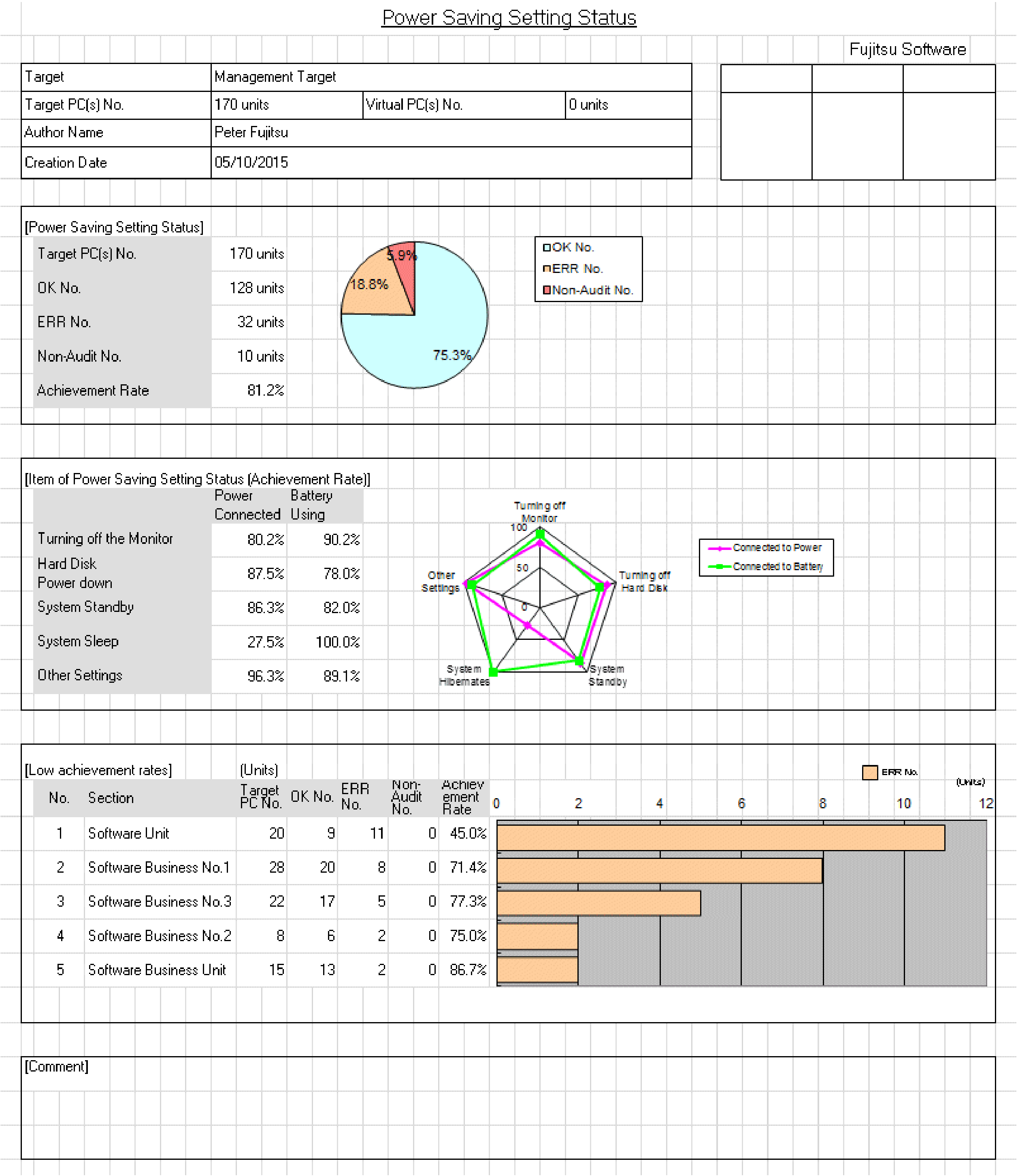
In addition, the power saving auditing result can be output in the form of report and used as attestation of correct execution of power saving countermeasures.

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	05/10/2015		

[Power Saving Setting Status]

Target PC(s) No.	170 units
OK No.	128 units
ERR 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%

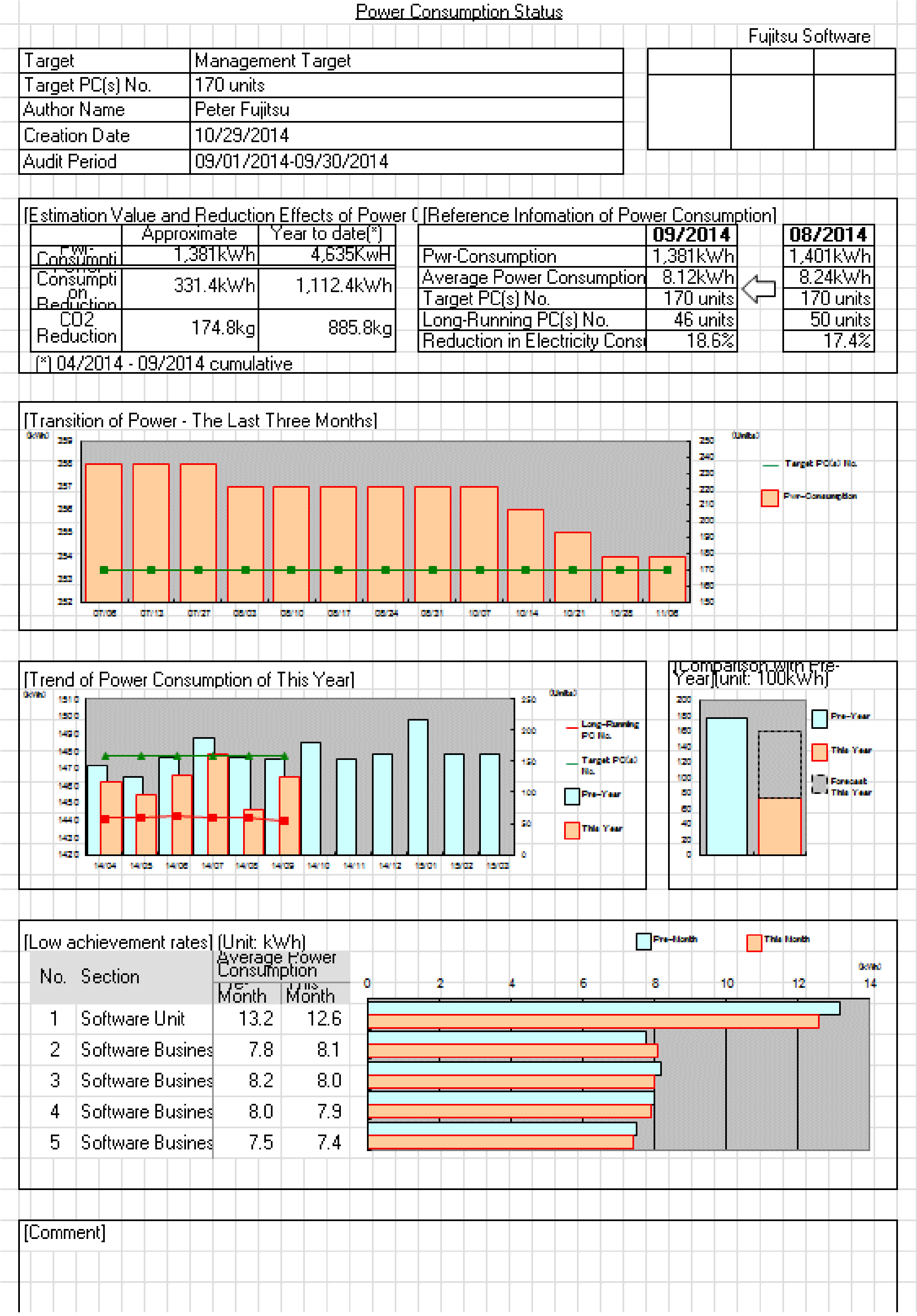
[Low achievement rates]

No.	Section	Target PC No.	OK No.	ERR 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%

(Units)

[Comment]

- Power consumption auditing report



Power Consumption Status

Fujitsu Software

Target	Management Target
Target PC(s) No.	170 units
Author Name	Peter Fujitsu
Creation Date	10/29/2014
Audit Period	09/01/2014-09/30/2014

[Estimation Value and Reduction Effects of Power (

	Approximate	Year to date(*)
Pwr- Consumpti	1,381kWh	4,635KwH
Consumpti on Reduction	331.4kWh	1,112.4kWh
CO2 Reduction	174.8kg	885.8kg

(*) 04/2014 - 09/2014 cumulative

[Reference Infomation of Power Consumption]

	09/2014	08/2014
Pwr-Consumption	1,381kWh	1,401kWh
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 Cons	18.6%	17.4%

[Transition of Power - The Last Three Months]

[Trend of Power Consumption of This Year]

[Comparison with Pre-Year](unit: 100kWh)

[Low achievement rates] (Unit: kWh)

No.	Section	Average Power Consumption	
		Pre- Month	This Month
1	Software Unit	13.2	12.6
2	Software Busines	7.8	8.1
3	Software Busines	8.2	8.0
4	Software Busines	8.0	7.9
5	Software Busines	7.5	7.4

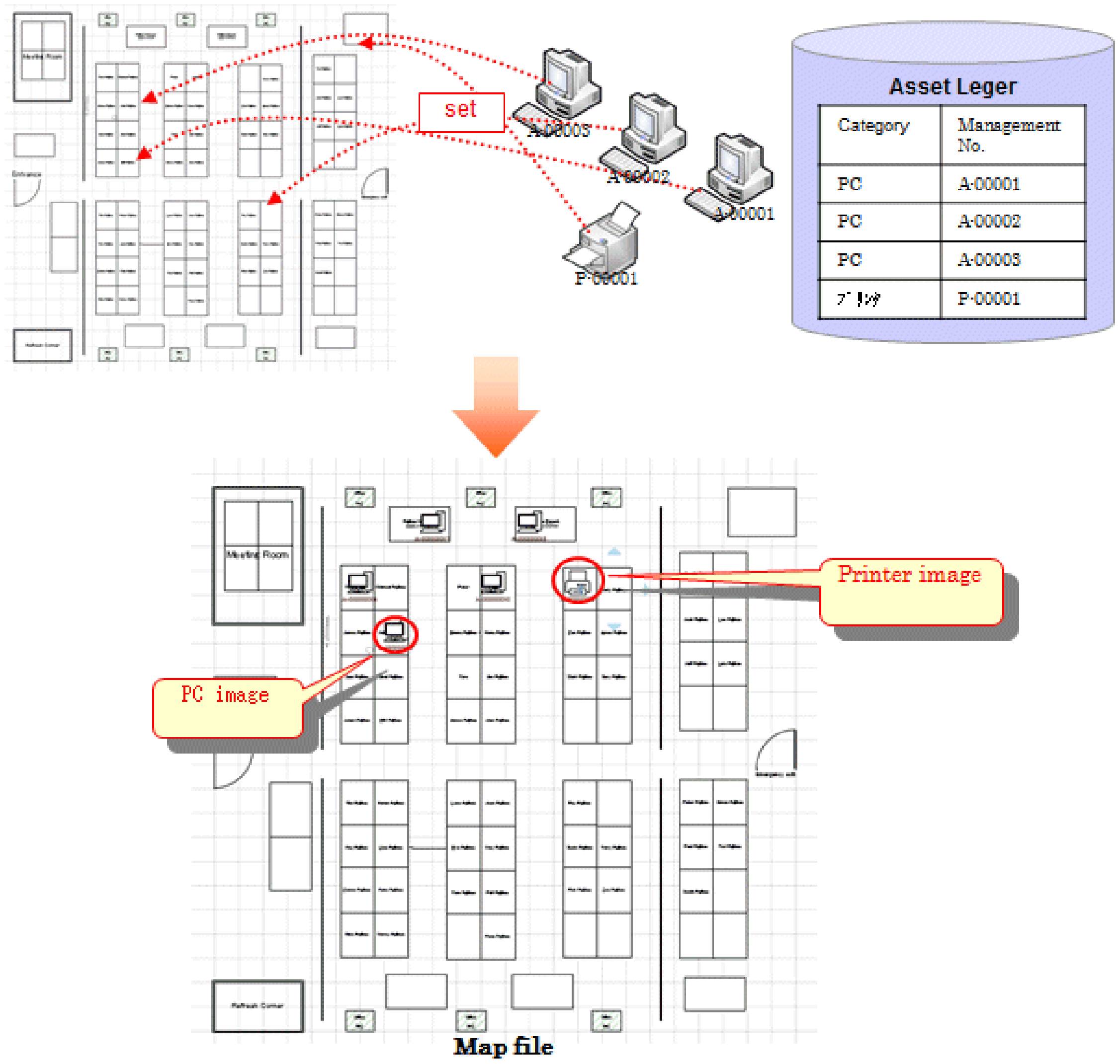
[Comment]

2.11 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(R) Office Visio(R) is necessary for performing device management according to the location map.



Category	Management No.
PC	A-00001
PC	A-00002
PC	A-00003
ﾌﾟﾘﾝﾀ	P-00001

2.12 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.

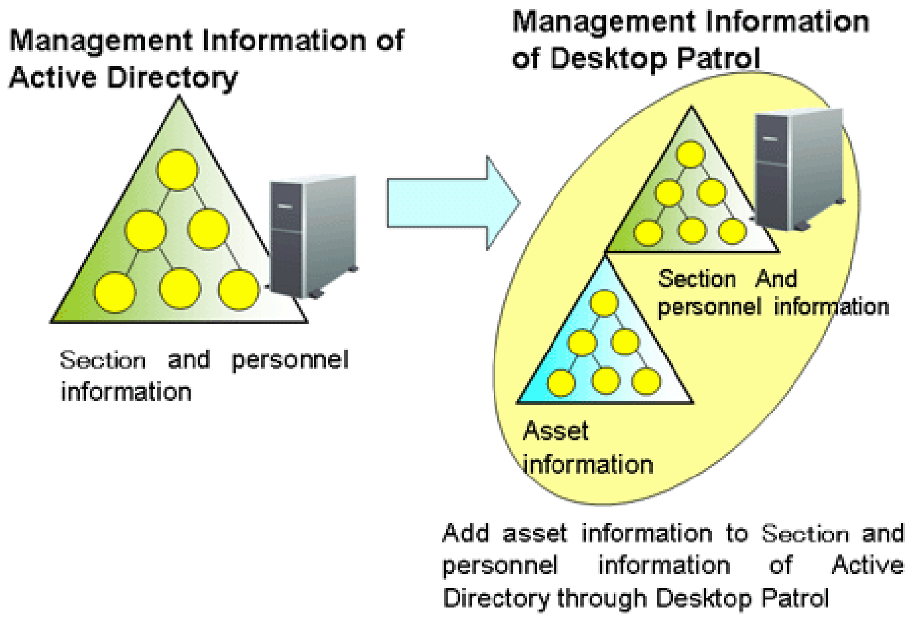
Active Directory linkage function

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.

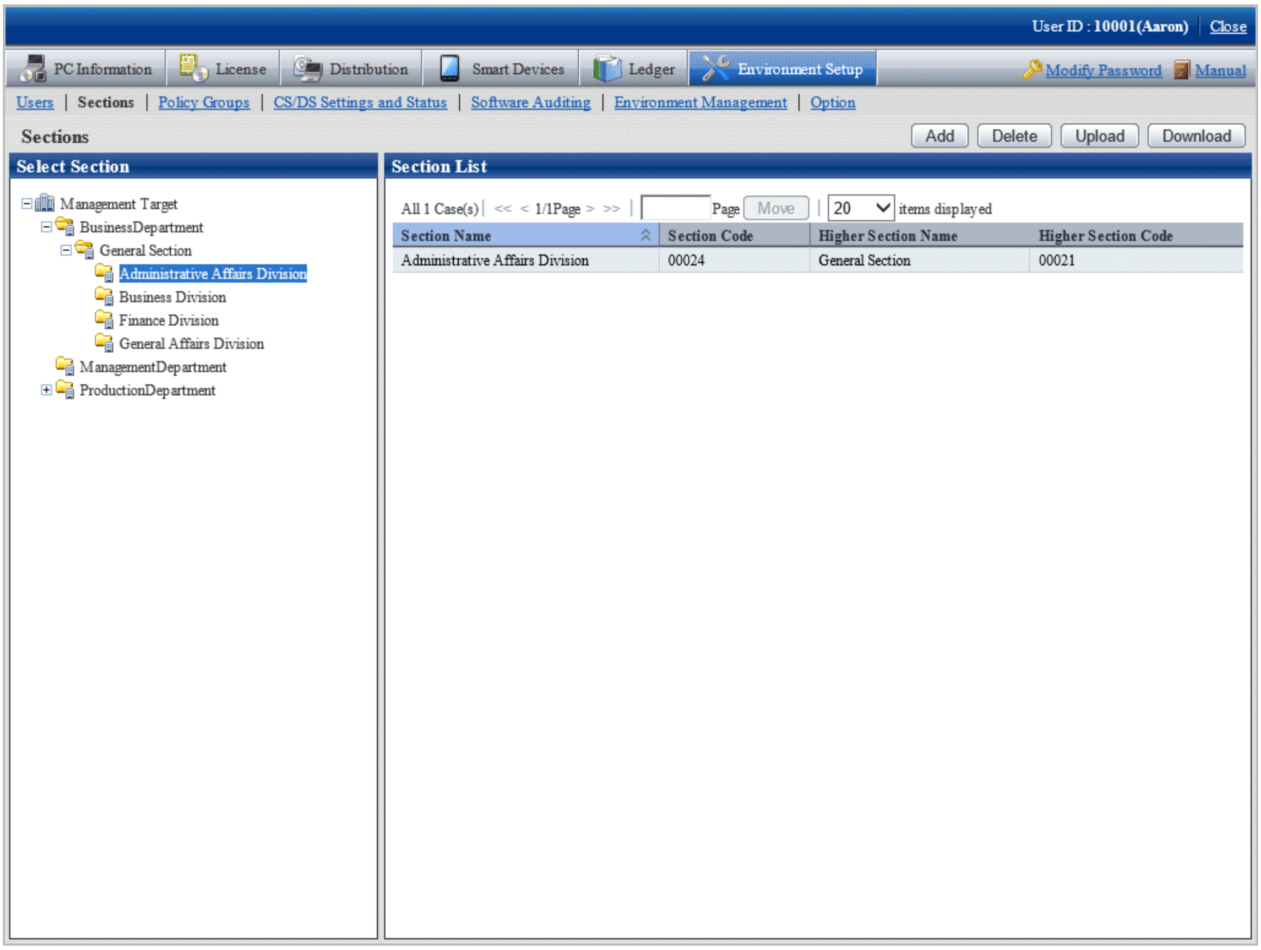
However, linkage with Active Directory is only limited to single domain application. Active Directory cannot link with Desktop Patrol in multi-domain application.

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.

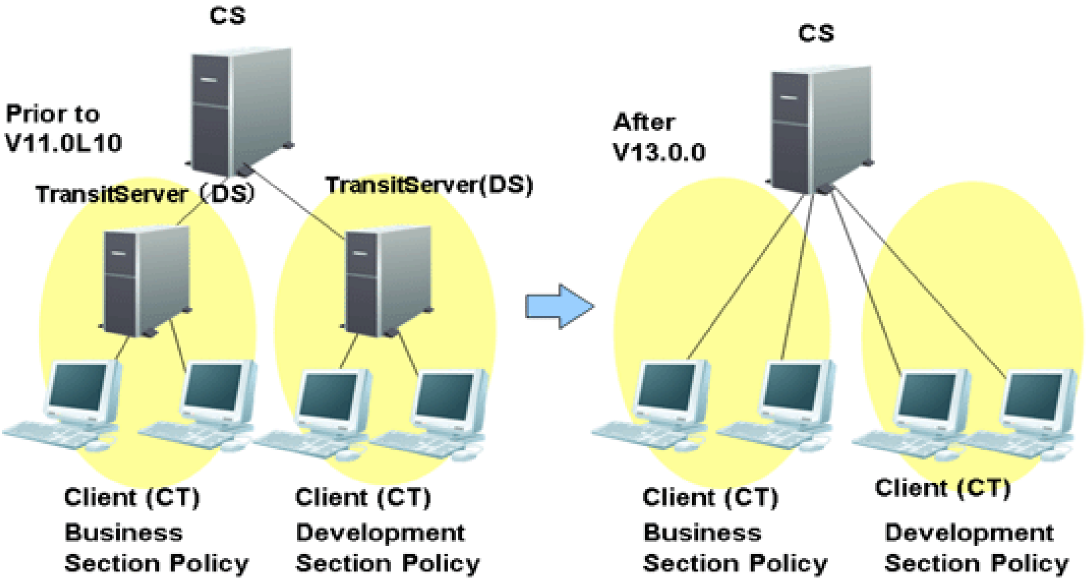


- Management Target
  - BusinessDepartment
    - General Section
      - Administrative Affairs Division
      - Business Division
      - Finance Division
      - General Affairs Division
  - ManagementDepartment
  - ProductionDepartment

Section Name	Section Code	Higher Section Name	Higher Section Code
Administrative Affairs Division	00024	General Section	00021

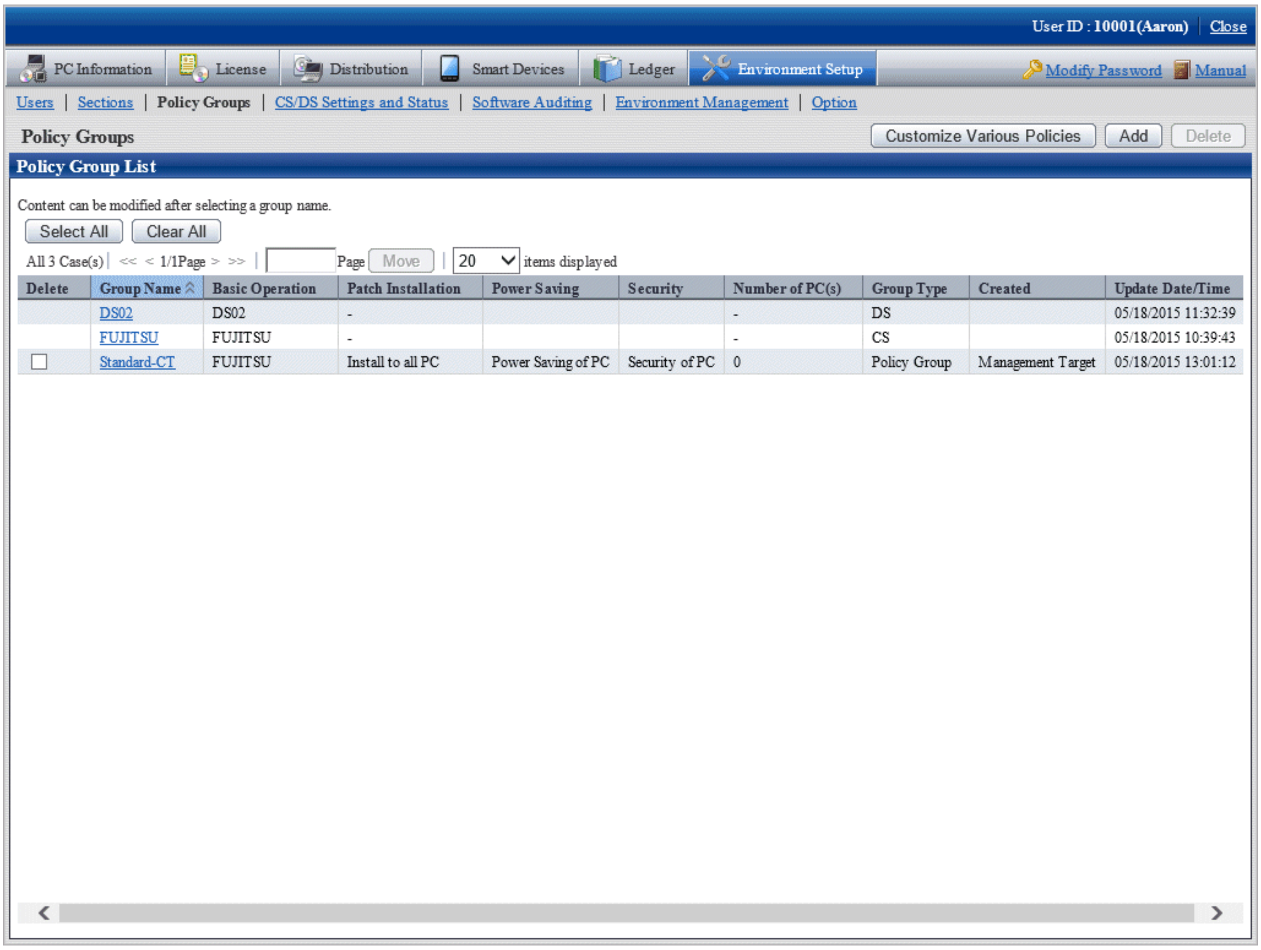
Policy group management

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.



Policy Groups

Policy Group List

Content can be modified after selecting a group name.

All 3 Case(s) << < 1/1Page > >> Page 20 items displayed

Delete	Group Name	Basic Operation	Patch Installation	Power Saving	Security	Number of PC(s)	Group Type	Created	Update Date/Time
	DS02	DS02	-			-	DS		05/18/2015 11:32:39
	FUJITSU	FUJITSU	-			-	CS		05/18/2015 10:39:43
☐	Standard-CT	FUJITSU	Install to all PC	Power Saving of PC	Security of PC	0	Policy Group	Management Target	05/18/2015 13:01:12

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 "1.3.2 Software Dictionary" for details.

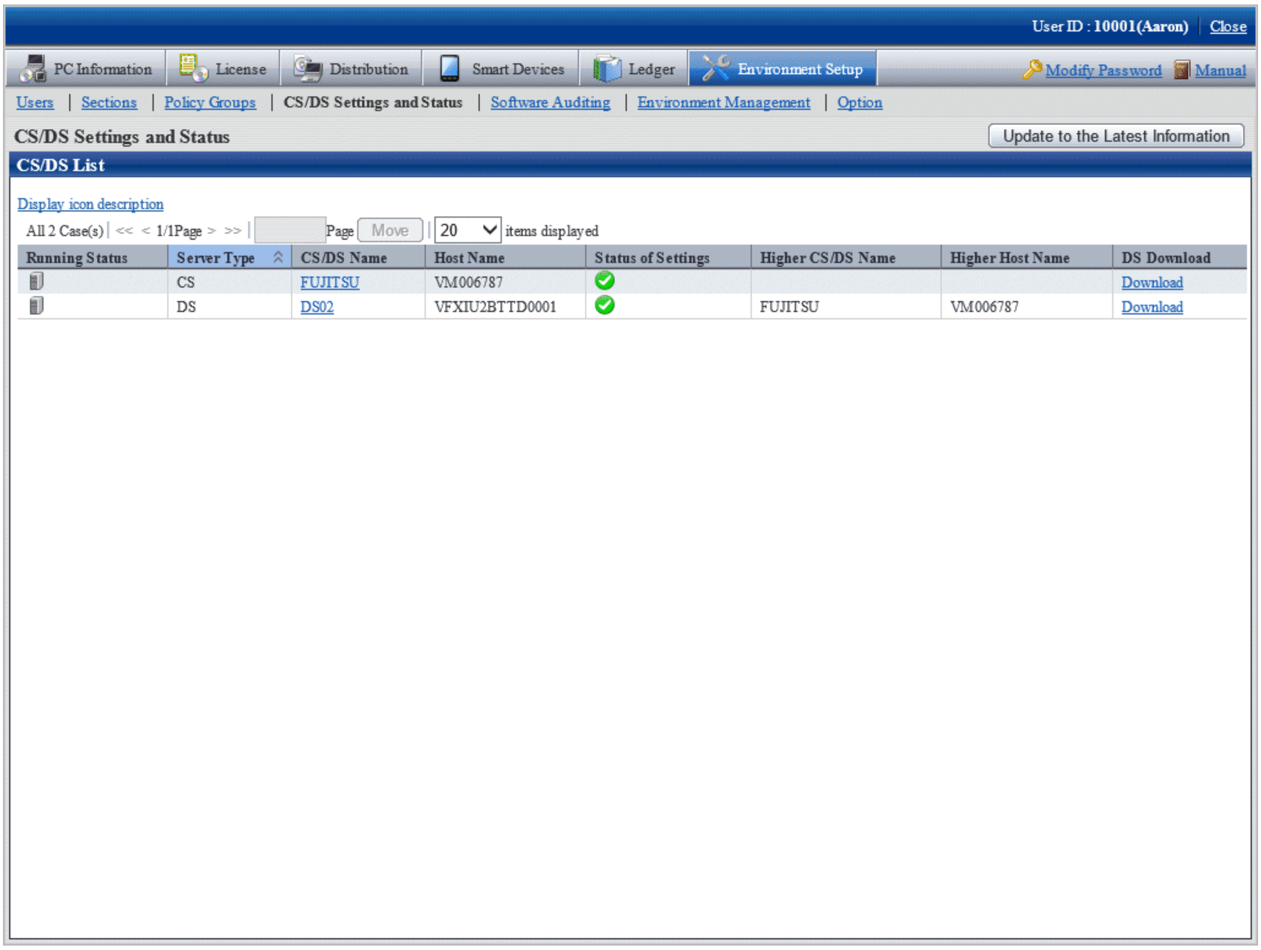
- Software dictionary defined by user

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.

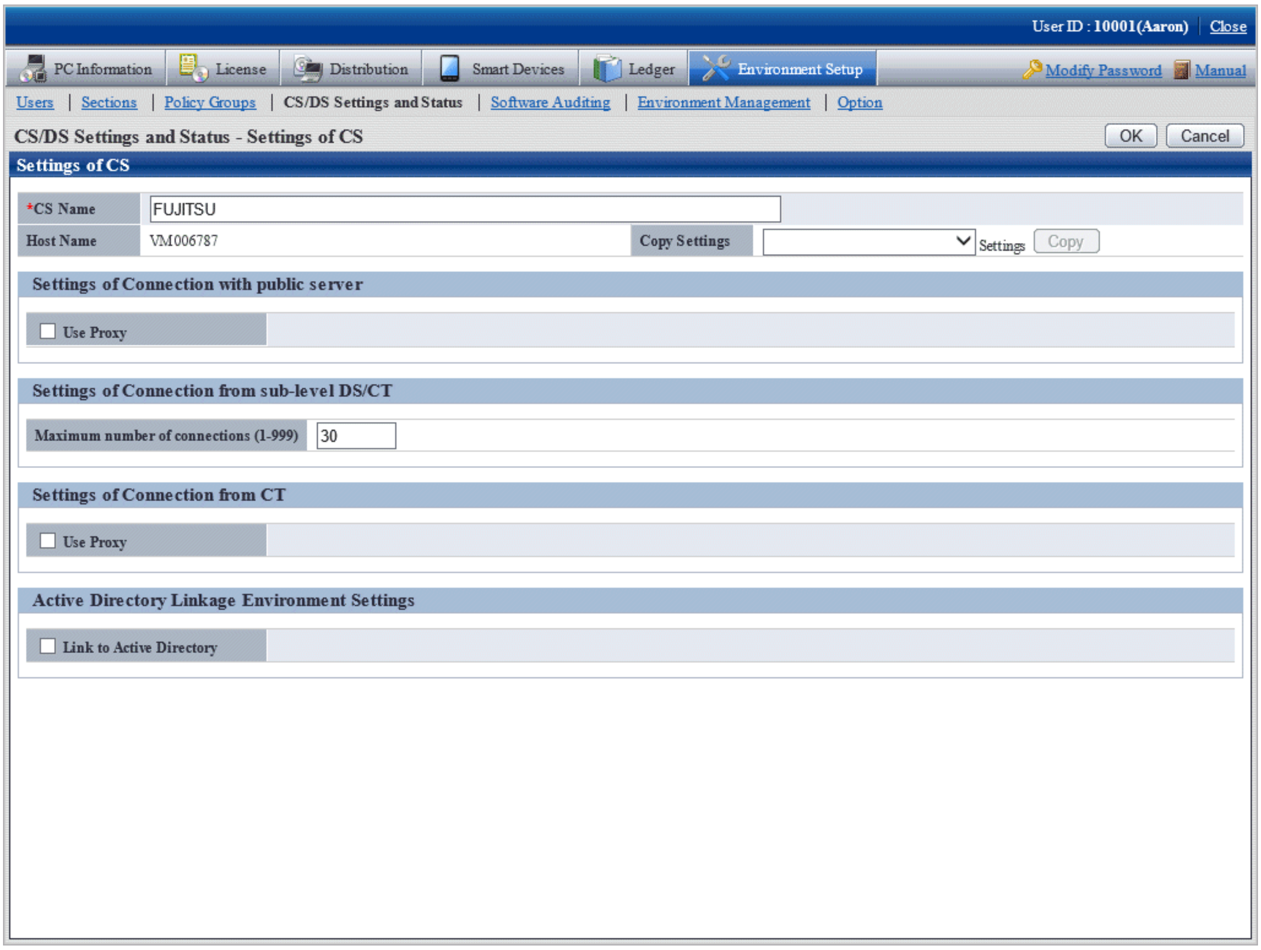


CS/DS Settings and Status

CS/DS List

Running Status	Server Type	CS/DS Name	Host Name	Status of Settings	Higher CS/DS Name	Higher Host Name	DS Download
▯	CS	FUJITSU	VM006787	✓			Download
▯	DS	DS02	VFXIU2BTTD0001	✓	FUJITSU	VM006787	Download

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



CS/DS Settings and Status - Settings of CS

Settings of CS

*CS Name	FUJITSU		
Host Name	VM006787	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)	30

Settings of Connection from CT

☐ Use Proxy

Active Directory Linkage Environment Settings

☐ Link to Active Directory

2.13 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 cannot 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.

2.14 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 distribution objects. It is not necessary for DS and CT administrators to carry out the application operation because this is automatic application.

2.15 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 Pane**l > **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 Remove Programs** window or **Programs and Features** > **Uninstall a program** 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

  Intel(R) Xeon(R) E5503 2GHz or higher

- Required memory capacity

Note

To import the data registered in the SAMAC Software Dictionary to the CS, at least 384 MB of memory is required.

- Required disk capacity (Note 1) (Note 4)

  720 MB (installation destination) + 90 MB (required by the system drive to store the runtime library) + the size of registered software or more+ the size of registered patches (Note 2) + the size of CT operation status log (Note 3) + 100MB (Note 4)

  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

Number of PC(s)	EXE Information Collection	Software Operation Status Collection	Database Capacity
	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 x User quantity x Save days

Note 4: The disk capacity required for installing and managing the software.
This space is secured under <*system drive*>\FujitsuF4CR.

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, properly set the maximum size of software save directory.

Upgrading from V12.0L10 or earlier

For database storage, approximately 1.2 times the required disk capacity estimated above is required.

Extending the Systemwalker standard database

The space allocated for database before extension is displayed for **Giving amount** in the **This is the current database usage** page of the **Operation Environment Maintenance Guide** wizard during the database extension. Check as required.

This disk available capacity must include the space required for backup data plus the space required for the database.

- For backup data storage drive, at least the same amount of space as the space allocated for database before extension is required.
- To change the database storage to a different drive, at least the same amount of space as the required disk capacity estimated above is required.
  If you are not changing the database storage drive, the difference between the required disk capacity estimated above and the space allocated for database before extension is required as space.

To collect smart device information, the database space shown below is additionally required.

Number of smart devices x 4.5 MB

To manage the devices (fixtures), the following additional database capacities will be required depending on the number of devices (fixtures), except PCs, that are to be managed.

Number of managed devices (fixtures) except PCs	Database capacity
100 - 2,999	Number of managed devices (fixtures) except PCs x 0.19 MB
3,000 or more	Number of managed devices (fixtures) except PCs x 0.16 MB

DS

- Required CPU specifications

  Intel(R) Xeon(R) E5503 (2 GHz) or higher

- Required memory capacity

  Over 720 MB (excluding usage amount of OS)

- Required disk capacity

  115 MB (installation destination) + 12 MB (required by the system drive to store the runtime library) + 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 or Xeon(R) 2GHz or higher

- Required memory capacity (Note)

  Over 256MB (excluding usage amount of OS)

- Required disk capacity (Note)

  Over 100MB

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

CT

Environment where Live Help Client is installed

- Required CPU specifications

  1 GHz or higher

- Required memory capacity

  Over 32MB (excluding usage amount of OS)

  Minimum resident memory

  - At normal time: 6MB
  - When collecting software operation status: 9MB
  - Non-resident memory for command mode CT.

- Required disk capacity

  42MB or more (regular version: installation destination) + 12 MB (required by the system drive to store the runtime library) + size of operating disk during patch installation (Note)

  Note: The size for the work disk used in patch application will be required during the use of the automatic patch installation function.

  - If applying a security patch (Hotfix): 20 MB or more
  - If applying a service pack: Approx. 9 GB

Environment where Live Help Client is not installed

- Required CPU spec

  1 GHz or more

- Required memory capacity

  32 MB or greater (not including the operating system usage)

  Minimum resident memory used

  - Under normal use: 6 MB
  - During the software operation status collection: 9 MB

  - Command mode CT is non-resident

- Required disk space

  17 MB or more (normal version: installation destination) + 12 MB (required by the system drive to store the runtime library) + disk size for tasks when applying patches (Note)

  8 MB 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(R) vPro or Intel(R) Centrino(R) Pro. PCs with AMT 2.0 - AMT 9.x are supported.

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.

SS

- Required CPU spec

  Intel(R) Xeon(R) E5503(2 GHz) or higher

- Required memory capacity

  2 GB or greater (not including the operating system usage)

- Required disk space

  2 GB or more

Smart device CT

- Required internal storage capacity

  30 MB or more

- Required external storage capacity

  At least the total size of distributed applications is required if the application distribution function (to smart devices) is used.

3.2 Software

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

3.2.1 Operating System

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

Portugal OS

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

CS

- Microsoft(R) Windows Server(R) 2008 Foundation Service Pack 2
- Microsoft(R) Windows Server(R) 2008 Standard Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 R2 Standard Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Essentials
- Microsoft(R) Windows Server(R) 2012 Foundation
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter

Note) Server Core is unusable.

DS

- Microsoft(R) Windows Server(R) 2008 Foundation Service Pack 2
- Microsoft(R) Windows Server(R) 2008 Standard Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 R2 Standard Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Essentials
- Microsoft(R) Windows Server(R) 2012 Foundation
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter

Note) Server Core is unusable.

Note

Note the following when using a 64-bit operating system:

- Systemwalker Desktop Patrol DS runs on 32-bit compatible mode.

AC

- Microsoft(R) Windows Vista(R) Ultimate Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise Service Pack 2
- Microsoft(R) Windows Vista(R) Business Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic Service Pack 2
- Microsoft(R) Windows Vista(R) Ultimate x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Business x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic x64 Edition Service Pack 2
- Windows(R) 7 Enterprise Service Pack no/1
- Windows(R) 7 Ultimate Service Pack no/1

- Windows(R) 7 Professional Service Pack no/1
- Windows(R) 7 Home Premium Service Pack no/1
- Windows(R) 8
- Windows(R) 8 Pro
- Windows(R) 8 Enterprise
- Windows(R) 8.1
- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise

CT

- Microsoft(R) Windows Server(R) 2008 Foundation Service Pack 2
- Microsoft(R) Windows Server(R) 2008 Standard Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 R2 Standard Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise Service Pack no/1 (Note)
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Essentials
- Microsoft(R) Windows Server(R) 2012 Foundation
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Vista(R) Ultimate Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise Service Pack 2
- Microsoft(R) Windows Vista(R) Business Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic Service Pack 2
- Microsoft(R) Windows Vista(R) Ultimate x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Business x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic x64 Edition Service Pack 2
- Windows(R) 7 Enterprise Service Pack no/1
- Windows(R) 7 Ultimate Service Pack no/1

- Windows(R) 7 Professional Service Pack no/1
- Windows(R) 7 Home Premium Service Pack no/1
- Windows(R) 8
- Windows(R) 8 Pro
- Windows(R) 8 Enterprise
- Windows(R) 8.1
- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise

Note) Server Core is unusable.

Note

Note to be taken when you are using Systemwalker Desktop Patrol in a 64-bit operating system is shown below:

- Systemwalker Desktop Patrol CT runs on 32-bit compatible mode.

ADT

- Microsoft(R) Windows Server(R) 2008 Foundation Service Pack 2
- Microsoft(R) Windows Server(R) 2008 Standard Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 R2 Standard no/1 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise no/1 (Note)
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Essentials
- Microsoft(R) Windows Server(R) 2012 Foundation
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Vista(R) Ultimate Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise Service Pack 2
- Microsoft(R) Windows Vista(R) Business Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic Service Pack 2
- Microsoft(R) Windows Vista(R) Ultimate x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Enterprise x64 Edition Service Pack 2

- Microsoft(R) Windows Vista(R) Business x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Premium x64 Edition Service Pack 2
- Microsoft(R) Windows Vista(R) Home Basic x64 Edition Service Pack 2
- Windows(R) 7 Enterprise Service Pack no/1
- Windows(R) 7 Ultimate Service Pack no/1
- Windows(R) 7 Professional Service Pack no/1
- Windows(R) 7 Home Premium Service Pack no/1
- Windows(R) 8
- Windows(R) 8 Pro
- Windows(R) 8 Enterprise
- Windows(R) 8.1
- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise

Note) Server Core is unusable.

Note

Note to be taken when you are using Systemwalker Desktop Patrol in a 64-bit operating system is shown below:

- Systemwalker Desktop Patrol ADT runs on 32-bit compatible mode.

SS

- Microsoft(R) Windows Server(R) 2008 Foundation Service Pack 2
- Microsoft(R) Windows Server(R) 2008 Standard Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Service Pack 2 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 R2 Standard no/1 (Note)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise no/1 (Note)
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Essentials
- Microsoft(R) Windows Server(R) 2012 Foundation
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter

Note) Server Core is unusable.

Note

Note to be taken when you are using Systemwalker Desktop Patrol in a 64-bit operating system is shown below:

- Systemwalker Desktop Patrol SS runs on 32-bit compatible mode.

Smart device CT

- Android 3.0 - 5.0

  Note

  Operations in the multi-user environment of Android 4.2 or later are not supported.

- iOS 5.0 - 8.1

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
  - Internet Information Services 8.0
  - Internet Information Services 8.5

The following software is required to edit CSV files.

- **Editor software for editing CSV files**

  Microsoft(R) Windows NOTEPAD, WORDPAD or Microsoft(R) Excel

DS

No software is required for the PC where the DS is to be installed.

AC

The PC installed with AC requires the following software.

- **Microsoft(R) Excel**

  Any one of the following products is required.

  - Microsoft(R) Office Standard Edition 2003 (Note 1)
  - Microsoft(R) Office Professional Edition 2003 (Note 1)
  - Microsoft(R) Office Ultimate 2007 (Note 2)

- Microsoft(R) Office Enterprise 2007 (Note 2)
- Microsoft(R) Office Standard 2007 (Note 2)
- Microsoft(R) Office Professional 2007 (Note 2)
- Microsoft(R) Office Professional Plus 2007 (Note 2)
- Microsoft(R) Office Personal 2007 (Note 2)
- Microsoft(R) Office Professional Plus 2010 (Note 3)
- Microsoft(R) Office Standard 2010 (Note 3)
- Microsoft(R) Office Professional 2010 (Note 3)
- Microsoft(R) Office Home and Business 2010 (Note 3)
- Microsoft(R) Office Personal 2010 (Note 3)
- Microsoft(R) Office Personal 2013 (Note 4)
- Microsoft(R) Office Home and Business 2013 (Note 4)
- Microsoft(R) Office Professional 2013 (Note 4)
- Microsoft(R) Office Excel 2003
- Microsoft(R) Office Excel 2007
- Microsoft(R) Office Excel 2010
- Microsoft(R) Office Excel 2013

Note 1: Microsoft(R) Office Excel 2003 is necessary.

Note 2: Microsoft(R) Office Excel 2007 is necessary.

Note 3: Microsoft(R) Office Excel 2010 is necessary.

Note 4: Microsoft(R) Office Excel 2013 is necessary.

The following software is required for apply location map.

- **Microsoft(R) Visio**

  Any one of the following products is required.

  - Microsoft(R) Office Visio(R) Standard 2003
  - Microsoft(R) Office Visio(R) Professional 2003
  - Microsoft(R) Office Visio(R) Standard 2007
  - Microsoft(R) Office Visio(R) Professional 2007
  - Microsoft(R) Office Visio(R) Standard 2010
  - Microsoft(R) Office Visio(R) Professional 2010
  - Microsoft(R) Office Visio(R) Premium 2010
  - Microsoft(R) Visio(R) Standard 2013
  - Microsoft(R) Visio(R) Professional 2013

Note

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

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(R) Internet Explorer 6
- Windows(R) Internet Explorer(R) 7
- Windows(R) Internet Explorer(R) 8
- Windows(R) Internet Explorer(R) 9
- Windows(R) Internet Explorer(R) 10
- Windows(R) Internet Explorer(R) 11

SS

The PC installed with SS does not require any software.

Relevant software

Software that can be used in the virtual OS

CS/DS

- VMware vSphere 4
- VMware vSphere 5
- VMware vSphere 5.5
- Microsoft Hyper-V
- KVM

CT/AC/ADT

- VMware vSphere 4
- VMware vSphere 5
- VMware vSphere 5.5
- VMware View 4
- VMware View 5.0
- VMware View 5.1
- VMware Horizon View 5.2
- VMware Horizon View 5.3
- VMware Horizon View 6.0
- Citrix XenDesktop 4.0
- Citrix XenDesktop 5.0
- Citrix XenDesktop 5.6
- Citrix XenDesktop 6.0
- Citrix XenDesktop 7.0
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7.5

    - Citrix XenDesktop 7.6
    - 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(R) Outlook Express

Microsoft(R) Outlook etc.

3.2.3 Products That Cannot Coexist

Products that cannot coexist with CS

When installing CS, the following products cannot coexist.

- Management Server and Master Management Server for Systemwalker Desktop Keeper V15.0.0 or later (Note 1)
- Operation Management Server for Systemwalker Centric Manager V15.0.0 or later (Note 2)
- Asset Management Server for Systemwalker Centric Manager V15.0.0 or later (Note 3)
- Windows Server Update Services (WSUS) function (Note 4)
-

Note 1: Products that cannot coexist

The following products cannot coexist.

- Windows (32-bit) Systemwalker Desktop Keeper and Windows (64-bit) Systemwalker Desktop Patrol
- Windows (64-bit) Systemwalker Desktop Keeper and Windows (32-bit) Systemwalker Desktop Patrol

Note 2: Products that cannot coexist

If the Asset Management function of the Systemwalker Centric Manager Operation Management Server is installed, the following products cannot coexist.

- Windows (32-bit) Systemwalker Centric Manager and Windows (64-bit) Systemwalker Desktop Patrol
- Windows (64-bit) Systemwalker Centric Manager and Windows (32-bit) Systemwalker Desktop Patrol

Note 3: Products that cannot coexist

The following products cannot coexist.

- Windows (32-bit) Systemwalker Centric Manager and Windows (64-bit) Systemwalker Desktop Patrol
- Windows (64-bit) Systemwalker Centric Manager and Windows (32-bit) Systemwalker Desktop Patrol

Note 4: Products than can coexist

If the operating system for the Systemwalker Desktop Patrol CS is x64 Edition, the software in question can coexist.

Products that cannot coexist with the SS

The products that cannot coexist with SS are the same as those that cannot coexist with CS.

3.3 Operations with Mixed Versions or Levels

This section explains operations where versions and levels of Systemwalker Desktop Patrol components are different.

CT/ADT

Even if the version or level of CT/ADT is different from that of the connection destination server, connections can still be established.

The following restrictions apply, however, depending on the version and level of the server to be connected.

- If the version of the connection destination server is older than that of CT/ADT, then connections cannot be established.

- If the version of the connection destination server is newer than that of CT/ADT, then only the functions from the older version can be used.

CS/DS/SS/AC

All components must be used with the same version and level.

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 or later	- Systemwalker Desktop Patrol configuration information can be exported, and then imported to Systemwalker Desktop Keeper as its own configuration information. - 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 or later	- 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	Y	Y	Y
Software information - file search	Y	N	Y
Software information- registry search (searched by program name)	Y	N	Y
Software information - registry search(searched by any key word and value)	N	N	Y
User information	Y (Note)	Y (Note)	Y
Software operation status	N	N	Y
Registry information	N	N	N
EXE information	N	N	N

Y: can be collected

N: 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.

Refer to the *Systemwalker Desktop Patrol 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.

Refer to the *Systemwalker Desktop Patrol Operation Guide: for Administrators* for record format and usage instructions.

4.4 Configuration Information

Systemwalker Desktop Patrol manages PCs using section-based configuration information (tree structure). By linking this configuration information with Systemwalker Desktop Keeper configuration information, installation can be simplified.

The Systemwalker Desktop Keeper versions with which configuration information can be linked are shown below:

- Systemwalker Desktop Keeper V13.0.0 or later

Note that this function cannot be used if operations linking Active Directory are performed.

Importing Systemwalker Desktop Keeper configuration information

By using the Systemwalker Desktop Keeper function, Systemwalker Desktop Keeper-managed configuration information (configuration information based on the logical group and management server) can be exported (output in CSV) and then it can be imported to Systemwalker Desktop Patrol section-based configuration information.

Refer to the *Systemwalker Desktop Patrol Operation Guide for Administrators* for details on how to use this function.

Exporting configuration information to Systemwalker Desktop Keeper

By using the Systemwalker Desktop Patrol function, Systemwalker Desktop Patrol-managed configuration information (section-based configuration information) can be exported (output in CSV) and then, using the Systemwalker Desktop Keeper function this time, it can be imported to Systemwalker Desktop Keeper configuration information based on the logical group and management server.

Refer to the *Systemwalker Desktop Patrol Operation Guide for Administrators* for details on how to use this function.

Note that if both Systemwalker Desktop Patrol and Systemwalker Desktop Keeper are of V14.2.0 or later, configuration information is automatically imported from Systemwalker Desktop Patrol to Systemwalker Desktop Keeper.

4.5 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.

4.6 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.

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.

Android device

A smart device in which Android(TM) is installed.

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 3 months, 6 months, or 1 year.

Auditing Schedule

It defines the time to perform security auditing. The certain date and start time must be set in every month.

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.

Batch Network Check

With this check, information of devices that support the network-connected ICMP is automatically detected from the CS server, without installing the ADT and bypassing segments.

Batch Processing

It modifies settings automatically when power saving and security settings violate the requirement based GUI operations of PC users.

Building Management Information

It records the summary of work area (office) information, which is necessary for management.

Client Policy

It defines the CT operation policy.

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, click **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Inventory Collection**, or **Apps** > **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.

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.

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.

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.

Contract Information

It indicates the contract-related information about devices that are managed with ledger, such as contract class company, and date.

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

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

custom installation

Installation type in which all setting values can be changed from their default.

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 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 higher 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.

global unicast address

An IPv6 address defined as "2000::/3". It is abbreviated as "GUA".

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.

iOS device

A smart device in which iOS is installed.

IP address

Generic term for IPv4 and IPv6 addresses.

IPv6 address type

These are categories corresponding to the IPv6 address bit. These categories are broadly divided into global unicast address, unique local address, link-local address, multicast address, and other addresses.

License Management Function

Administrator manages the license number according to each license dispensed through **License** > **License Giving menu** from the main menu. Only the administrator has such authority.

Using license management, illegal and unused licenses can be identified.

link-local address

An IPv6 address defined as "fe80::/10" and used in identical L2 networks. It is also abbreviated as "LLA".

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.

multicast address

An IPv6 address defined as "ff00::/8".

multiple IP addresses

State in which both IPv4 and IPv6 addresses are used.

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.

one-off address (anonymous address)

An address used for sending. It is allocated to the node when the stateless automatic configuration (RA) is used, and is changed after a certain period of time. Refer to "RFC 3041" for details.

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 higher servers.

The operation of the policy group unit can be set in the main 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.

product information

Information collected on the software listed in **Uninstall a program** and **Add or Remove Programs** (or **Programs and Features**) > **View installed updates**.

Program Information

It collects information displayed in the **Add or Remove Programs** menu.

RA

It is the abbreviation of Router Advertisement, a method used in the automatic configuration of the IPv6 address. It periodically notifies the network prefixes that can be used with the router IPv6 addresses in the network. The notified network prefixes can be global unicast address or unique local address.

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

Registry Information

It indicates information in the OS registry. Users can check the information when configuring registry information in the main menu.

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.

SAMAC

Association of SAM Assessment & Certification, a non-profit incorporated association established for appropriate promotion of software asset management.

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.

smart device

Generic term for Android devices and iOS devices.

smart device CT

It is the abbreviation of Systemwalker Desktop Patrol Client.

SNMP

It is the abbreviation of Simple Network Management Protocol. SNMP monitors servers and network devices connected through TCP/IP around the network.

Software Dictionary

The software dictionary is distributed by Systemwalker randomly.

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 Distribution Function

It manages software that is distributed to CT. The management includes registration, update, deletion, and incremental distribution.

Software Group for Distribution

It is created during software distribution and used when software is distinguished by category.

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 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.

SS

It is the abbreviation of Smart Device Relay Server (Systemwalker Desktop Patrol SS).

standard installation

Installation type that uses the default values to install and build with ease in an environment with up to 300 managed devices.

Status Icon

It displays the bar chart of the status window at the top-left corner, indicating the percentage of the problem PCs.

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.

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 Client

Client used in smart devices. It is installed on smart devices that manage the assets through inventory collection.

It is abbreviated as "Smart Device CT".

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 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 PC.

It uses the database storing the section information relating to ICT asset information (ICT repository), personnel, and sections to provide web browser services including distribution of security patches, security auditing and license management. Normally, one server is installed per company.

It is abbreviated as Desktop Patrol CS or CS.

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.

Systemwalker Desktop Patrol SS (Smart Device Relay Server)

Server used to manage smart devices. It is installed between the Corporate Server (CS) and the Client Terminal (CT) for smart devices. To notify the inventory information from the smart device to the CS, it relays that data. It can operate regardless of whether it coexists with the CS.

It is abbreviated as "SS".

unique local address

An IPv6 address defined as "fc00::/7" and used in identical sites.

It is also abbreviated as "ULA".

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 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 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** > **Software Auditing** > **User definition menu**.

User Definition

The administrator creates the criteria for checking the unregistered software in the software dictionary, and defines software use inside enterprises.

User Management Information

It is the information of assembled users, which is necessary for construction of management information.

User Memo

It is the information which can be set freely for devices.

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.