FUJITSU

FUJITSU Software
Systemwalker Desktop Patrol

Operation Guide: for Administrators

Windows

B1WD-3288-04ENZ0(00)
July 2015

Preface

Purpose of this guide

This guide explains necessary settings and operating procedures to use the following products.

- 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 those responsible for operating and managing an assets management system using Systemwalker Desktop Patrol.

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

- General knowledge regarding Internet Information Services(IIS)
- General knowledge regarding personal 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 How to Use Systemwalker Desktop Patrol

This chapter describes how to use Systemwalker Desktop Patrol.

Chapter 2 Set Operation Environment

This chapter describes how to set Systemwalker Desktop Patrol.

Chapter 3 View PC Information

This chapter describes how to set collected content, timing of collection and how to view the information collected from Systemwalker Desktop Patrol CT.

Chapter 4 Audit/Control PC Operational Configuration

This chapter describes how to audit and manage the security settings and power saving settings of PC.

Chapter 5 License Management

This chapter describes the management and application of license.

Chapter 6 Distribute/Install Security Patches

This chapter describes the distribution/installation of security patches.

Chapter 7 Distribute Files

This chapter describes how to distribute files.

Chapter 8 Distribute Software

This chapter describes how to distribute software.

Chapter 9 Managing Smart Devices

This chapter describes how to manage smart devices.

Chapter 10 Distributing Applications to Smart Devices

This chapter describes how to distribute applications to smart devices.

Chapter 11 Assets Management by Ledger

This chapter describes how to manage the asset of device and contract .etc by total account.

Chapter 12 Manage Machine by Layout Diagram

This chapter describes how to manage machines by layout diagram.

Chapter 13 Output Report

This chapter describes how to output report of asset and security.

Chapter 14 Link with Other Products

This chapter describes how to link Systemwalker Desktop Patrol with other products.

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.
Systemwalker Desktop Patrol User's 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 (This Guide)	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.

Symbol	Meaning
{ }	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

Abbreviation	Full Name
	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
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

Abbreviation	Full Name
	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 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.

First edition, July 2015

Copyright 2002 - 2015 FUJITSU LIMITED

Contents

Chapter 1 How to Use Systemwalker Desktop Patrol 1
1.1 Operation Authority 1
1.2 Main menu 2
1.3 Download menu 6
1.4 AC Menu 7

Chapter 2 Set Operation Environment 11
2.1 Construct Master Data 11
2.1.1 Design Master Data 11
2.1.2 Procedure of Constructing Master Data at Active Directory Linkage 15
2.1.3 Procedure of Constructing Master Data 22
2.1.4 Create Section Management Information 23
2.1.4.1 Register Section 24
2.1.4.2 Delete Section 25
2.1.4.3 Register through Uploading 27
2.1.5 Create User Management Information 33
2.1.5.1 Register User or Building 33
2.1.5.2 Set the Operation Authority 49
2.2 Set Auditing Software 53
2.2.1 Select Software from Support Center Definition 53
2.2.2 Create User Definition 56
2.2.2.1 Create User Definition from Inventory Information 67
2.2.3 Import the SAMAC Software Dictionary 71
2.3 Set Client Policy 73
2.3.1 Create Policy Group 76
2.3.1.1 Add Policy Group 76
2.3.1.2 Add Command Mode CT 81
2.3.1.3 Modify Policy Group Information 84
2.3.1.4 Delete Policy Group 86
2.3.2 Customize Various Policies 87
2.3.2.1 Customize Basic Operation Policy 90
2.3.2.2 Customize Patch Installation 92
2.3.2.3 Customize Power Saving Policy 94
2.3.2.4 Customize Security Policy 95
2.4 Import/Export Structure Information 96
2.4.1 Import Structure Information 98
2.4.2 Export Structure Information 100
2.5 Set Alarm Notification 102
2.6 Control Executable file 108
2.6.1 Settings 109
2.6.1.1 Set Executable File and Message 109
2.6.1.2 Set the Collection of Software Operation Status 115
2.6.1.3 Apply Client Policy 115
2.6.1.4 Log on CT Again 115
2.6.2 Operation 115

Chapter 3 View PC Information 117
3.1 Settings Performed as Needed 117
3.1.1 Perform Operation Settings of Client 118
3.1.2 Perform Operation Settings of the Entire System 125
3.1.2.1 Set Software Dictionary 125
3.1.2.2 Set the Item Label of User Information 125
3.1.3 Perform Settings of Inventory Collection by Command Mode CT 130
3.1.4 Perform Settings of PC Operation Management 137
3.1.4.1 Settings of CS 137

3.1.4.2 Settings of Operation Management Target PC....137
3.1.5 Perform Settings Related to Operation Status....139
3.1.6 Perform Settings Related to Operation Processing....147
3.2 Operation....153
3.2.1 View Inventory Information....153
3.2.2 Deleting Inventory Information....178
3.2.3 Viewing the Product Information....184
3.2.4 View Auditing Information of Software....187
3.2.4.1 Confirm Installation of Security Patches....191
3.2.4.2 Confirm Installation of Anti-Virus Software....194
3.2.5 View Software Operation Status....197
3.2.6 View Security Information....200
3.2.7 Perform Operation Management of PC....207
3.2.7.1 Collect Inventory Information (Hardware Information) Immediately....208
3.2.7.2 Operate Power....210
3.2.8 View the Collected File....213
3.2.9 Confirm the Collection Status of PC Information....214
3.2.10 Timing of Collecting PC Information....218
3.2.10.1 Collection at Installation....220
3.2.10.2 Collection at the Time Set in Schedule....220
3.2.10.3 Collect after Automatic Installation of Security Patches has Completed....223
3.2.11 Display Operation Status and Perform Operation Processing....225
3.2.11.1 View Status Window from Login....225
3.2.11.2 View the Display of Aggregation Items....228
3.2.11.3 View Details According to Aggregation Items....240
3.2.11.4 View Corresponding PC according to Aggregation Item....243
3.2.11.5 View Status of Systemwalker Desktop Keeper....256
3.2.12 Check the Operation Status of CT....258
3.2.12.1 Check the Operation Status of CT on CT....259
3.2.12.2 Check the Operation Status of CT on CS....266
3.2.13 Checking the Operational Status of CS/DS....268
3.2.14 Collect Simple Operation Log File....273

Chapter 4 Audit/Control PC Operational Configuration....277
4.1 Operation Procedure....277
4.2 Settings....278
4.2.1 Settings for Auditing Power Saving Settings....279
4.2.1.1 Set the Auditing Items of Power-Saving Settings....280
4.2.2 Settings Related to Auditing Security Settings....295
4.2.2.1 Set the Auditing Items of Security Settings....299
4.3 How to Operate Diagnosis result window of operation settings....314
4.3.1 Structure of Diagnosis result window of operation settings....314
4.3.1.1 Structure of Diagnosis Result Window of Power Saving....316
4.3.1.2 Structure of Security Diagnosis Result Window....320
4.3.2 Operate Diagnosis Result Window of Power Saving....327
4.3.3 Operate Diagnosis Result Window of Security....328
4.4 Confirm Status Window....332
4.5 Confirm Report....332
4.5.1 Procedure of Confirming Power Saving Setting Status Report....333
4.5.2 Procedure of Confirming Auditing Report of Power Consumption....334

Chapter 5 License Management....341
5.1 Steps of License Management....341
5.1.1 License Management by Systemwalker Desktop Patrol....341
5.1.2 Confirm and Change Current License State with Systemwalker Desktop Patrol....342
5.1.3 Allocate Current License with Systemwalker Desktop Patrol....342
5.1.4 Detect and Correct the License Violation PC with Systemwalker Desktop Patrol....343
5.1.5 Return License of Unwanted Software....344

5.1.6 License Change Going with Personnel Change....344
5.1.7 Manage Software License by Using Downgrade Rights....345
5.1.8 Manage Software License Expanded to Second License....346
5.1.9 Check License Usage....347
5.2 Definition of License....348
5.2.1 Registration of License definition....348
5.2.2 Modify License Definition....351
5.2.3 Delete License Definition....355
5.3 Confirm PC of License Violation....357
5.3.1 Management of Current License....357
5.3.1.1 Register Current License Information....361
5.3.1.2 Modify Information of Current License....368
5.3.1.3 Delete Current License....374
5.3.1.4 View the Registered Software in Current License....377
5.3.2 Allocate License....380
5.3.3 Set as Needed....386
5.3.3.1 When Purchasing Software....386
5.3.3.2 When Purchasing License....386
5.3.3.3 When Discarding License....387
5.3.4 Operation....387
5.3.4.1 Confirm License Violation PC....387
5.3.4.2 Processing at Confirmation of License Violation PC....390
5.4 Confirm Idle Assets....391
5.4.1 Settings....391
5.4.2 Use....391
5.4.2.1 Confirm Idle Asset....392
5.4.2.2 Processing at Confirmation of Idle Assets....397

Chapter 6 Distribute/Install Security Patches....399
6.1 Operation Steps....399
6.2 Setup....401
6.2.1 Confirm and Publish Server Connection....401
6.2.2 Update of Software Dictionary....402
6.2.3 Select security Patches to be Installed to Special PC....402
6.2.4 Select Security Patches....408
6.2.5 Acquisition of Security Patches....414
6.2.5.1 Automatic Acquisition of Security Patches....414
6.2.5.2 Obtain Security Patches Manually....415
6.2.6 Settings of Installation & Distribution Intervals of Security Patches....421
6.3 Setup as Needed....428
6.3.1 Delete Security Patches....428
6.3.2 When Important Security Patches are Made Public....429
6.3.3 Set Retry Times and Message When Installation of Security Patches Fails....430
6.3.4 Steps to Install Security Patches to Server....435
6.4 Confirmation....436
6.4.1 Confirmation of Acquisition of Security Patches....436
6.4.2 Processing to Acquisition Failure....437
6.4.3 Confirmation of Installation of Security Patches....438
6.4.4 Processing to Installation Failure....446
6.5 Type of Use....446
6.5.1 Operation of General Applicability and Key Points of Setup....446
6.5.2 Usage Mode of Security Patches Installation After Logon....449
6.5.3 Usage mode of Regular Confirmation and Installation of Security Patches (Use as Per Original Setup)....451
6.5.4 Operation of Security Patches Installation at Night....454

Chapter 7 Distribute Files....457
7.1 Operation Procedure....457
7.2 Settings....458

7.2.1 Set Distributed File and PC to be distributed and Distribute....459
7.3 Operation....471
7.3.1 Confirm Distributed Result....471
7.3.2 Stop Distribution....476
7.3.3 Re-Distribution....478
7.3.4 Distribute the Distribution Task that is Ready to be Distributed....480
7.3.5 Confirm the Content of Registered Distribution Task....481
7.3.6 Modify the Content of Registered Distribution Task....483
7.3.7 Delete Unnecessary Distribution Task....485
7.3.8 Confirm Distribution Result with CT Operation Status Check Command....486

Chapter 8 Distribute Software....488
8.1 Operation Steps....488
8.2 Settings....489
8.2.1 Perform Settings of Server to Distribute Software....490
8.2.2 Set Conditions to Distribute Software to Client....496
8.2.3 Register Software Distribution to be Released....501
8.2.3.1 Notes of Software Distribution to PC with Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012....511
8.2.4 Settings of Distribution Target....511
8.3 Settings as Needed....517
8.3.1 Message Display of Software Download....518
8.4 Operation....521

Chapter 9 Managing Smart Devices....523
9.1 Synchronizing Inventory Information (Android Device Only)....523
9.1.1 How to Synchronize the Inventory Information....523
9.1.2 Checking the Operational Status of the Smart Device CT....524
9.2 Referencing Collected Inventory Information....525
9.3 Referencing Collection Information in Security Settings....533
9.4 Managing an Individually Owned Smart Device (Android Device Only)....537

Chapter 10 Distributing Applications to Smart Devices....541
10.1 Procedure....541
10.2 Setup and Distribution....541
10.3 Operation....550
10.3.1 Checking Distribution Results....551
10.3.2 Stopping Distribution....555
10.3.3 Performing Distribution Again....557
10.3.4 Distributing Ready Distribution Tasks....559
10.3.5 Checking the Content of Registered Distribution Tasks....560
10.3.6 Changing the Content of Registered Distribution Tasks....562
10.3.7 Deleting Unnecessary Distribution Tasks....564

Chapter 11 Assets Management by Ledger....566
11.1 Management Ledger Settings....566
11.1.1 Set Contract Expiration Notification....566
11.1.2 Set Registration for Device Information....570
11.1.3 Set Security Auditing....572
11.1.4 Set History Management....574
11.1.5 Set Asset Classification Name....576
11.1.6 Set Window Item Name....579
11.1.7 Set Other Product Information Reflection....581
11.1.8 Set Unregistered Device Notification....581
11.2 Register Asset Information to Ledger....583
11.2.1 Procedures for Registering/Modifying Asset Information....583
11.2.2 Register/Modify Ledger....588
11.2.3 Registration/Modification by Automatically Detecting Device Information....593

11.2.3.1 Import Detected Device Information....602
11.2.3.2 Display/Register Unregistered Device....604
11.3 Device Management....624
11.3.1 Confirm/Delete Device Information....624
11.3.1.1 Confirm Various Device Information....625
11.3.1.2 Confirm List of Device....632
11.3.1.3 Confirm Device Details....635
11.3.1.4 Confirm History Information....640
11.3.1.5 Delete Device Information....646
11.3.2 Register/Modify Device Information....648
11.3.3 Save Device Information as Ledger....653
11.4 Contract Management....654
11.4.1 Confirm Contract Information....654
11.4.1.1 Confirm Various Contract Information....655
11.4.1.2 Confirm List of Contract....660
11.4.1.3 Confirm Details of Contract....662
11.4.1.4 Delete Contract Information....665
11.4.2 Register/Modify Contract Information....666
11.4.3 Distribute Contract Information....668
11.4.4 Save Contract Information as Ledger....671
11.4.5 Extend Contract....672
11.5 Stocktaking Support....676
11.5.1 Confirm Stocktaking Status....676
11.5.1.1 Confirm Various Stocktaking Status....676
11.5.1.2 Confirm List of Stocktaking....681
11.5.1.3 Confirm List of Excluded Stocktaking....685
11.5.2 Save Stocktaking Status as Ledger....686
11.5.3 Stocktaking Operation....687

Chapter 12 Manage Machine by Layout Diagram....695
12.1 Preparation....695
12.2 Perform Installation Settings of Location Map Function....695
12.2.1 Create the Target for Saving Map File....699
12.2.2 Create Map File....699
12.2.3 Set the Target for Saving Map File....701
12.2.4 Associate Map File....701
12.2.5 Create Stencil for Map....703
12.2.6 Association of Shape....706
12.2.7 Perform Automatic Configuration Settings of Machine....708
12.3 Operate Location Map....710
12.3.1 Create Map File....711
12.3.2 Confirm Machine Information....719
12.3.3 Confirm the Difference with Asset Ledger....726
12.3.4 Confirm Status of Machine....728
12.3.5 Icon in Map File....729

Chapter 13 Output Report....730
13.1 Output Asset Operation Status....730
13.1.1 Procedure....730
13.1.2 Example of Outputting Asset Operation Status....733
13.2 Output Contract Status....736
13.2.1 Procedure....736
13.2.2 Example of Outputting Contract Status....739
13.3 Output Stocktaking Status....743
13.3.1 Procedure....743
13.3.2 Example of Outputting Stocktaking Status....746
13.4 Output License Usage Status....749
13.4.1 Preparation....749

13.4.2 Procedure ... 750
13.4.3 Example of Outputting License Usage Status ... 752
13.5 Output Security Auditing Status ... 755
13.5.1 Preparation ... 755
13.5.2 Procedure ... 766
13.5.3 Example of Outputting Security Auditing Status ... 770
13.6 Output Power Saving Setting Status ... 774
13.6.1 Procedure ... 774
13.6.2 Example of Outputting Power Saving Setting Status ... 778
13.7 Output Power Consumption Status ... 783
13.7.1 Preparation ... 783
13.7.2 Procedure ... 784
13.7.3 Example of Outputting Power Consumption Status ... 790

Chapter 14 Link with Other Products ... 797
14.1 Event Linkage ... 797
14.1.1 Event linkage Based on Alarm Notification ... 797
14.1.2 Event linkage Based on Event Log Output ... 798
14.2 Collection of Inventory Information ... 800
14.2.1 Inventory Information Collection with Systemwalker Centric Manager ... 800
14.2.1.1 Linkage Method with Coexistence with Systemwalker Centric Manager ... 801
14.2.1.2 Linkage Method without Coexistence with Systemwalker Centric Manager ... 805
14.2.2 Inventory Information Collection with CSV Linkage ... 807
14.3 Import to Asset Ledger ... 821

Chapter 1 How to Use Systemwalker Desktop Patrol

This chapter describes the operation authority and startup method of each window for the method of using Systemwalker Desktop Patrol.

1.1 Operation Authority

Operation Authority is required when using products in Systemwalker Desktop Patrol. In this system, operation authorities to be used are shown as follows. For AC menu, refer to "1.4 AC Menu".

- System Account
- Section Management Account
- User Account

System account

System Account is the authority of the System Administrator. All menu items of main menu and AC menu can be set and viewed.

Distribute the user ID/password for system account according to the following conditions.

Item	Length	Characters can be specified
User ID	1 to 20 characters	Single-byte alphanumeric characters Following single-byte symbols "-", "@". "_" English letters are case-sensitive.
Password	4 to 12 characters	Single-byte alphanumeric characters Single-byte space Following single-byte symbols "-", "=", "*", "+", "", "@", "~", " (",")", "&", "$", "#", "", "!", "?", "%", "\", ".", ",", "/", ":", ";", "`", " [", "]", "|", "<", ">", "{", "_", "}" English letters are case-sensitive.

Section management account

Section Management Account is the authority of section administrators. For the menu items of main menu and AC menu, the information of the section and its subordinate sections to which a login user belongs can be set and viewed.

In addition, the Section Management Account cannot perform the following operations.

- Main menu
  - **PC Information** > **Displayed Item Settings** of **Inventory Information**
  - **PC Information** > **PC Operation Management**
  - **License** > **License Definition**
  - **Distribution** > **Software Distribution** > **Add software group for distribution** button > **Settings of Distribution Software** button
  - **Distribution** > **Security Patches Distribution**
  - **Ledger** > **Display Item Settings** of **Device Management**
  - **Ledger** > **Display Item Settings** of **Contract Management**

  - **Ledger** > **Display Item Settings** of **Stocktaking**
  - **Environment Setup** > **Software Auditing**
  - **Environment Setup** > **Option**
- AC menu
  - Settings for security auditing
  - Settings for output of license usage status
  - Settings for output of security auditing report

The user ID/password registered during the construction of Master Data can be added/modified/deleted in **Environment Setup** of the main menu. For Master Data, refer to relevant content in "2.1 Construct Master Data".

Allocate authority for user ID/password in **Environment Setup** of the main menu.

User account

It is the authority of users. In menu items of the main menu, only information of user that has logged in can be viewed. It is the authority allocated to all user IDs when constructing Master Data.

For Master Data, refer to relevant content in "2.1 Construct Master Data".

1.2 Main menu

This section describes the preparation items before starting the main menu, notes of using, and the startup method.

Preparations

The main menu uses Internet Explorer to display data. Therefore, settings of Internet Explorer is required on the PC that uses the main menu.

For setting method, refer to "Preparations on the PC that uses Web Browser" of *Systemwalker Desktop Patrol Installation Guide*.

- Do not start multiple main menus on the same PC.
- To reference both the Asset Management feature of Systemwalker Desktop Patrol, and Systemwalker Centric Manager at the same time on the same terminal, use a separate browser session for each product. To start a new browser session:
  1. After starting the Web browser, press Alt to display the menu bar.
  2. On the **File** menu, select **New session** to start the new browser session in a separate window.
  3. Enter the URL for each product in the relevant address bar and log in to the other product using the new session.
- For CSV files that are output or downloaded, right-click the download link and select **Save to a file** or **Save the link** to save them. The files can then be referenced. If the download link itself is clicked, the contents may not be displayed correctly.

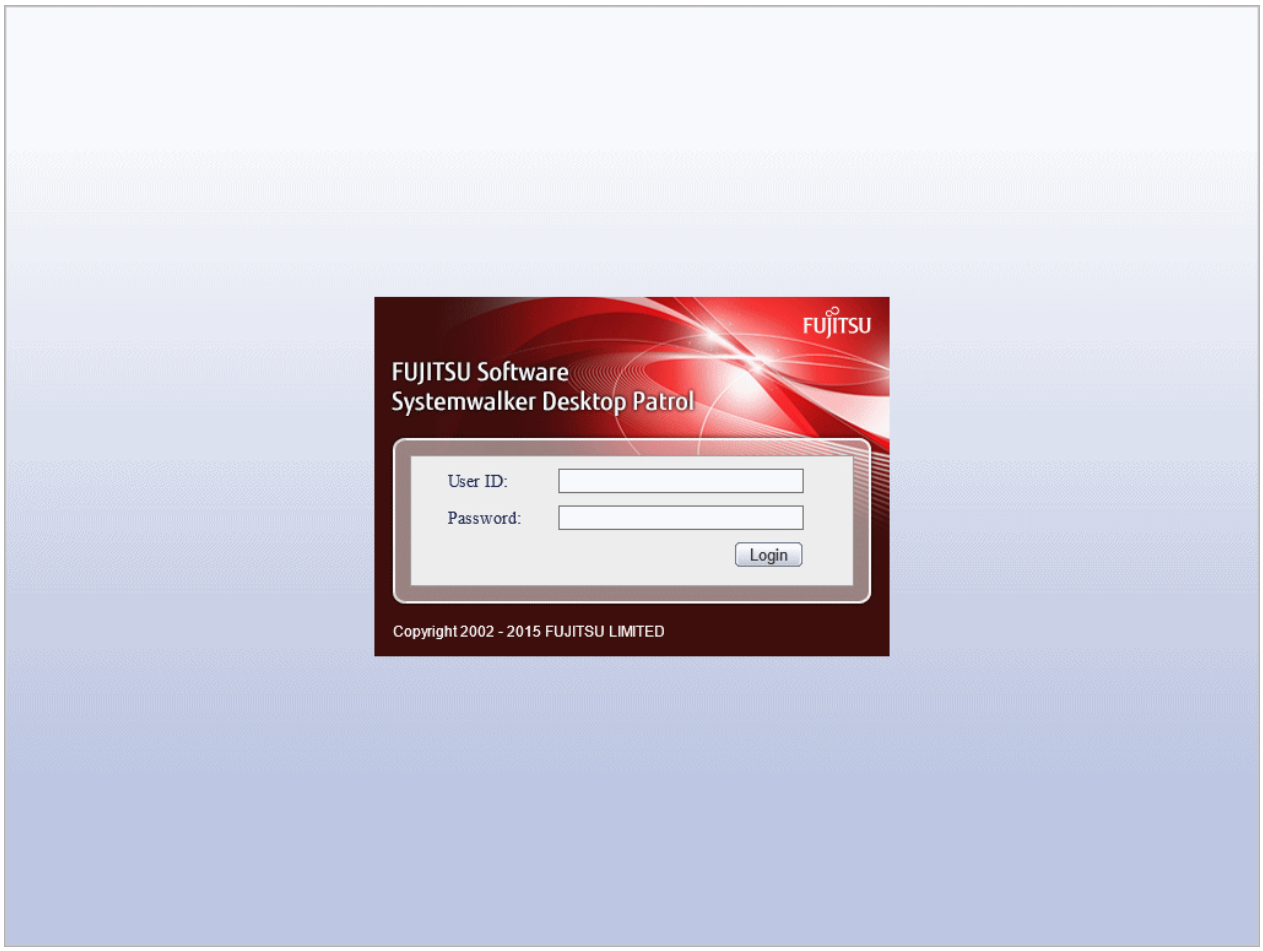
Steps

The procedure of login to the main menu is as follows.

1. Enter the following URL in the **Address** bar of the Web browser.

http://Server Information (FQDN name or host name or IP address of CS)/DTP/index.html

The login window is displayed.



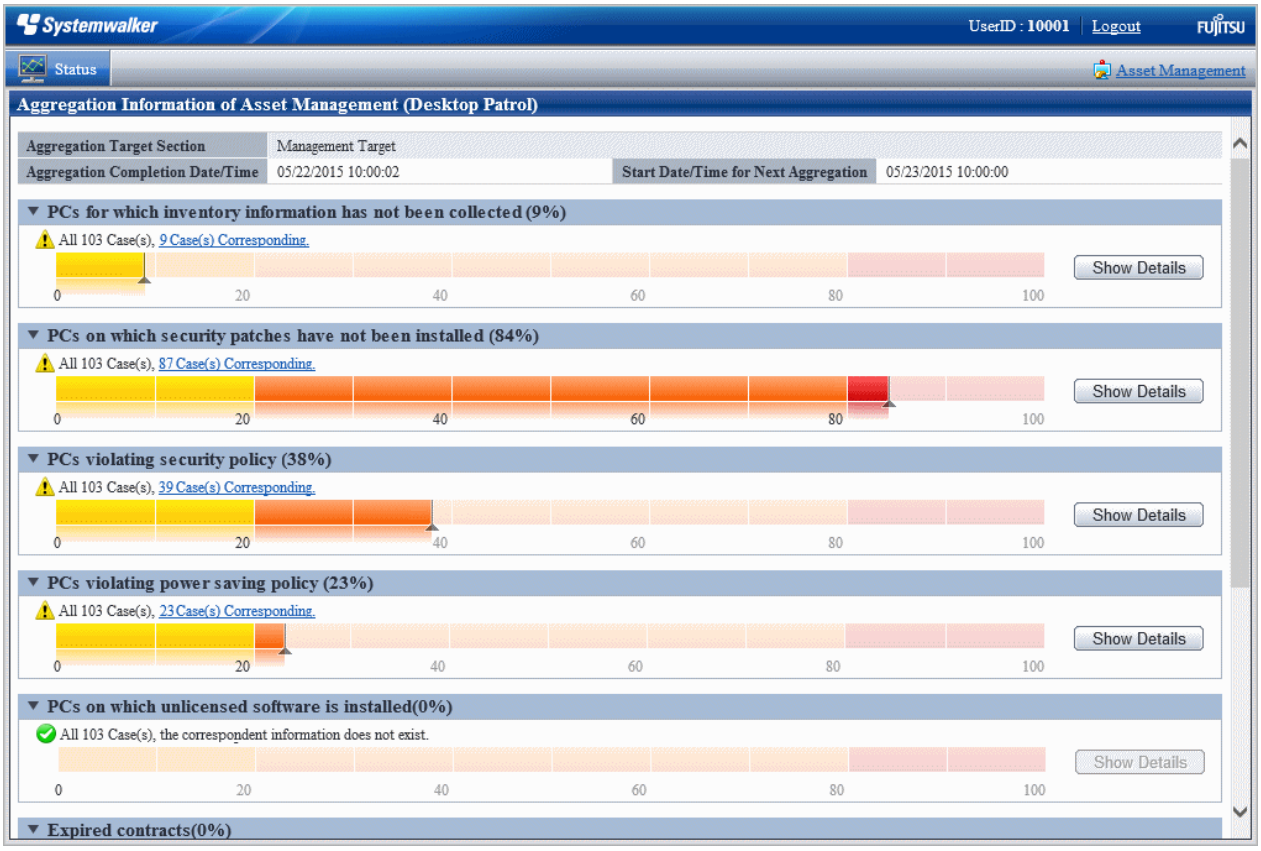
2. Enter the following information and click the **Login** button.

   - **User ID** text box
   - **Password** text box

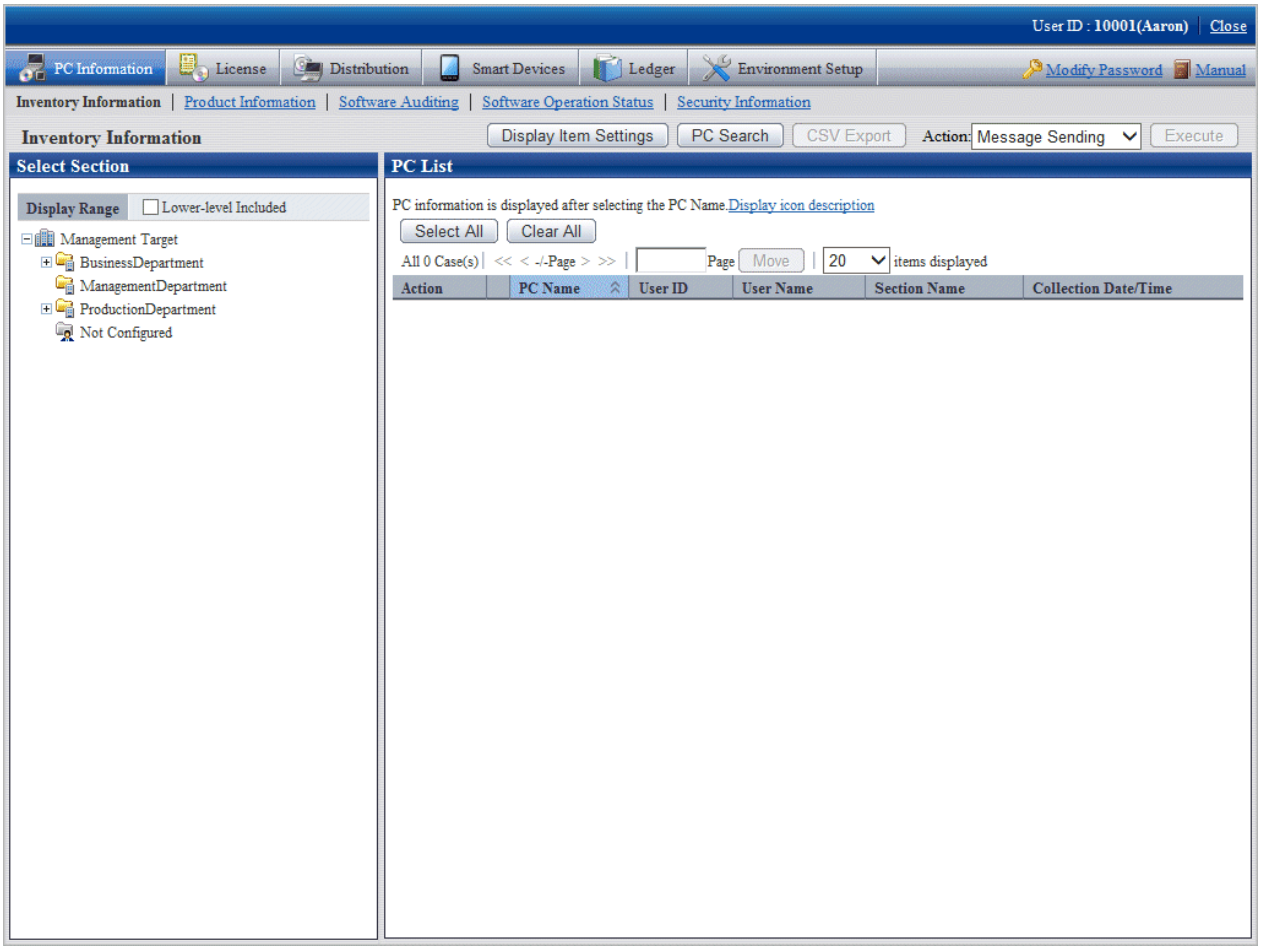
   The menu window is displayed according to the authority allocated to the user ID.

In case of system account

When login with the user ID to which the system account is allocated, the following status window will be displayed as the top page of system account.



By clicking the **Assets Management** of the status window, the following menu will be displayed.



In this guide, the procedure after login to the main menu will be described in the above-mentioned menu after the **Assets Management** is clicked in the status window.

In case of section management account

After login using the user ID to which the section management account has been allocated, the status window will be displayed.

It is the same as the window after login with system account.

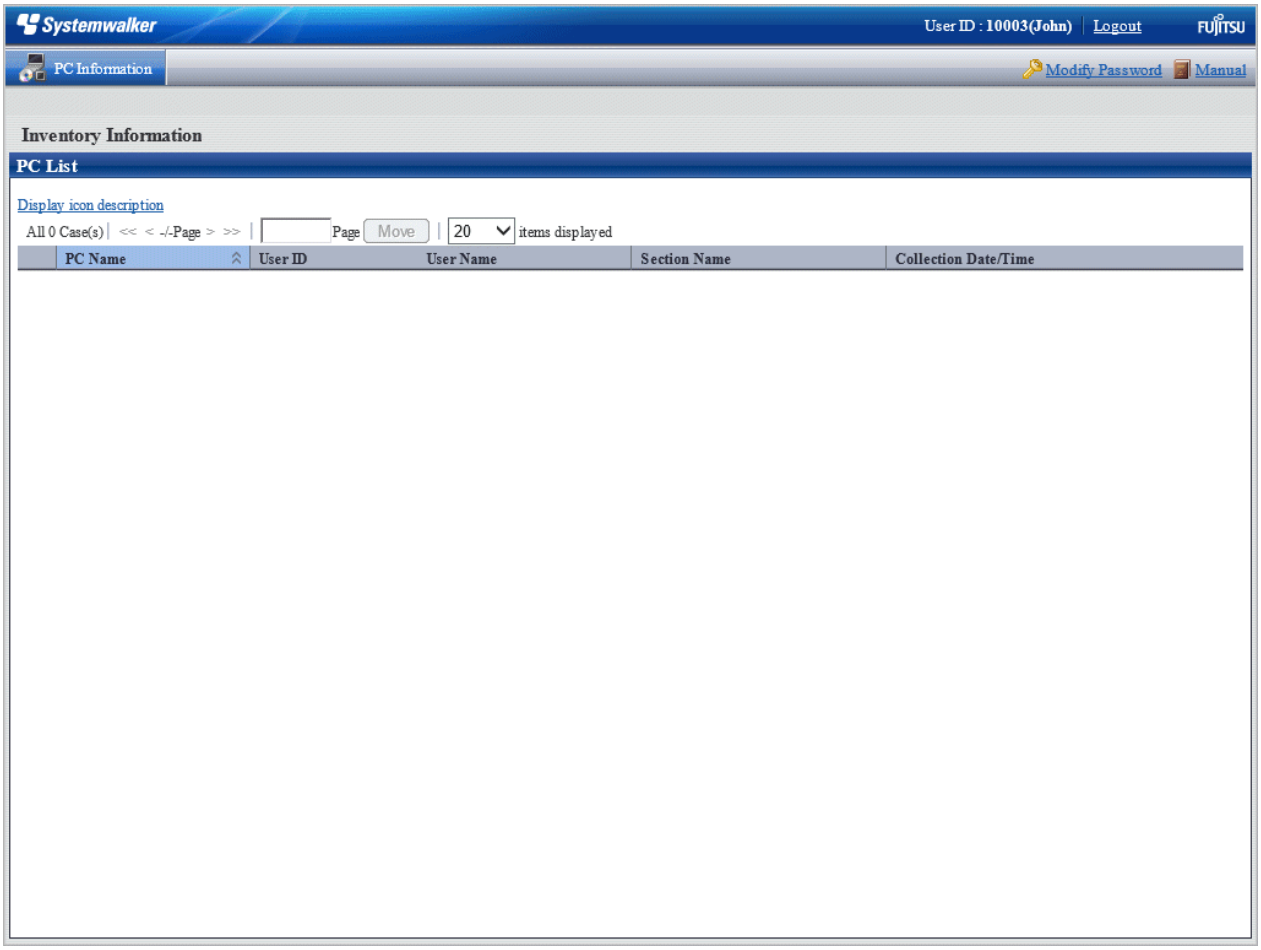
The section management account can only set or view the information of the section and its subordinate sections to which a login user belongs.

In case of user account

After login using the user ID to which the user account is allocated, the following menu will be displayed.

In this menu, only the following information of the user that has logged in can be viewed.

- PC Information (Inventory Information)



1.3 Download menu

This section describes the preparation items before starting download menu, notes of using, and the startup method.

Preparations

The download menu uses Internet Explorer to display data. Therefore, the setting of Internet Explorer is required on the PC that uses download menu.

The setting method of Internet Explorer is the same as that of situation when the main menu is used. Refer to "Preparations".

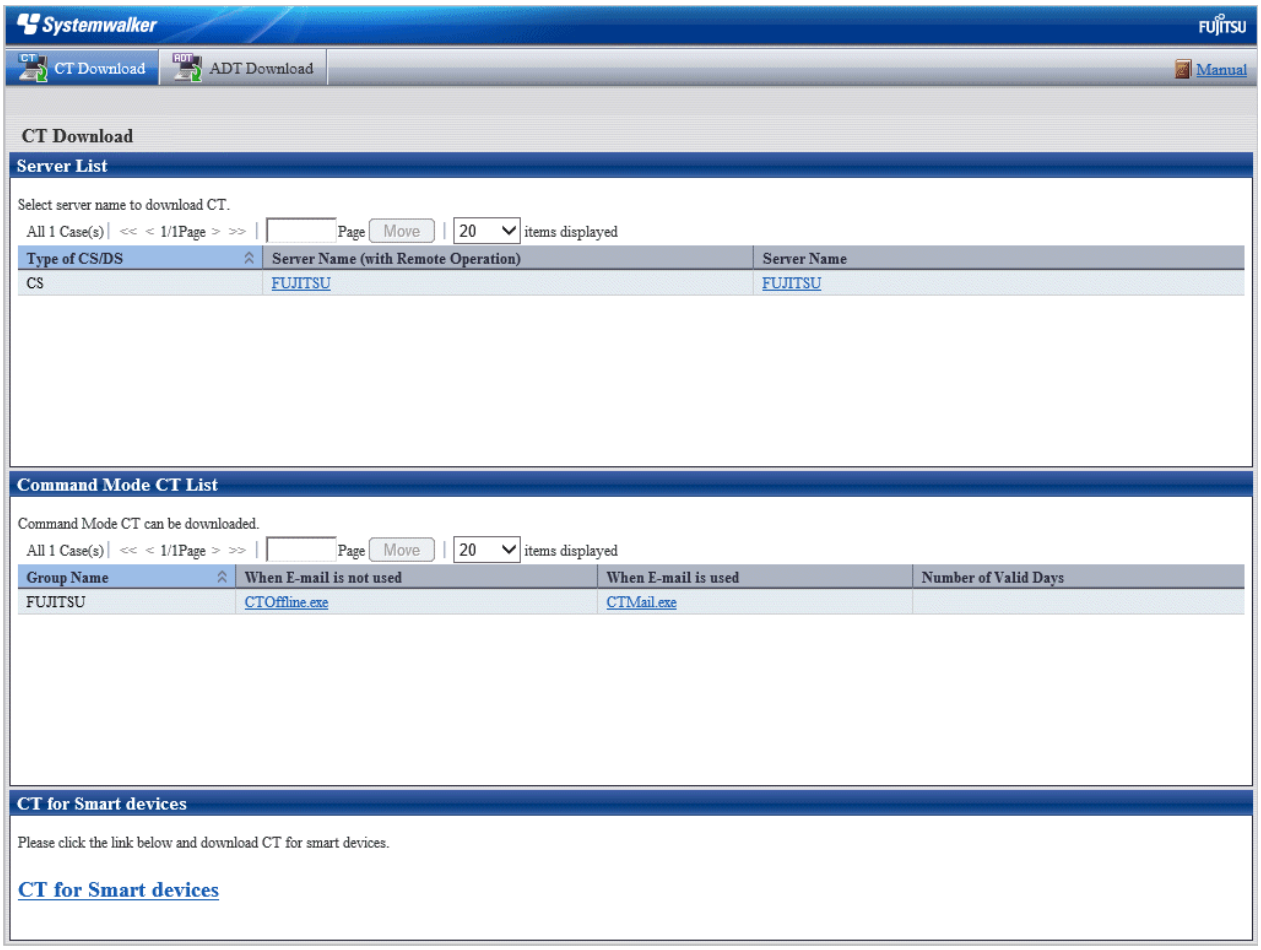
Steps

The procedure of displaying download menu is as follows.

1. Enter the following URL in the address bar of the Web browser.

http:// Server Information (FQDN name or host name or IP address of CS)/DTP/dwl.html

The download menu is displayed.



1.4 AC Menu

This section describes the preparation items before starting the AC Menu, notes of using, and the startup method.

Preparations

The AC menu uses Microsoft(R) Excel to display data. Therefore, perform the following preparations and operations on the PC that uses the AC menu.

- When installing Microsoft(R) Excel, make sure you also install Visual Basic for Applications.
- When the security level of Microsoft(R) Excel is set to **High** or **Highest**, the AC Menu cannot be operated.

  When Microsoft(R) Office Excel 2003 is used, select **Macro** > **Security** from the **Tool** menu of Microsoft(R) Excel, and modify the security level to **Medium**.

  When Microsoft(R) Office Excel 2007 is used, modify the settings according to the following procedure:

  1. Click the **Office** button of Microsoft(R) Excel, and click the **Excel Options** button.
  2. In the **Basic Settings** tab of the option dialog, select the **Show Developer tab in Ribbon** item and click the **OK** button.
  3. Click the **Development** tab displayed in the ribbon and click **Macro Security**.
  4. In the **Macro Settings** window, select **Enable All Macros** and click the **OK** button.

  When Microsoft(R) Office Excel 2010 is used, modify the settings according to the following procedure:

1. Click **File**, and then **Options**.
2. In the **Excel Options** dialog, click **Trust Center**, and in **Microsoft Excel Trust Center**, click **Trust Center Settings**.
3. In the **Trust Center** dialog, click **Macro Settings**. In **Macro Settings**, select **Disable all macros with notification**, and then click **OK**.

When Microsoft(R) Office Excel 2013 is used, modify the settings according to the following procedure:

1. From the Microsoft(R) Excel **Start** screen, display the menu bar through operations such as clicking **Open Other Workbooks**.
2. Click **File**, and then **Options**.
3. In the **Excel Options** dialog, click **Trust Center**, and in **Microsoft Excel Trust Center**, click **Trust Center Settings**.
4. In the **Trust Center** dialog, click **Macro Settings**. In **Macro Settings**, select **Disable all macros with notification**, and then click **OK**.

- In the **Security Warning** window of Microsoft(R) Excel, when Disable Macro] is selected, the AC Menu cannot be operated.

  When the **Security Warning** window of Microsoft(R) Excel is displayed, make sure to select **Enable Macro** or **Enable Content**.

If the above preparations and operations are not performed, the AC Menu cannot run normally. At this time, perform the above settings again after logging off the AC Menu, and then start the AC Menu again.

Notes

- In the process of starting the AC Menu, if the Excel file is being edited at the same time, pay attention to the following items.
  - The AC Menu performed operations such as display data through linking with Microsoft(R) Excel. Therefore, since the AC Menu is using Microsoft(R) Excel, do not open a new Excel file in the display window. If it is needed to open an Excel file using Microsoft(R) Excel during the operation of the AC Menu, start another instance of Microsoft(R) Excel.
  - When opening a new file from the Microsoft(R) Excel being used by the AC Menu, the Excel file may not be displayed, or it may take a long time before it can be displayed.
    If it is still not displayed after 30 seconds, log off the AC Menu and start Microsoft(R) Excel. Then, open the new file from this Microsoft(R) Excel.
- When a new file is opened from the Microsoft(R) Excel being used by the AC Menu, pay attention to the following items.
  - The **x** button at top right of the Microsoft(R) Excel window should not be clicked. To close the Excel file that is newly opened, click the **x** button of this Excel file, or select **Close** or **Exit** from the **File** menu.
  - Do not copy the sheet or modify the sheet name for the Excel file that is being used by the AC Menu. To execute, use it after logging off from the AC Menu.
- When the AC Menu is being used to display or operate data, if the **F11** key is pressed, graph sheet will be added. At this time, return to the previous window according to the following steps.
  1. Right-click the added graph sheet in the sheet list displayed at the bottom of window.
  2. Select delete in the displayed pop-up menu.
  3. When the deletion confirmation message is displayed, click the **OK** button to execute deletion.

Steps

The procedure of starting the AC Menu is as follows.

1. 1. Start the AC Menu.

   On the PC installed with Systemwalker Desktop Patrol AC, select **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Asset Console** or **Apps** > **Systemwalker Desktop Patrol** > **Asset Console**.

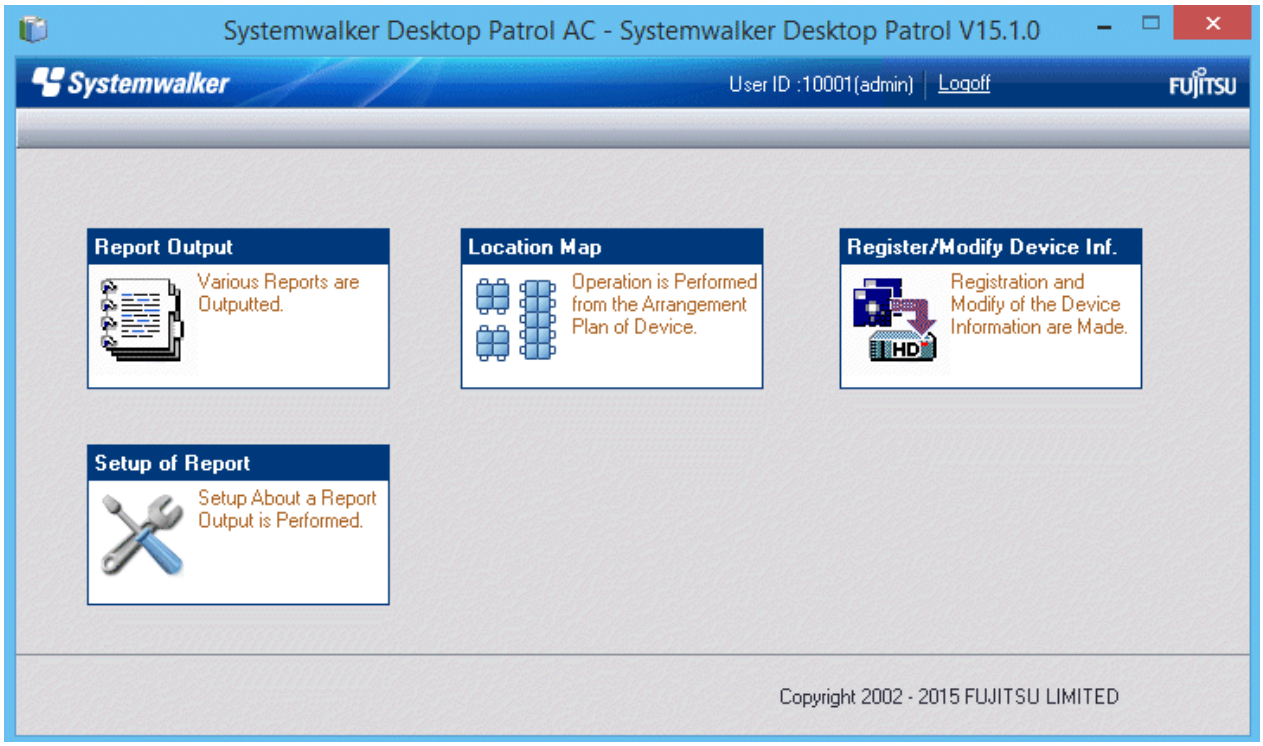
The following window is displayed.

2. Logon.

   Set the following information and click the **Logon** button.

Item	Description
UserID	Set the following information. - System account can set and view the entire system. - Section Management Account can only set and view the entire affiliated section.
Password	Set the password corresponding to the user ID.

The following window is displayed.



3. Select menu according to application.

Chapter 2 Set Operation Environment

This chapter describes the settings of operation environment of Systemwalker Desktop Patrol.

2.1 Construct Master Data

Design the information of section system and managed PCs in order to construct Master data.

In addition, if the operation linked with Active Directory is not performed and under the environment that the Systemwalker Desktop Keeper has been installed, the structure information of Systemwalker Desktop Keeper can be imported into Systemwalker Desktop Patrol.

2.1.1 Design Master Data

The design flow is as follows. For details on the input characters, refer to the *Systemwalker Desktop Patrol Reference Manual*.

1. Divide an organization system into buildings
2. Device each building into sections
3. Specify an higher section
4. Determine the information of a user who manages PCs or smart devices

Divide an organizational system into buildings

Divide an organization system into buildings and determine the office code and building name of each building. The items to be defined are as follows.

Items to be defined	Required/ Optional	Design points	Input length	Characters can be specified
Building Code	Required	Design a code that is easy to identify the building.	1 to 4 digits (Note)	Single-byte numbers
Building Name	Required	Design the building name.	Up to 30 multi-byte characters or 60 single-byte characters	Single-byte alphanumeric characters Single-byte space Multi-byte character The following single-byte symbols "-", "@", ".", "(", ")", "[", "]", "{", "}", "<", ">", ":", ";" However, when multi-byte characters are specified, only 180 bytes can be specified. English letters are case-sensitive.

Note) Though 5 digits can be entered, it is used by Active Directory, so do not use.

Divide each building into sections

Divide each building into coherent sections and determine a particular code and name to each section. The items to be defined are as follows.

The items defined in this step and the items defined in the following "Specifying a higher section" are called Section Management Information.

Items to be defined	Required/ Optional	Design points	Input length	Characters can be specified
Section Code	Required	Divide each section into groups and design the codes.	1 to 36 characters	Single-byte alphanumeric characters The following single-byte symbols "-" When the section code is English letters, enter capital letter (lower-case letter will be registered as capital letters as well).
Section Name	Required	Specify the name of section, etc.	Up to 30 multi-byte characters or 60 single-byte characters	Single-byte alphanumeric characters Single-byte space Multi-byte character The following single-byte symbols "-", "@", ".", "(", ")", "[", "]", "{", "}", "<", ">", ":", ";". However, when multi-byte characters are specified, only 180 bytes can be specified. English letters are case-sensitive.

Specify a higher section

Specify the code as that of higher section based on the designed "Section Code". Items to be defined are as follows.

The items to be defined in this step and the items mentioned previously in the "Divide each building into sections" are called Section Management Information.

Items to be specified	Required/ Optional	Design points	Input length	Characters can be specified
Higher Section Code	Optional	In the upper and lower level structure of section, etc, specify the code of higher section.	1 to 36 characters	Single-byte alphanumeric characters The following single-byte symbols "-" When the higher section code is English letters, enter capital letter (lower-case letter will be registered as capital letters as well).

Determine the information of a user who manages PCs or smart devices

Determine the information of a user who manages PCs or smart devices. The items to be defined are as follows.

The items defined in this step are referred to as User Management Information.

Items to be defined	Required/ Optional	Design points	Input length	Characters can be specified
User ID	Required	Design a user number.	1 to 20 characters	Single-byte alphanumeric characters The following single-byte symbols "-", "@", ".", "_" English letters are case-sensitive.
User Name	Required	Specify the name of a user.	Up to 30 multi-byte characters or 60 single-byte characters	Single-byte alphanumeric characters Single-byte space Multi-byte character The following single-byte symbols "-", "@", ".", "(", ")", "[", "]", "{", "}", "<", ">", ":", ";". However, when multi-byte characters are specified, only 60 bytes can be specified. English letters are case-sensitive.
Password	Optional (Note 1)	Design a password that makes the operation of system easier. The password can be easily changed in the main menu.	4 to 12 characters	Single-byte alphanumeric characters Single-byte space The following single-byte symbols "-", "=", "*", "+", "'", "@", "~", "(", ")", "&", "$", "#", """, "!", "?", "%", "\", ".", ",", "/", ":", ";", "`", "[", "]", "|", "<", ">", "{", "_", "}" English letters are case-sensitive.
Telephone Number	Optional	Specify the telephone Number of a user.	Up to 20 single-byte characters	Single-byte alphanumeric characters Single-byte space The following single-byte symbols "*", "+", ",", "-", ".", "/", "#", "(", ")", "_" English letters are case-sensitive.
Fax Number	Optional	Specify the Fax number of a user.	Up to 20 single-byte characters	Single-byte alphanumeric characters Single-byte space The following single-byte symbols "*", "+", ",", "-", ".", "/", "#", "(", ")", "_" English letters are case-sensitive.

Items to be defined	Required/ Optional	Design points	Input length	Characters can be specified
Email Address	Optional	Specify the Email address of a user.	Up to 50 single-byte characters	Single-byte alphanumeric characters The following single-byte symbols "-", "@", ".", "_", "*" English letters are case-sensitive. Only alphanumeric characters can be specified at the beginning of E-mail address. When two or more "@" symbols are used, error occurs.
Section Code	Optional	Specify a code of the section to which a user belongs.	1 to 36 characters	Single-byte alphanumeric characters The following single-byte symbols "-" When the section code is English letters, enter capital letter (lower-case letter will be registered as capital letters as well).
Building Code	Optional	Specify a building office code that indicates the location of users.	1 to 4 digits (Note 2)	Single-byte numbers

Note 1) When logging in to the main menu, password is required.

Note 2) Though 5 characters can be entered, it is used by Active Directory, so do not use.

Point

The displayed window of main menu will be sorted in the display sequence according to character code.

Therefore, when registering the Master data, the file in CSV format will be created according to the following points. Therefore, the content displayed on the main menu will be sorted in a simple way.

- Define the beginning of user name, section name and building name in alphabet order and ascending numeric order.

Example of User Name

Master Data	Improvement Example with Sort Sequence being Considered
- Fujitsu Taro - Fujitsu Hanako	- a001_Fujitsu Taro - a002_Fujitsu Hanako

Example of Section Name

Master Data	Improvement Example with Sort Sequence being Considered
- Sales Section	- 00_Sales Section

Master Data	Improvement Example with Sort Sequence being Considered
- Administration Section	- 01_Administration Section

2.1.2 Procedure of Constructing Master Data at Active Directory Linkage

This section describes how to construct the Master data of Systemwalker Desktop Patrol when linking with Active Directory.

Relationship between management information of Active Directory and master data

It describes the relationship when the management information of Active Directory is registered as the Master data of Systemwalker Desktop Patrol.

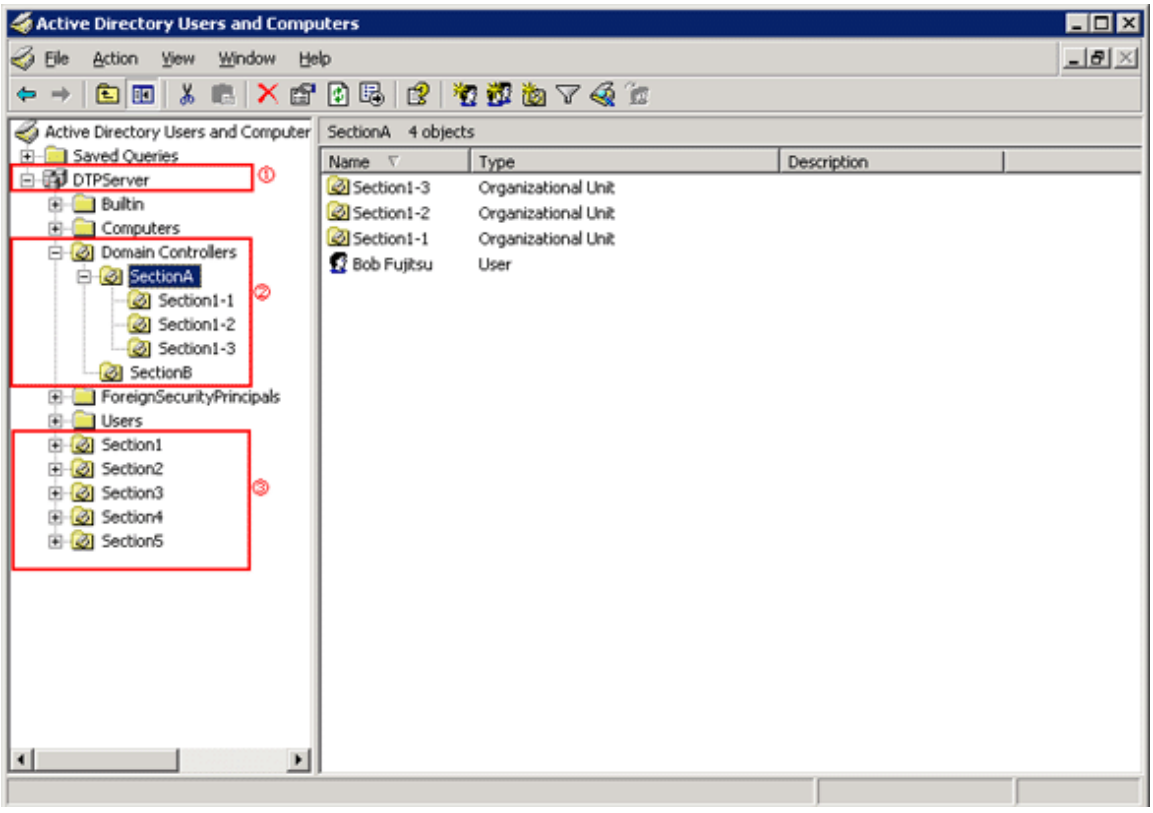
On Systemwalker Desktop Patrol, obtain the OU (Organizational Unit) information of Active Directory.

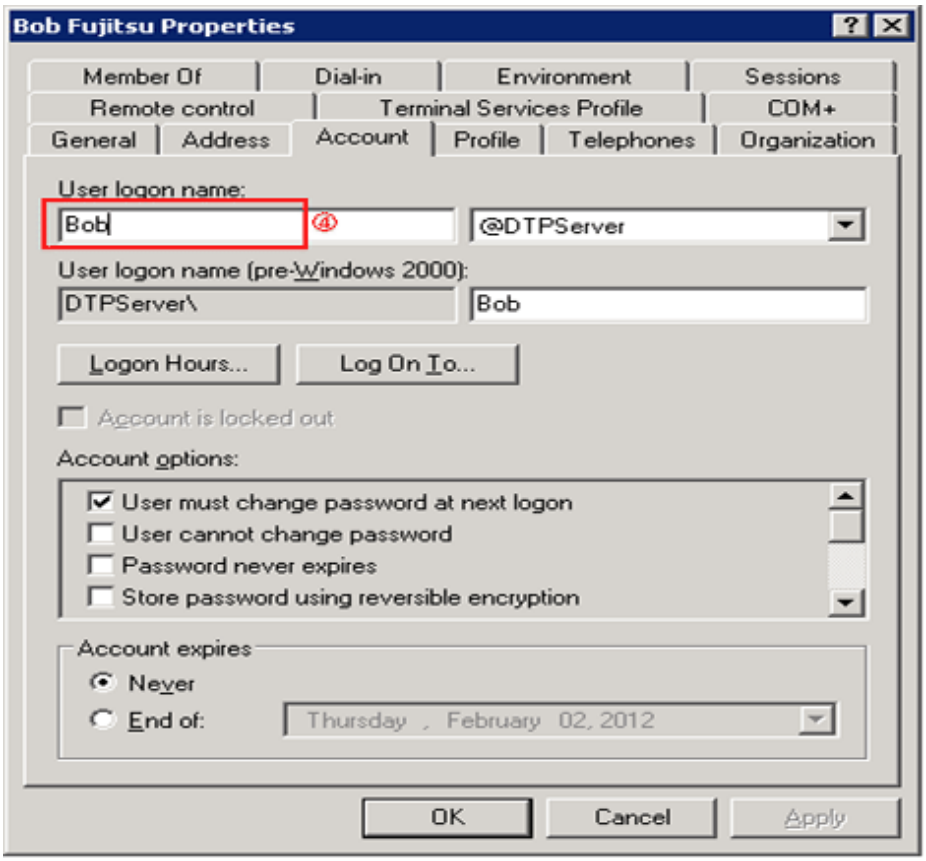
In the following example, only the OU of "Domain Controllers" and user creation is expected to be obtained. In addition, for user information, the user information that belongs to each OU will be used as the user that belongs to the section of Systemwalker Desktop Patrol directly.

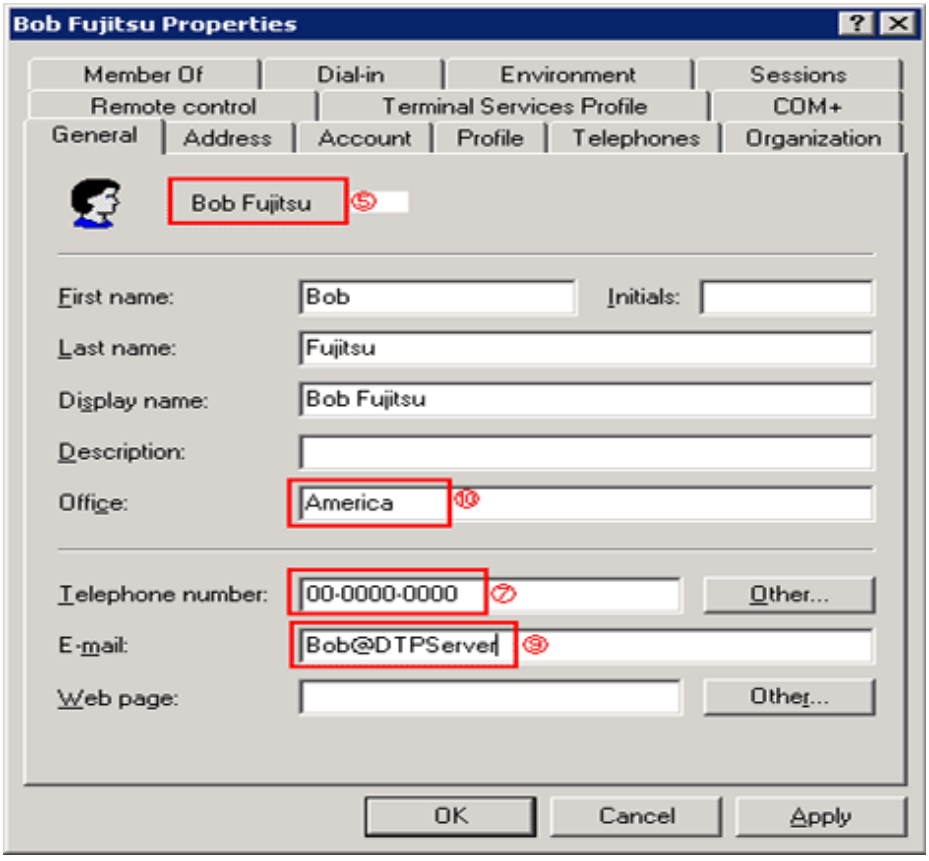
Refer to the following diagram for the relationship of information. (1) ~ (10) of management information of Active Directory corresponds to (1) ~ (10) of the main menu.

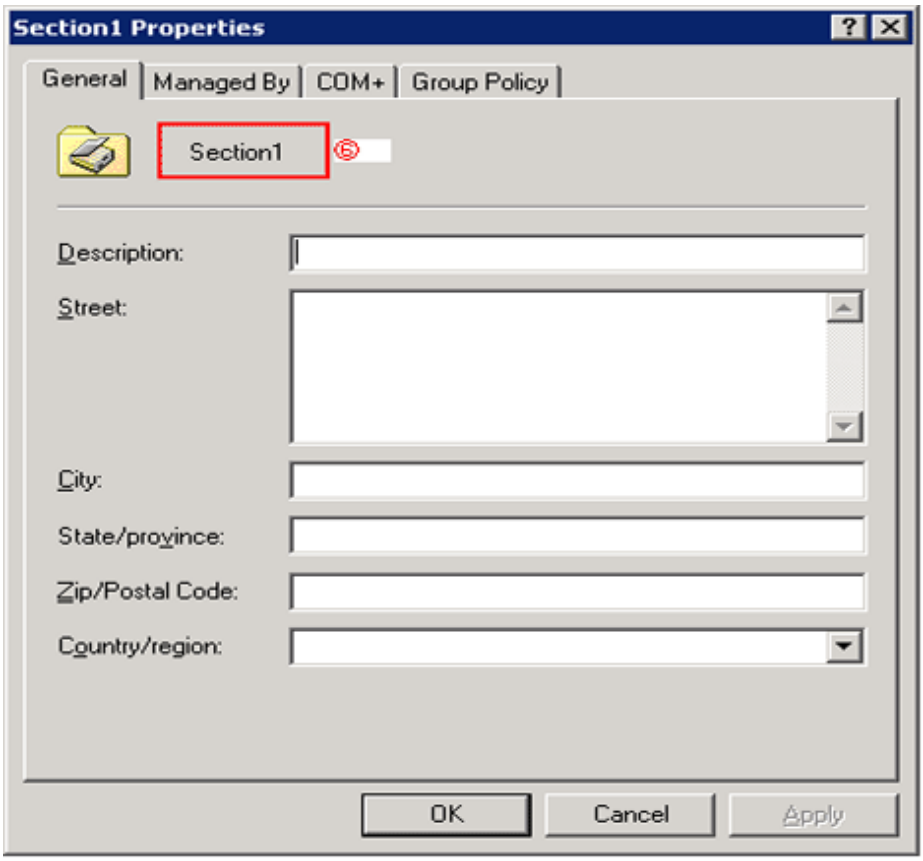
Example of Management Information of Active Directory

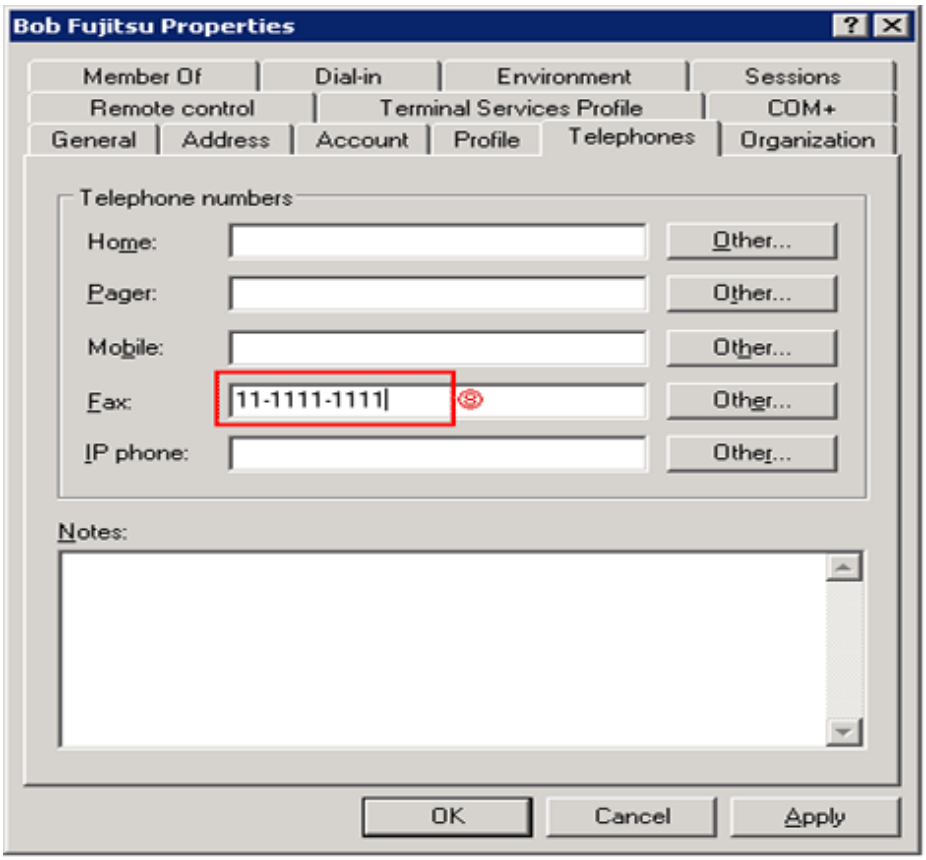
The example of management information of Active Directory is shown as follows.




Bob Fujitsu Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User logon name:
Bob
④
@DTPServer
User logon name (pre-Windows 2000):
DTPServer\
Bob
Logon Hours...
Log On To...
Account is locked out
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Thursday , February 02, 2012
OK
Cancel
Apply


Bob Fujitsu Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Bob Fujitsu
⑤
First name:
Bob
Initials:
Last name:
Fujitsu
Display name:
Bob Fujitsu
Description:
Office:
America
⑩
Telephone number:
00-0000-0000
⑦
Other...
E-mail:
Bob@DTPServer
⑨
Web page:
Other...
OK
Cancel
Apply


Section1 Properties
General
Managed By
COM+
Group Policy
Section1
Description:
Street:
City:
State/province:
Zip/Postal Code:
Country/region:
OK
Cancel
Apply

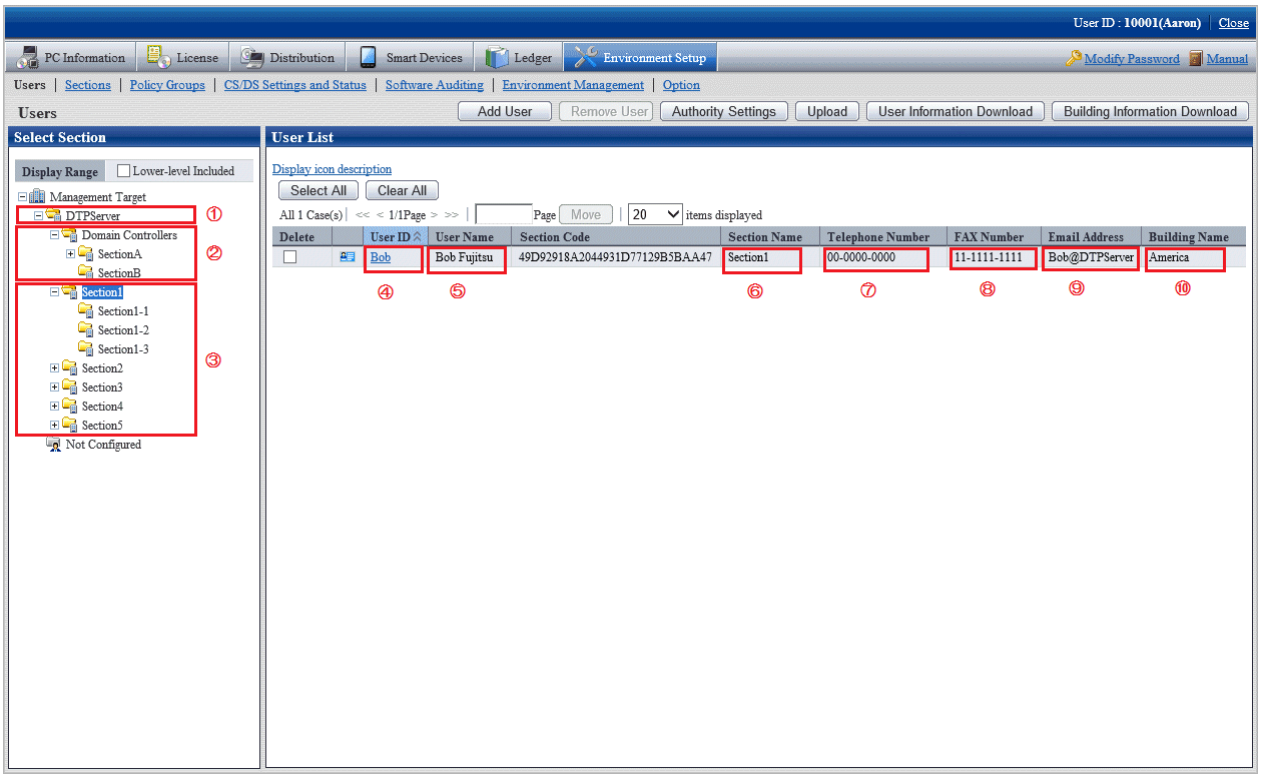

Bob Fujitsu Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Telephone numbers
Home:
Pager:
Mobile:
Fax:
11-1111-1111
IP phone:
Other...
Notes:
OK
Cancel
Apply

Display Example of main menu

The example when the management information of Active Directory mentioned above is used as the Master data of Systemwalker Desktop Patrol is shown below.

The section information obtained from Active Directory is displayed under the section tree in which the domain name is the highest level section.

In addition, section tree may be different from the display sequence of Active Directory.



Point

When the management information of Active Directory is used as the Master data of Systemwalker Desktop Patrol, the entire section in which the domain name is as the highest level section will become the linkage object. The other sections can be managed in the same way as the time when Active Directory linkage is not performed.

Note

After the OU information of Active Directory has been deleted, when the OU is created again with the same name, the section management information of Systemwalker Desktop Patrol will also be deleted. Therefore, when license management is being used, do not delete OU information.

About restrictions of input value of master data

When linking with Active Directory, the management information of Active Directory will be defined as the Master data of Systemwalker Desktop Patrol as shown in the following table. At this time, the restrictions of input characters will comply with the restriction value of Master data of Systemwalker Desktop Patrol.

In addition, when linking with Active Directory, since password is not defined as Master data, define is if necessary.

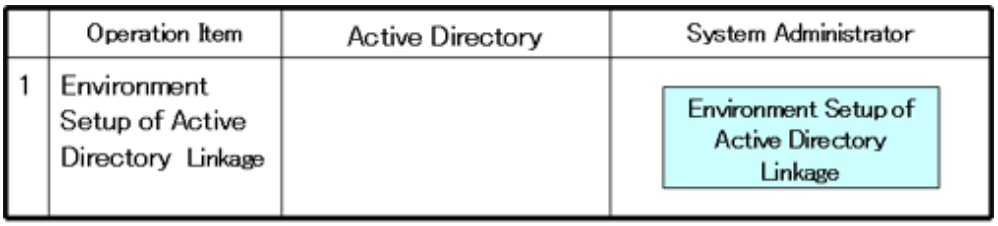
	User Management Information	Section Management Information	Building Management Information
User ID	String before the @ of User Principal Name	-	-
User Name	name	-	-
Password	-	-	-
Telephone Number	telephone Number	-	-
Fax Number	Facsimile Telephone Number	-	-
E-mail Address	mail	-	-
Section Code	-	Object GUID	-
Section Name	-	OU name	-
Higher Section Code	-	Object GUID	-
Building Code	-	-	A code with 5 digits or more is generated automatically.
Building Name	-	-	Physical Delivery Office Name

Procedure of linking with Active Directory

The procedure of linking with Active Directory is shown as follows.

Start linking with Active Directory

Start linking with Active Directory according to the following flow.



1. Use one of the following methods to configure the Active Directory linkage environment setup:

   - Execute the dtpadset.exe (Active Directory linkage environment setup) command.
   - Log in to the main menu, click **Environment Setup** > **CS/DS Settings and Status**, and configure the CS environment setup.

   For details on the dtpadset.exe (Active Directory linkage environment setup) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

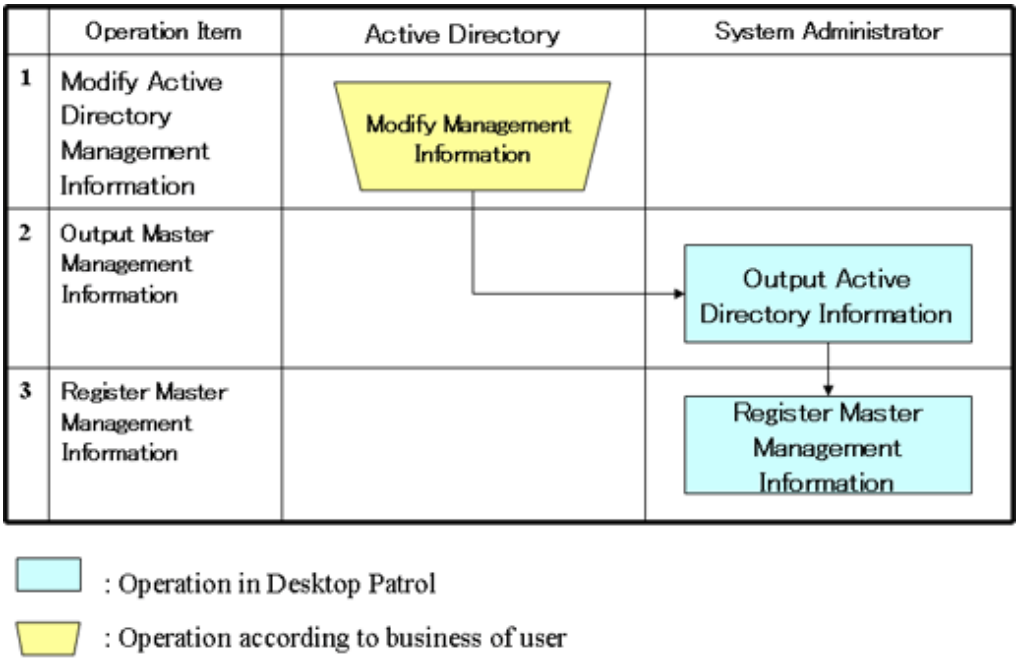
   Refer to the *Systemwalker Desktop Patrol Installation Guide* for details on environment setup from the main menu.

   If the environment for linking with Active Directory has been set, the following value will be set automatically as the timing of logon to the Windows domain again in the **User Identification Information** table of CT.

   - User ID: Logon name of Windows domain
     (In case of "user@domain.jp", "domain\user", the part of "user" will be set.)

- PC Name: Computer name

Link with Active Directory



1. Modify the management information on Active Directory.
2. Execute the dtpadmst.exe (Active Directory information output) command to output Master data. For details on the dtpadmst.exe (Active Directory information output) command, refer to *Systemwalker Desktop Patrol Reference Manual*.
3. Register Master data through the dtpmast.exe (Master data construction) command or the **Environment Setup** window of the main menu. For details on the dtpmast.exe (Master data construction) command, refer to *Systemwalker Desktop Patrol Reference Manual*. For information on how to register through the **Environment Setup** window of the main menu, refer to "2.1.3 Procedure of Constructing Master Data".

Note

In the Master data output through the dtpadmst.exe (Active Directory information output) command, do not modify the content apart from password. If the section code, user ID, building code has been modified, linkage cannot be performed normally. When other information is modified, the management information of Active Directory will be overwritten at next time of linkage.

Point

After the operation has been started, the difference (add, modify, delete) from the latest information of Active Directory management information through making the above "Step 2" and "Step 3" into batch file will be reflected to the Master data of Systemwalker Desktop Patrol and operation can be automated.

- Example of batch file

  In this example, the Master data is output to the work directory, and the master information is registered using the dtpmast.exe (Master data construction) command. If the Master data file has already existed, overwrite this file. Make proper modification in actual operation.

```
@ECHO OFF
SETLOCAL

SET WORKDIR= Name of work directory (optional)
```

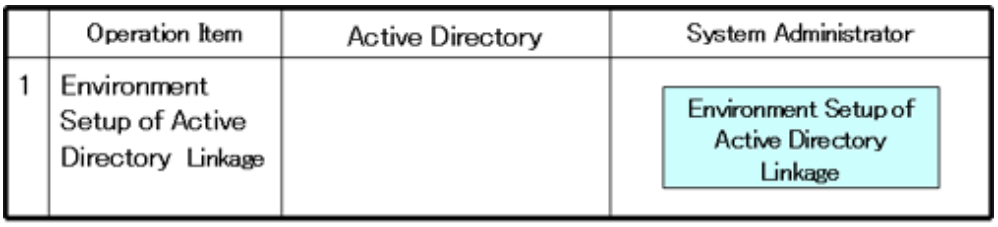
```
SET CMD_DTPADMST="Installation Directory of CS\bnserv\bin\dtpadmst.exe"
SET CMD_DTPMAST=" Installation Directory of CS\bnserv\bin\dtpmast.exe"


REM Extract information from Active Directory.
%CMD_DTPADMST% /d%WORKDIR%
IF ERRORLEVEL 1 GOTO end

REM Delete the data exists in Systemwalker Desktop Patrol but does not exist in Active Directory.
%CMD_DTPMAST% /d /me /f%WORKDIR%/deluser_ad.csv /e%WORKDIR%/deluser_err.log
IF ERRORLEVEL 1 GOTO end
%CMD_DTPMAST% /d /mg /f%WORKDIR%/delsect_ad.csv /e%WORKDIR%/delsect_err.log
IF ERRORLEVEL 1 GOTO end
%CMD_DTPMAST% /d /mb /f%WORKDIR%/delbldg_ad.csv /e%WORKDIR%/delbldg_err.log
IF ERRORLEVEL 1 GOTO end

REM Register the information extracted from Active Directory.
%CMD_DTPMAST% /s /me /f%WORKDIR%/moduser_ad.csv /e%WORKDIR%\moduser_err.log
IF ERRORLEVEL 1 GOTO end
%CMD_DTPMAST% /s /mg /f%WORKDIR%\modsect_ad.csv /e%WORKDIR%\modsect_err.log
IF ERRORLEVEL 1 GOTO end
%CMD_DTPMAST% /s /mb /f%WORKDIR%\modbldg_ad.csv /e%WORKDIR%\modbldg_err.log
IF ERRORLEVEL 1 GOTO end

:end
ENDLOCAL
EXIT /b %ERRORLEVEL%
```

Note

The information of the **User Identification Information** tab of CT will not be modified automatically, modify it if necessary.

Stop linking with Active Directory

Stop linking with Active Directory according to the following flow.



1. Use one of the following methods to configure the Active Directory linkage environment setup:

   - Execute the dtpadset.exe (Active Directory linkage environment setup) command.
   - Log in to the main menu, click **Environment Setup** > **CS/DS Settings and Status**, and configure the CS environment setup.

   For details on the dtpadset.exe (Active Directory linkage environment setup) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

   Refer to the *Systemwalker Desktop Patrol Installation Guide* for details on environment setup from the main menu.

2.1.3 Procedure of Constructing Master Data

The data that is used in common at many scenario of this system such as section and personnel information, etc will be managed collectively according to type. This type of data is called Master data and the following types are included.

Type	Description	Relationship of other management information file
User Management Information	File of user information	Link through **Section Code** and **Building Code** of other management information file.
Section Management Information	File of section information	Link through user information and **Section Code**. (**Section Code** is obtained by referring to **Higher Section Code**.)
Building Management Information	File of building information	Link with user information through **Building Code**.

When registering this type of Master data to this system, it is necessary to construct Master data. In addition, before using the system, the following Master data must be registered.

- User Management Information
- Section Management Information

The relationship between type and item of Master data is shown as follows. Refer to it when constructing the Master data. In addition, the definition of symbol in the table is as follows.

- "Y": required items in management information
- "O": optional items in management information
- "N": not required in management information

	User Management Information	Section Management Information	Building Management Information
User ID	Y	N	N
User Name	Y	N	N
Password	O(Note)	N	N
Telephone Number	O	N	N
Fax Number	O	N	N
E-mail Address	O	N	N
Section Code	O	Y	N
Section Name	N	Y	N
Higher Section Code	N	O	N
Building Code	O	N	Y
Building Name	N	N	Y

Note) Password is required when login to the main menu.

The Master data is registered on **Environment Setup** of the main menu. The method of registration is as follows. In addition, when constructing Master data, make sure to perform by system administrator only.

- Construction of Master data through data upload
- Construction of Master data through the dtpmast.exe (Master data construction) command

For details on "Construction of Master data through data upload", refer to the following description. For details on "Construction of Master data through the dtpmast.exe (Master data construction) command", refer to "dtpmast.exe (Master data construction)" of *Systemwalker Desktop Patrol Reference Manual*.

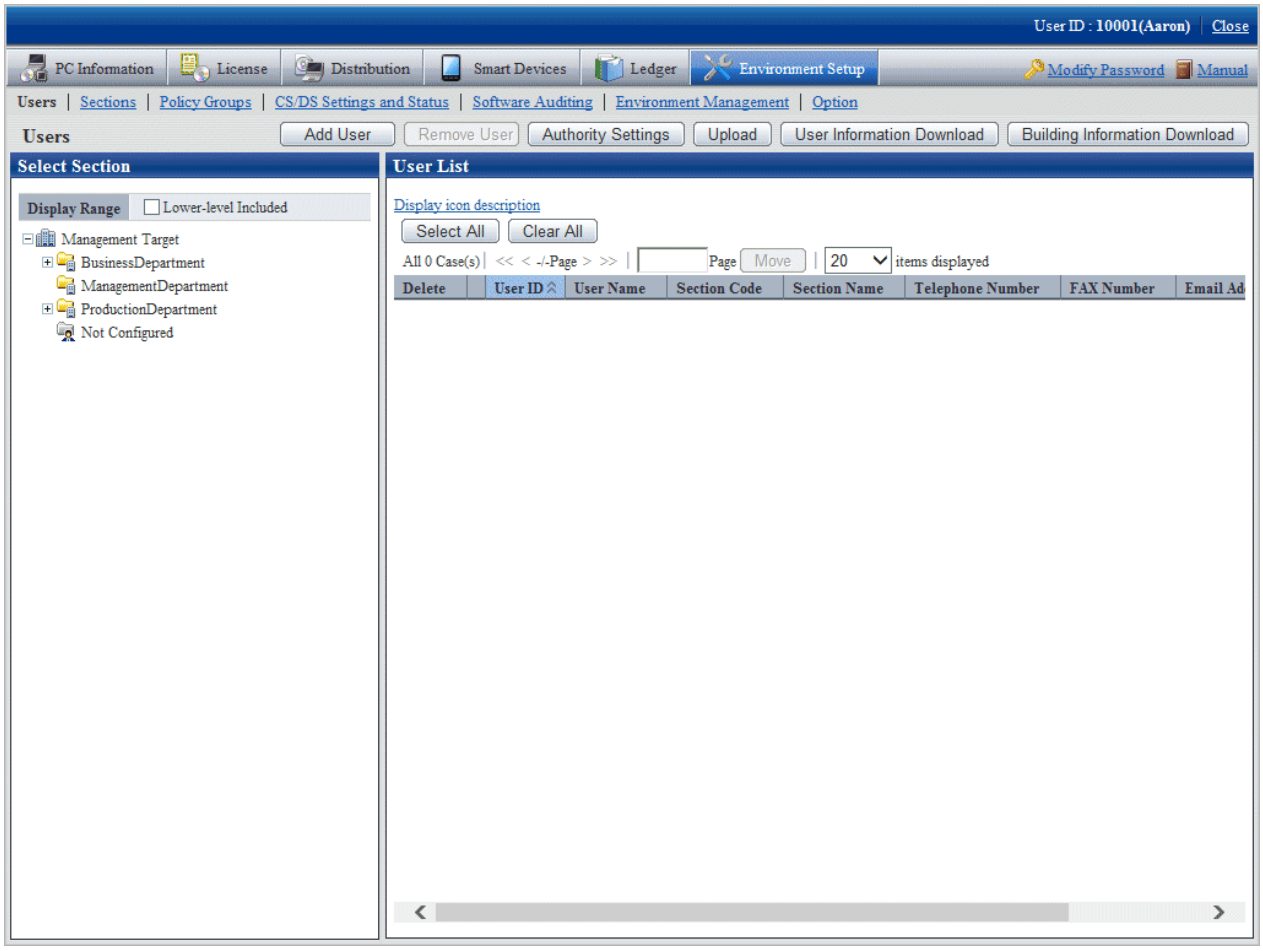
Procedure

Before the operation of Systemwalker Desktop Patrol, it is necessary to construct Master data.

Construct Master data according to the following procedure.

1. Login to the main menu, and click **Environment Setup**.

   The **Environment Setup** window is displayed.



2. Click the following item to construct Master data.

   - **Users**
   - **Sections**

   The selected window will be displayed. For the displayed window, refer to the description after the following items.

3. To exit, click the **Close** button to logout from the main menu.

2.1.4 Create Section Management Information

Create section information through one of the following approaches.

- Register or delete through the operation of the **Environment Setup** window

- Register through uploading the CSV file

2.1.4.1 Register Section

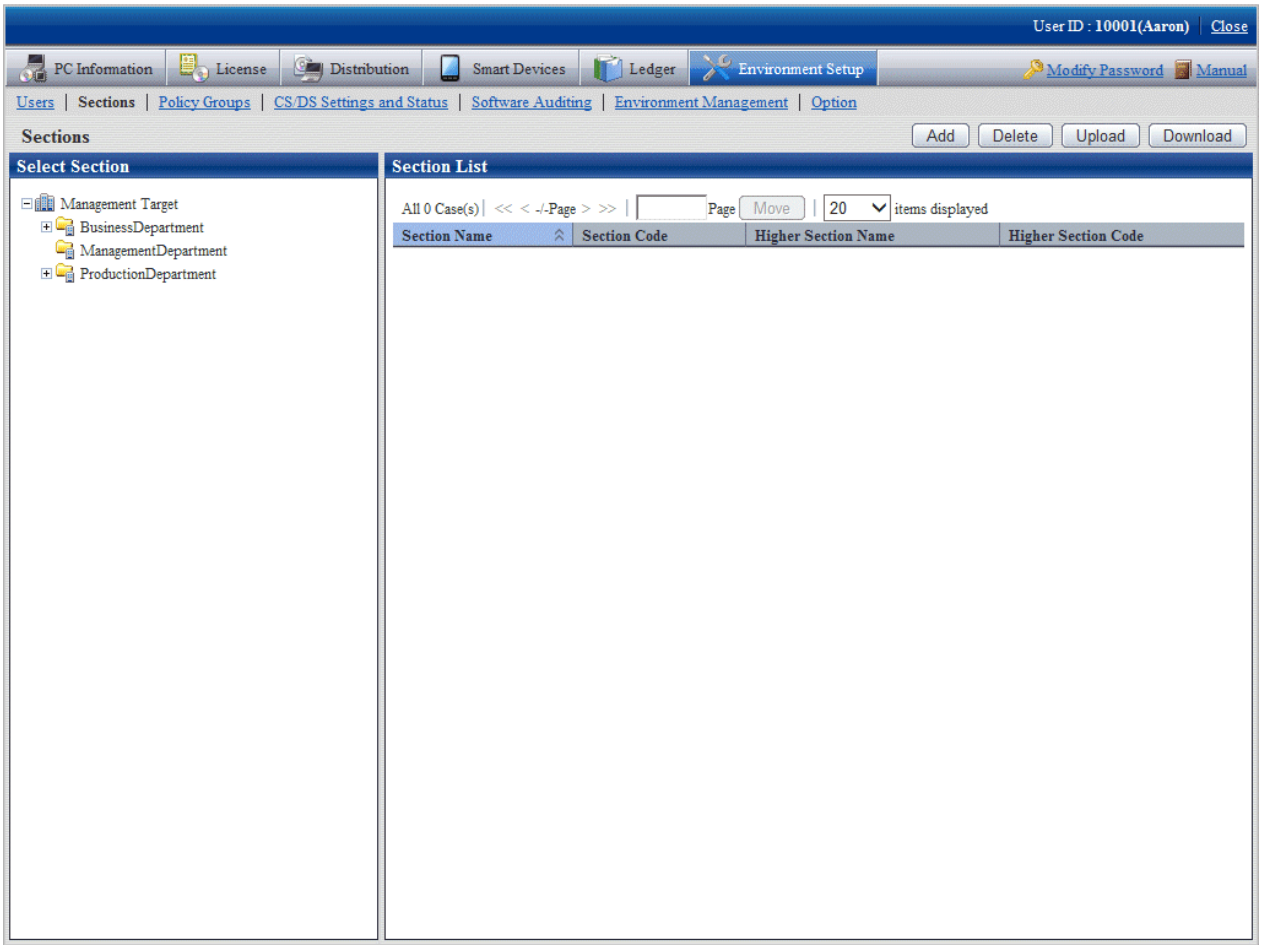
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**

   The **Environment Setup** window is displayed.

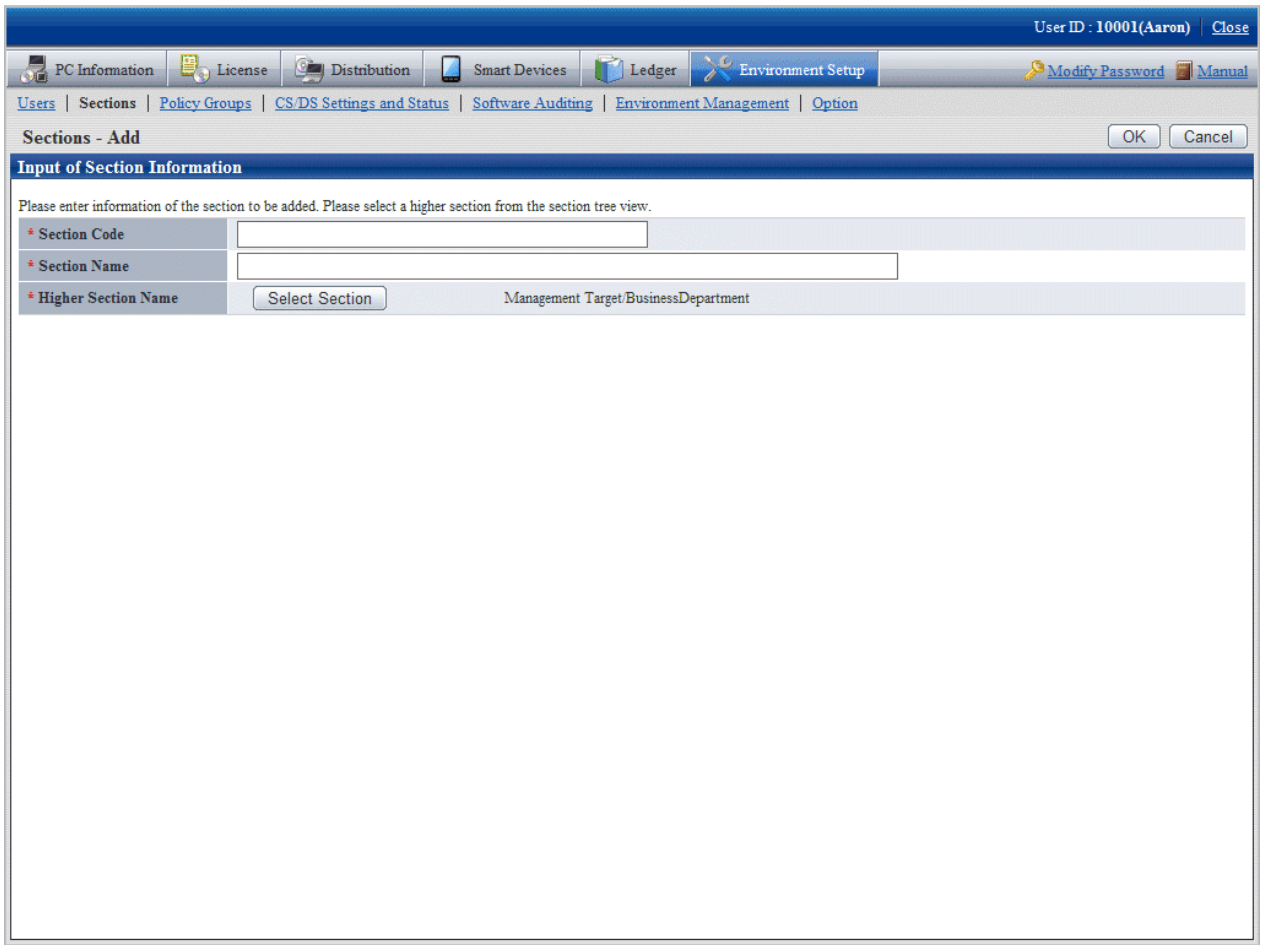
2. Click the **Sections** button.

   The following window is displayed.



3. Click the **Add** button.

   The following window is displayed.



4. Enter the information of the section to be registered.

Items to be defined	Input Characters
Section Code	Specify a section code. Use up to 36 single-byte alphanumeric characters and "-". When the section code is English letters, enter capital letter (lower-case letter will be registered as capital letters as well).
Section Name	Specify the name of a section or section. 30 multi-byte characters or 60 single-byte characters (alphanumeric characters and the following single-byte symbols). "-", "@", ".", "(", ")", "[", "]", "{", "}", "<", ">", ":", ";". However, when multi-byte characters are specified, only 180 bytes can be specified.
Higher Section Name	Enter the section at the higher of the section to be added. Click the **Select Section** button and select.

5. Click the **OK** button.

   The section management information is registered.

2.1.4.2 Delete Section

It describes how to delete a section.

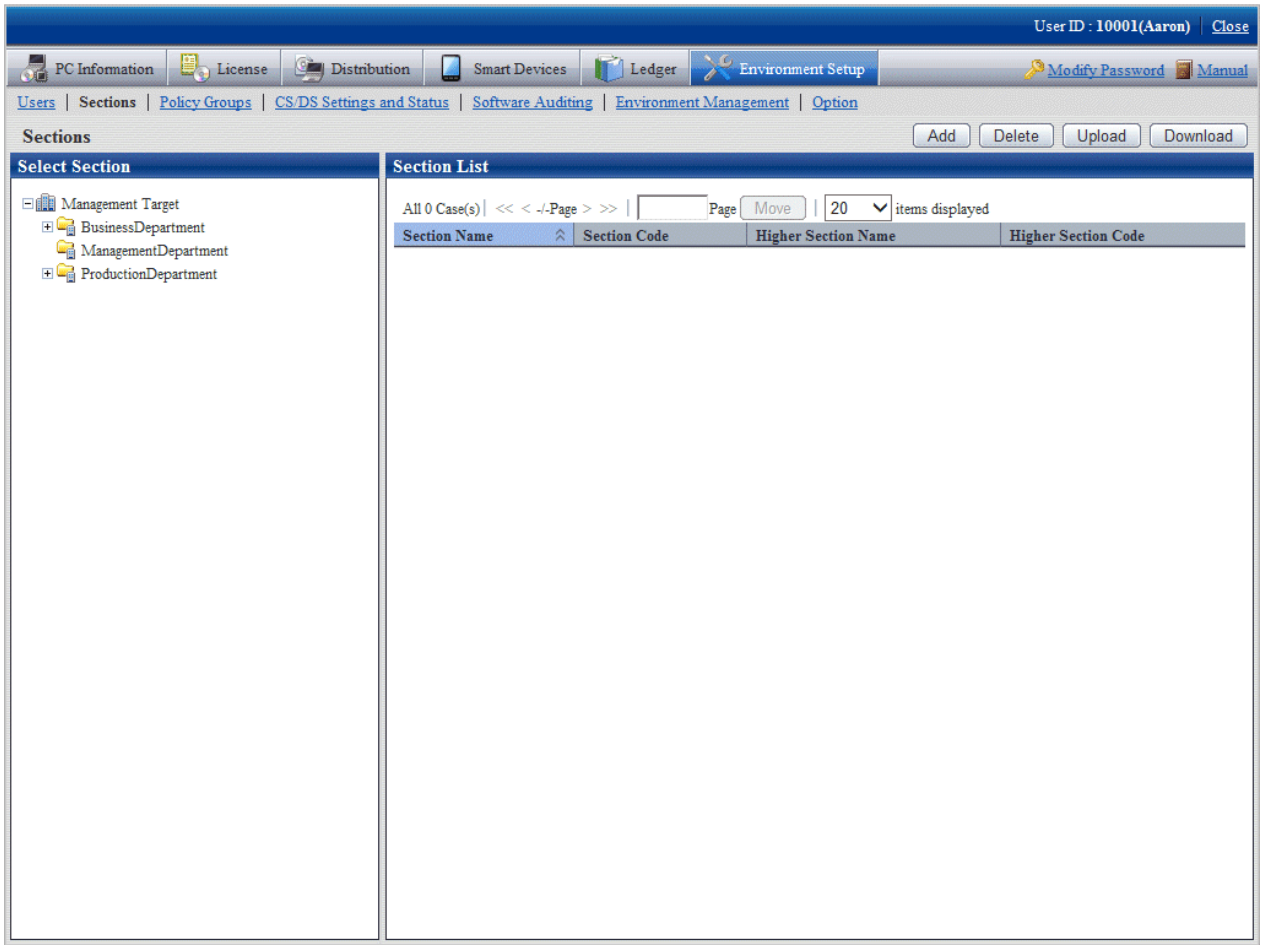
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

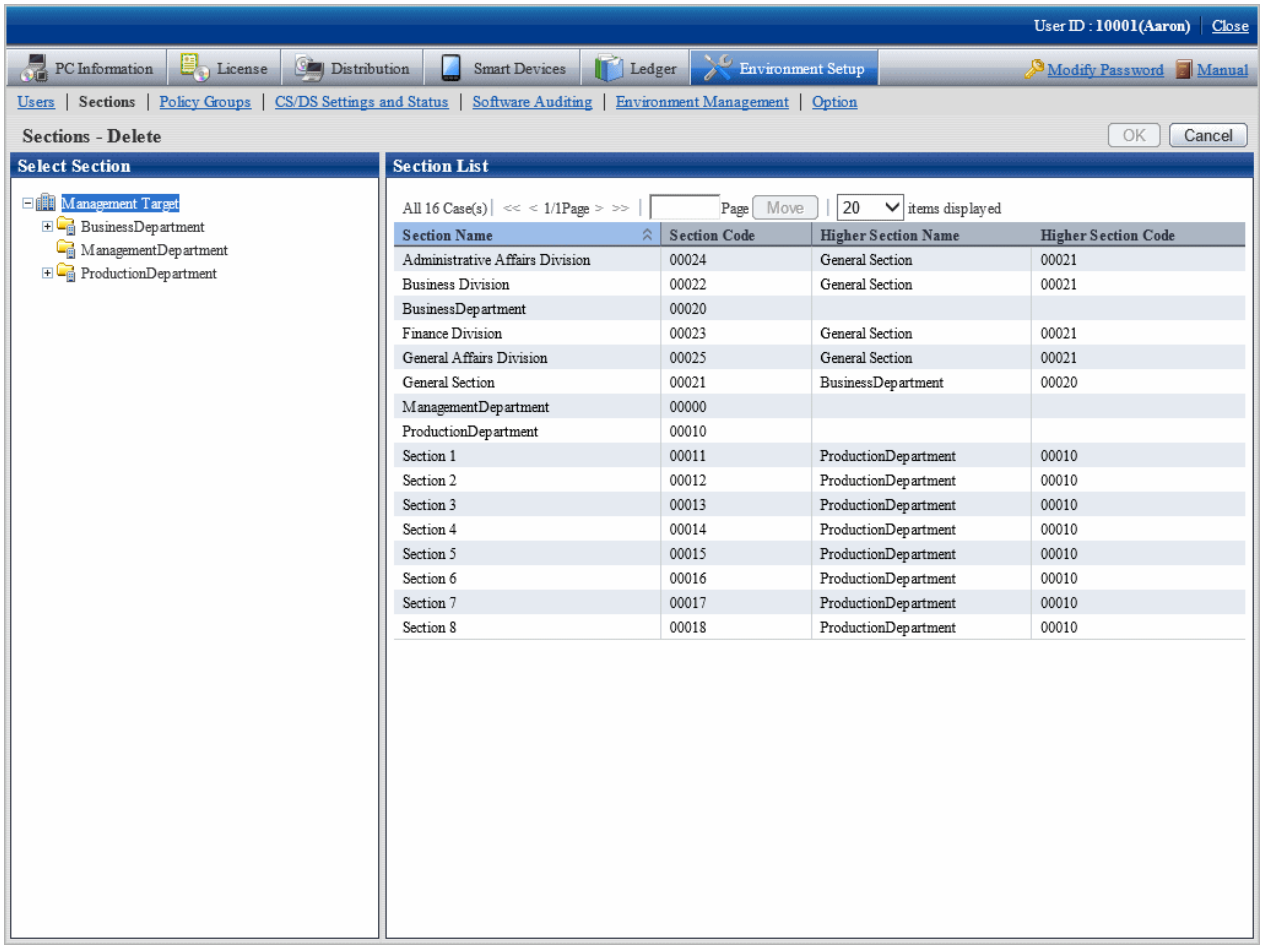
2. Click the **Sections** button.

   The following window is displayed.



3. Click the **Delete** button.

   The following window is displayed.



4. Select the section to be deleted from the tree on the left, and click the **OK** button.

   Section management information is deleted.

   - If PC exists in the section to be deleted, the section cannot be deleted.

     If the section to which the user of PC (user) belongs has been modified, delete the section after modifying the section to which the user belongs or deleting the user. Alternatively, delete the section after deleting the correspondent PC in the deletion of **PC Information** > **Inventory Information** window.

   - After the section has been deleted, the user of "Section Management Account" that belongs to the deleted section will become "User Account".

   - After the section has been deleted, the user that belongs to the section to be deleted will be moved to the not Configured user.

2.1.4.3 Register through Uploading

Record the section management information to a file in CSV format, and register the section by uploading this file.

For details of the CSV file format, refer to the *Systemwalker Desktop Patrol Reference Manual*.

New registration

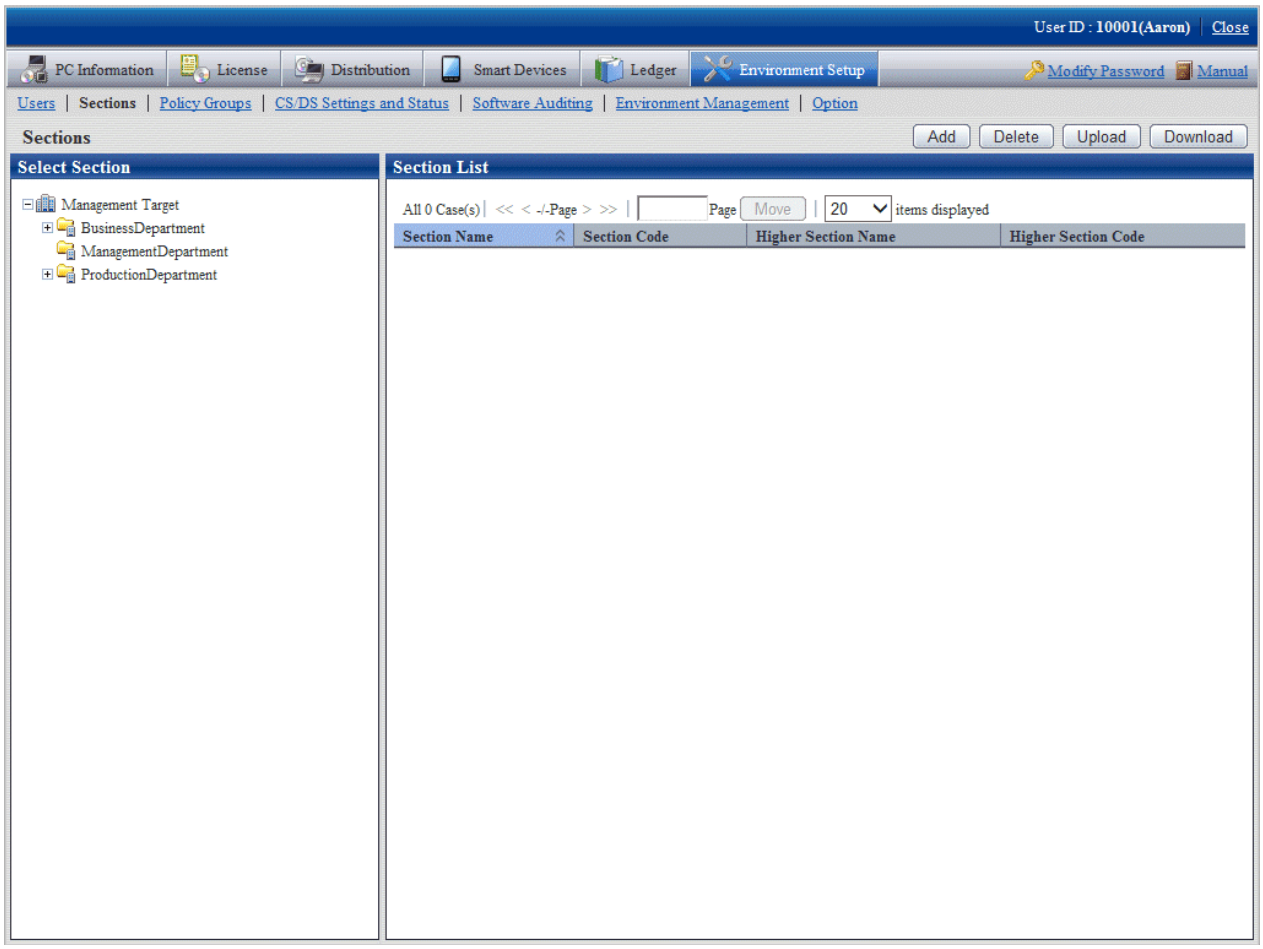
The method of new registration by uploading is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

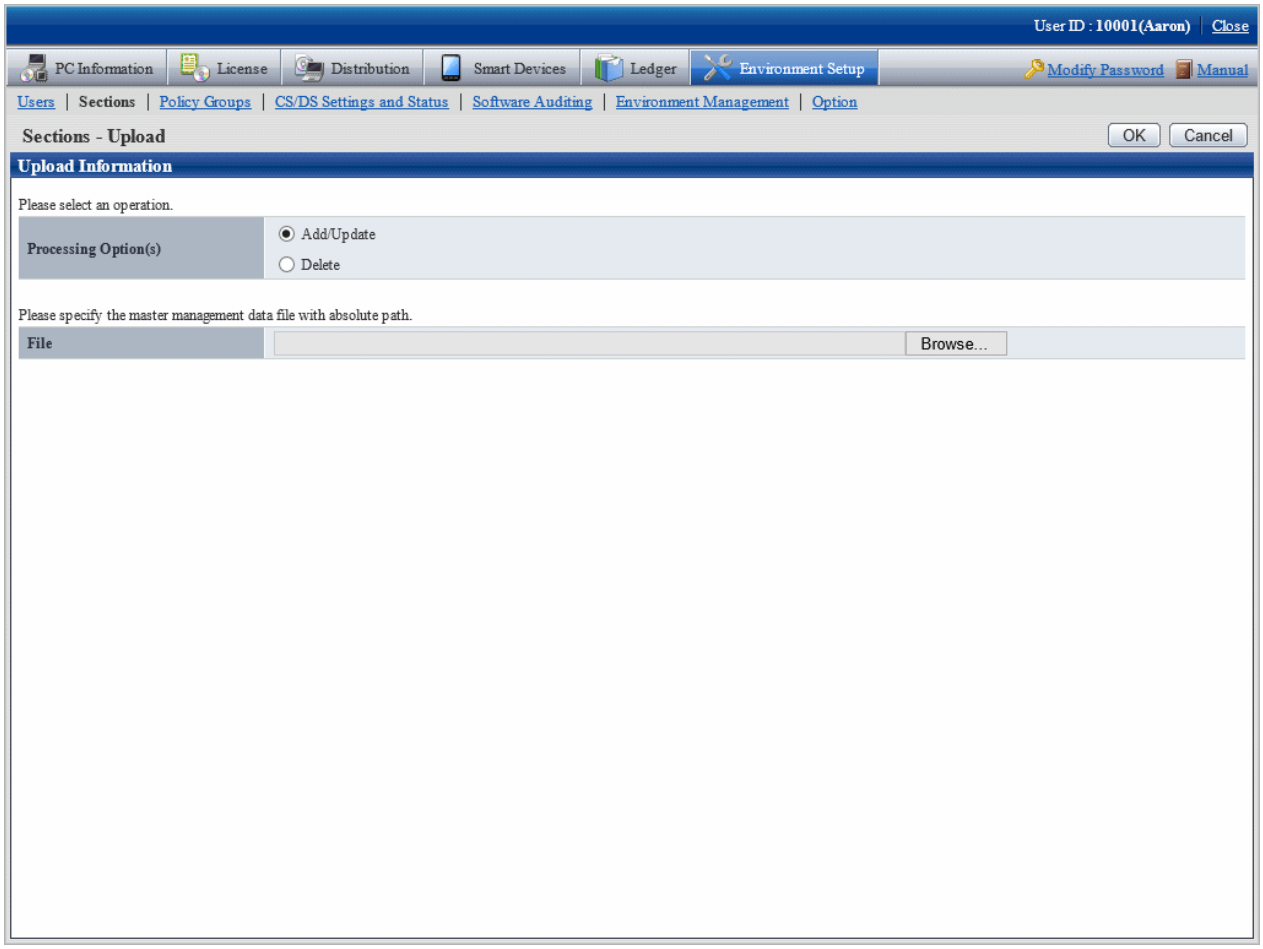
2. Click the **Sections** button.

   The following window is displayed.



3. Click the **Upload** button.

   The following window is displayed.



4. Enter the following items.

   - **Processing Option(s)**

     Select the operation content from the following items.

Item	Meaning
Add/Update	Add/Update the data that has been registered in Master data. Register new data in which the value of key item of the data to be uploaded should not be duplicated as the value of **Key Item** of the management information that has been registered. Update the data in which the value of the key item of data to be uploaded is matched with the value of **Key Item** of the management information that has been registered. * The **Key Item** is the initial item of management information created in CSV format.
Delete	Delete the data that has been registered in Master data. Delete the data in which the value of **Key Item** of the data to be uploaded is the same as the value of **Key Item** of the management information that has been registered, * The **Key Item** is the initial item of management information created in CSV format.

- **File**

  Select the file in CSV format.

5. After the specification has completed, click the **OK** button.

   The upload result is displayed.

   When error occurred, the list of section that cannot be added/updated due to inconsistence of section management information can be downloaded.

   For error content, refer to the error content of "dtpmast.exe (Master data construction)" command in *Systemwalker Desktop Patrol Reference Manual*.

Modify a registration

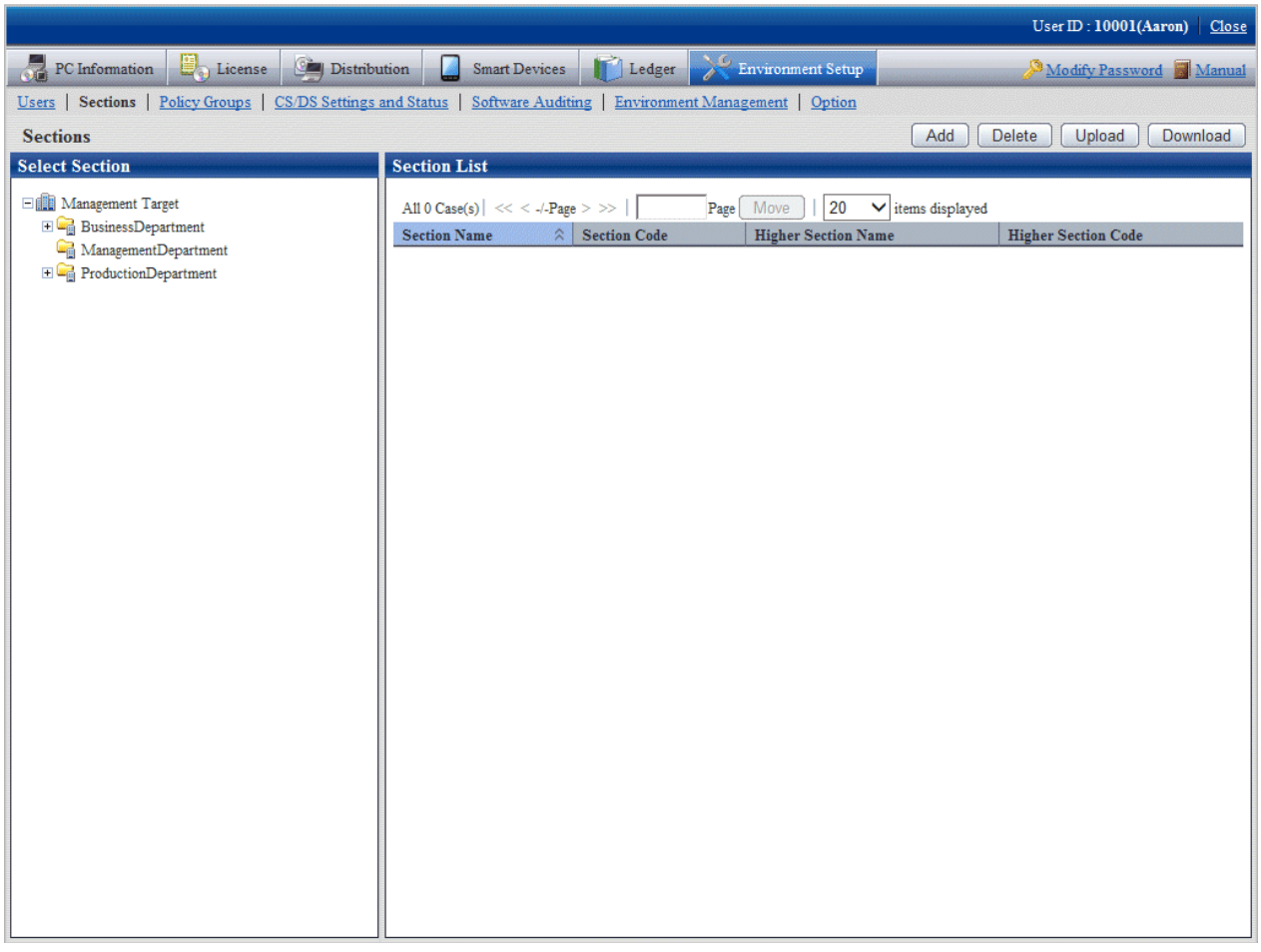
The method of modifying the registered Master data is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

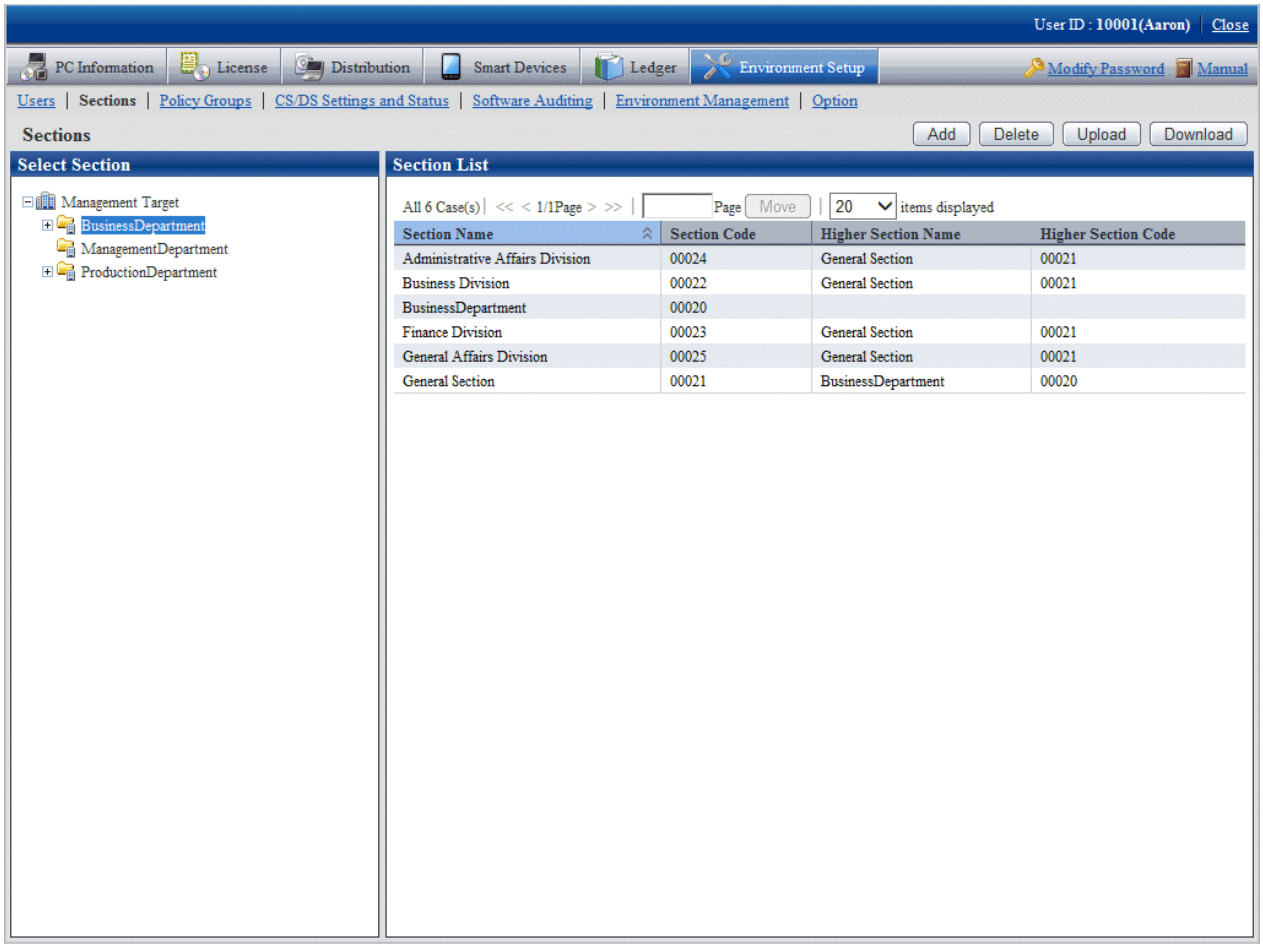
2. Click the **Sections** button.

   The following window is displayed.



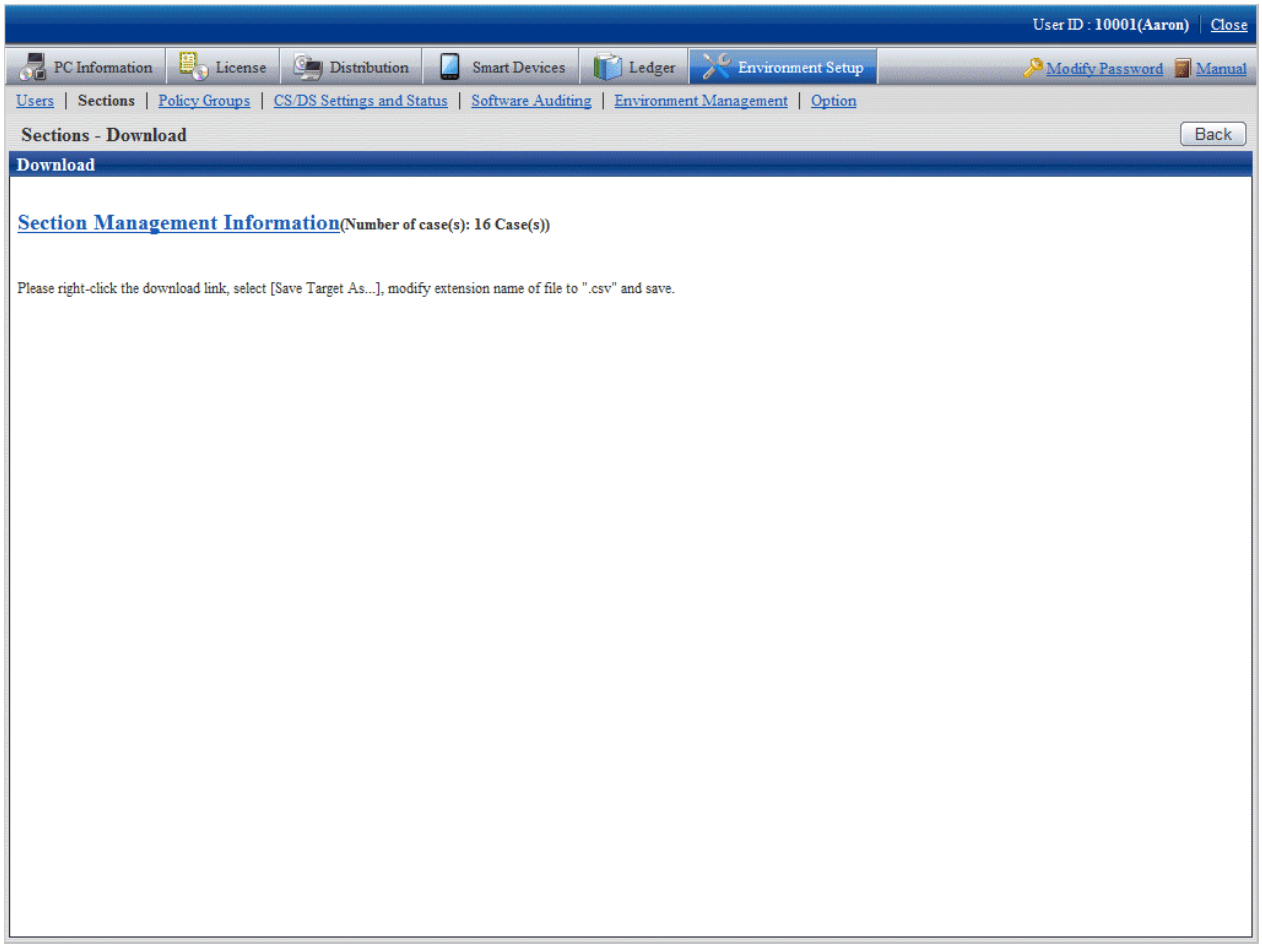
3. Select a section from the tree of the left field.

   The organizations under the selected section is displayed on the right field.



4. Click the **Download** button.

   The following window is displayed.



5. Right-click the download anchor and select **Save to a file** or **Save the link**. Save it by the ".csv" extension.
6. Edit the downloaded file and create a data file according to the purpose of addition, updating, or deletion.

Note

When modifying and saving the downloaded file with CSV format using Microsoft Excel, pay attention to the following.

- Although the double quotation marks are used for displaying values in the original file, they may disappear after modifying and saving with Excel.

  At this time, add double quotation marks using text editor, etc.

- When the front part is 0, like "000001", in the original file, after modifying and saving with Excel, the number 0 in the front part will disappear and will be replaced by "1".

  In this case, when modifying with Excel, use the user format that displays "0" at higher, or add the single quotation marks in the front of the value, and it is recognized compulsorily as a character item in Excel.

7. As in the content of new registration mentioned above, register the management information of CSV format from the **Sections - Upload** window.

   After the section has been deleted, the user of "Section Management Account" that belongs to the deleted section will become "User Account".

Procedure of modifying section code

It describes how to modify the section code.

The procedure is as follows.

1. Download the CSV file of section management information. refer to the procedure of "Modify a registration" of "2.1.4.3 Register through Uploading".
2. In the CSV file downloaded in "1.", modify the section code and other content that is required to be modified.
3. Delete the section to be modified. Refer to "2.1.4.2 Delete Section".
4. Register the CSV file edited in "2.". Refer to the procedure of "New Registration" of "2.1.4.3 Register through Uploading".

If the lower-level section exists under the section to be modified, the lower-level section also needs to be modified. If the lower-level section exists, it is unable to delete only the higher section.

2.1.5 Create User Management Information

The procedure of creating the user management Information or building management information is as follows.

1. User or building registration
2. Settings of operation authority

2.1.5.1 Register User or Building

There are five methods of registering user management information or building management information. The method to be used depends on the method of entering the information to be registered.

- Register new information by uploading a CSV file
- Update a registration by uploading a CSV file
- Register a new user from the main menu
- Change a user from the main menu
- Delete a user from the main menu

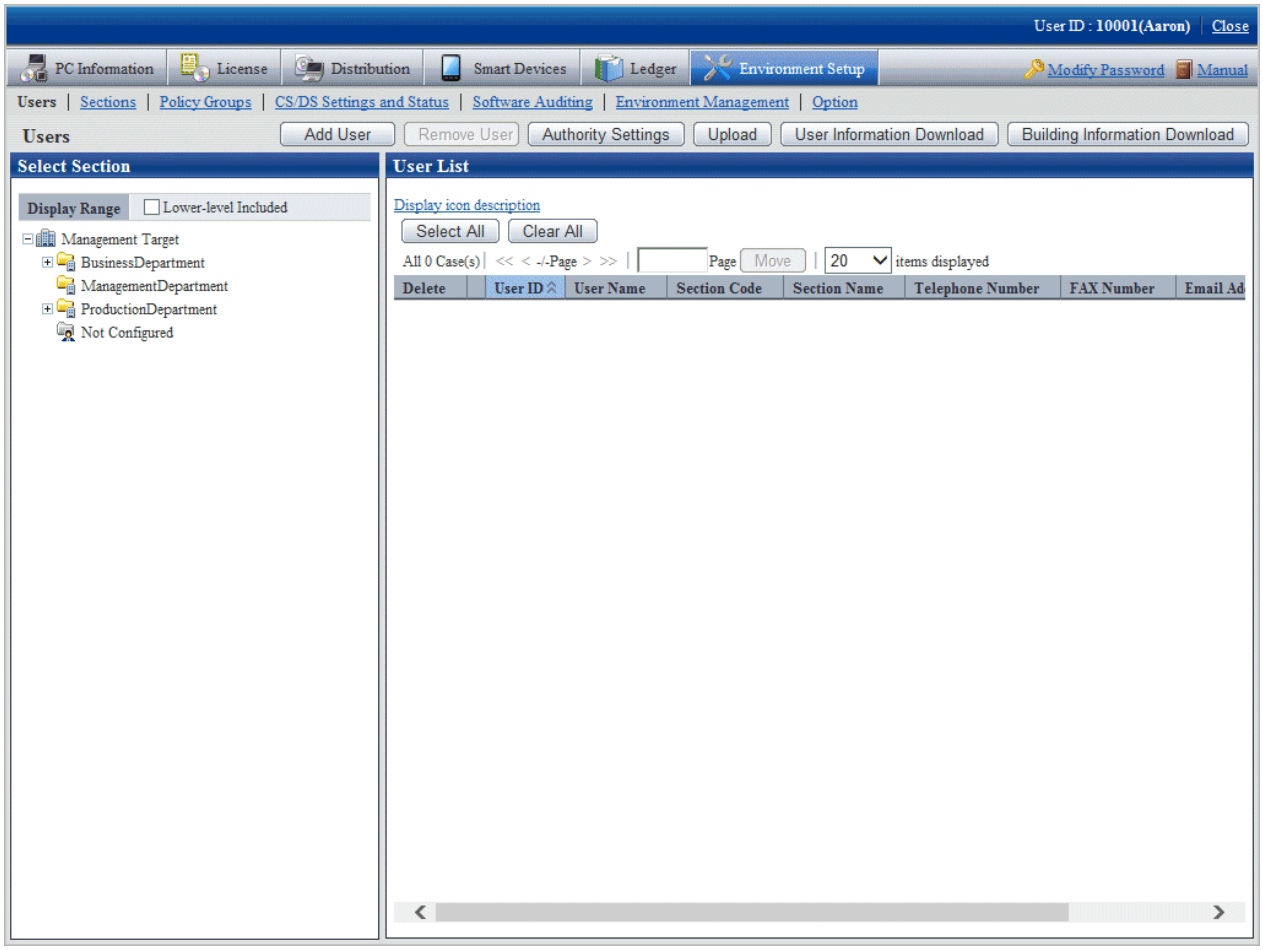
Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on the CSV file formats.

Register new information by uploading a CSV file

The method of new registration by uploading is as follows.

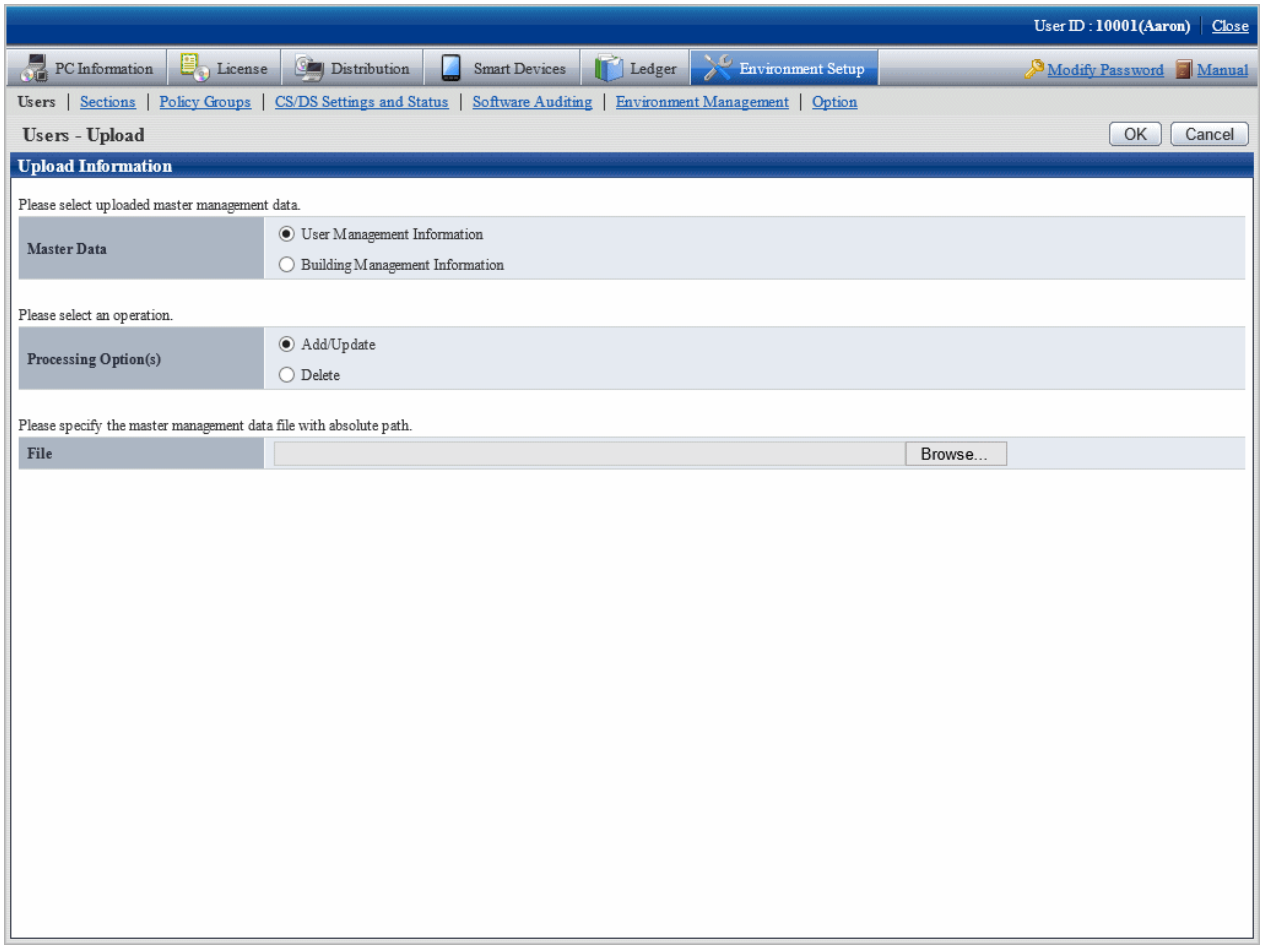
1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.



2. Click the **Upload** button.

   The following window is displayed.



3. Select the following items.

   - **Master Data**

     Select the management information to be updated.

     - **User Management Information**
     - **Building Management Information**

   - **Processing Option(s)**

     Select the operation from the following content.

Item	Meaning
Add/Update	Add/Update the data that has been registered in Master data. Register new data in which the value of **Key Item** of the data to be uploaded should not be duplicated as the value of **Key Item** of the management information that has been registered. Update the data in which the value of **Key Item** of data to be uploaded is matched with the value of **Key Item** of the management information that has been registered. * The **Key Item** is the initial item of management information created in CSV format.
Delete	Delete the data that has been registered in Master data.

Item	Meaning
	Delete the data in which the value of **Key Item** of the data to be uploaded is the same as the value of **Key Item** of the management information that has been registered, * The **Key Item** is the initial item of management information created in CSV format.

- **File**

  Select the file in CSV format.

4. After the specification has completed, click the **OK** button.

   The upload result is displayed.

   When error occurred, the list of Masters that cannot be added/updated due to inconsistence of Master management information can be downloaded.

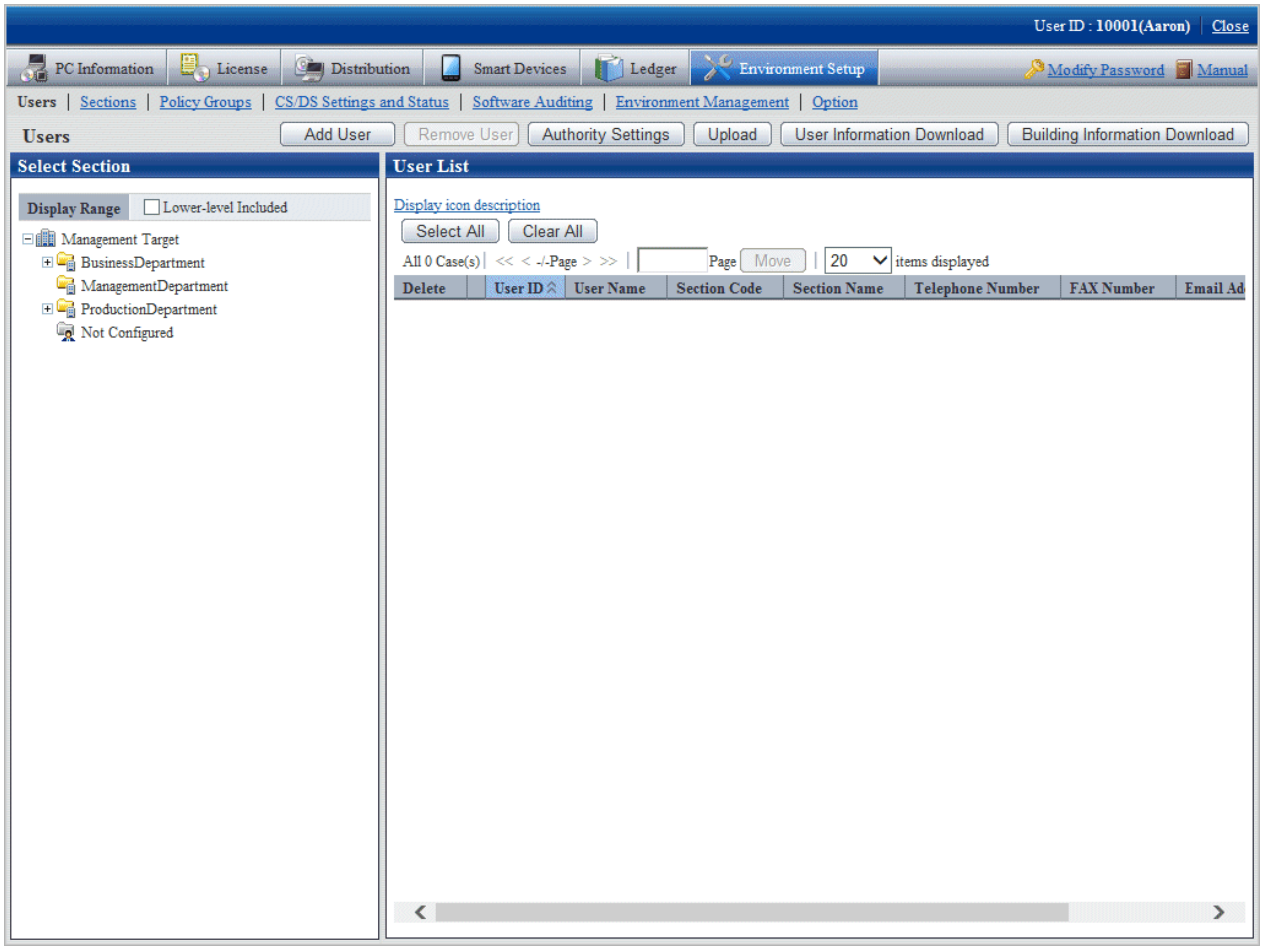
   For error content, refer to the error content of "dtpmast.exe (Master data construction)" command in *Systemwalker Desktop Patrol Reference Manual*.

Update a registration by uploading a CSV file

The method of modifying the registered Master data is as follows.

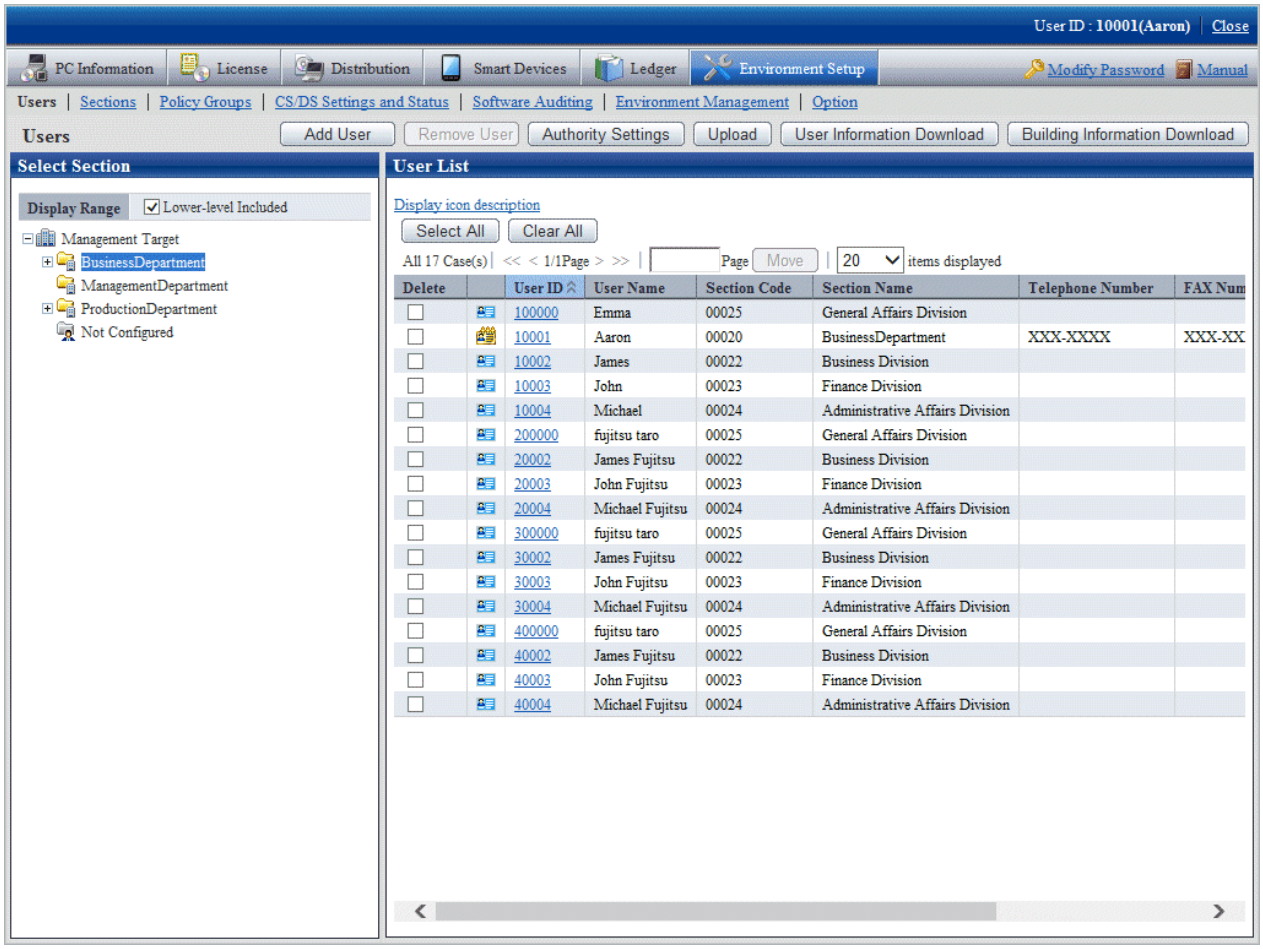
1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.



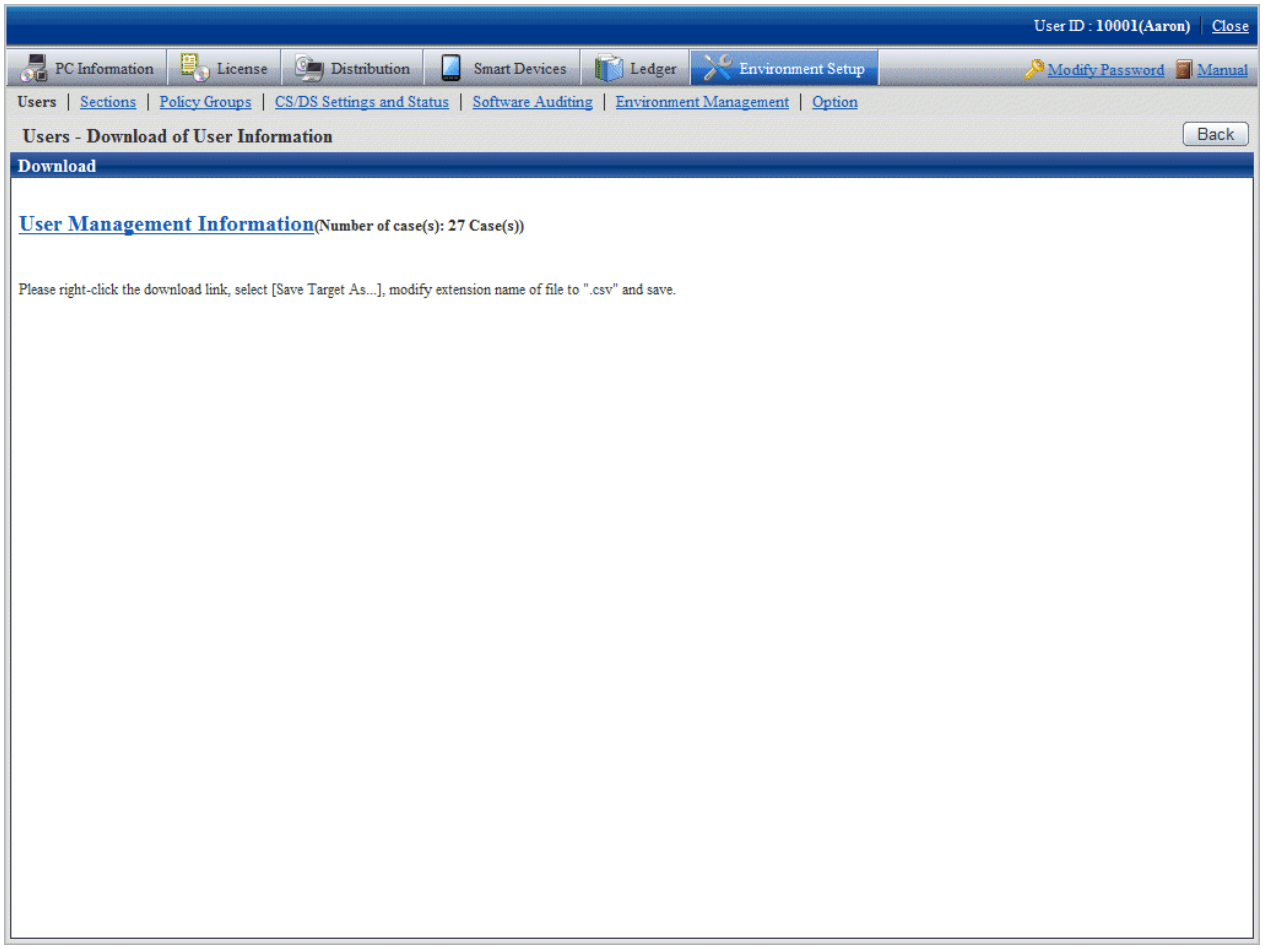
2. Select a section from the tree of the left field.

   The organizations under the selected section is displayed on the right field.

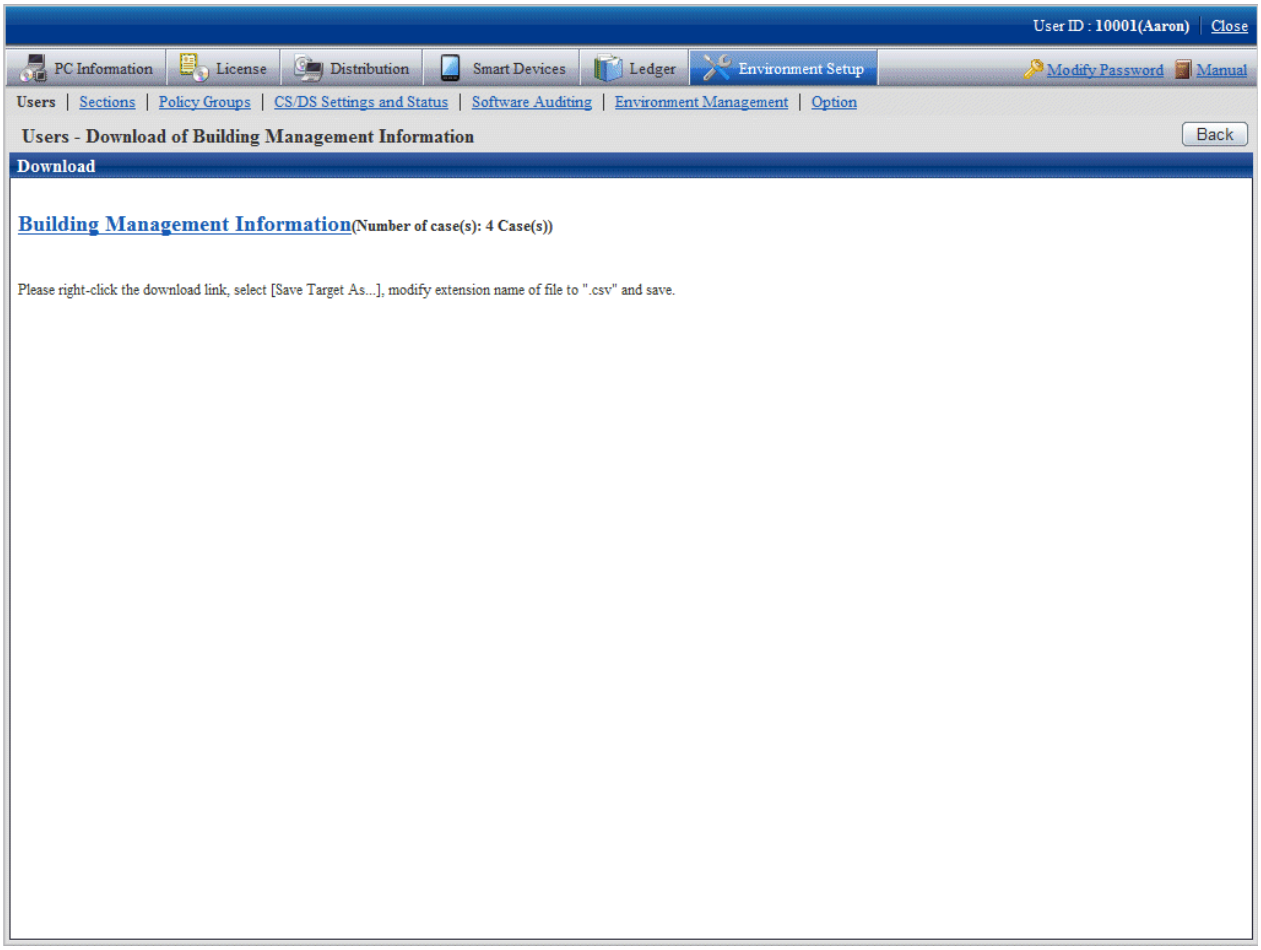


3. Click the **User Information Download** button.

   The following window is displayed.



Click the **Building Information Download** button, the following window will be displayed.



4. Right-click the download anchor and select **Save to a file** or **Save the link**. Save it by the ".csv" extension.

   In case of section management account user, the master data of the belonging section and the section under it can be downloaded. The master data containing higher and other section cannot be downloaded.

5. Edit the downloaded file and create a data file according to the purpose of addition, updating, or deletion.

Note

When modifying and saving the downloaded file with CSV format using Microsoft Excel, pay attention to the following.

- Although the double quotation marks are used for displaying values in the original file, they may disappear after modifying and saving with Excel.

  At this time, add double quotation marks using text editor, etc.

- When the front part is 0, like "000001", in the original file, after modifying and saving with Excel, the number 0 in the front part will disappear and will be replaced by "1".

  In this case, when modifying with Excel, use the user format that displays "0" at higher, or add the single quotation marks in the front of the value, and it is recognized compulsorily as a character item in Excel.

Note

When editing CSV files, edit the password information of each user, and replace the password after uploading.

When using the original password of each user, make the set password effective by omitting the password information in CSV files.

6. As in new registration mentioned above, register the management information with CSV format in the **Users - Upload** window.

   - For the user that has been registered, the code of section to which it belongs cannot be modified and user management information cannot be deleted.
   - When trying to delete the user of system account, the user will be moved to the not Configured account under the status of system account. If you really want to delete this user, execute the deletion process again after modifying the authority.
   - When deleting building management information, since "Building Code: 9990" is the code used internally in the system, it cannot be deleted.
   - After a section has been deleted, the user of "Section Management Account" that belongs to the deleted section will become "User Account".

Register a new user from the main menu

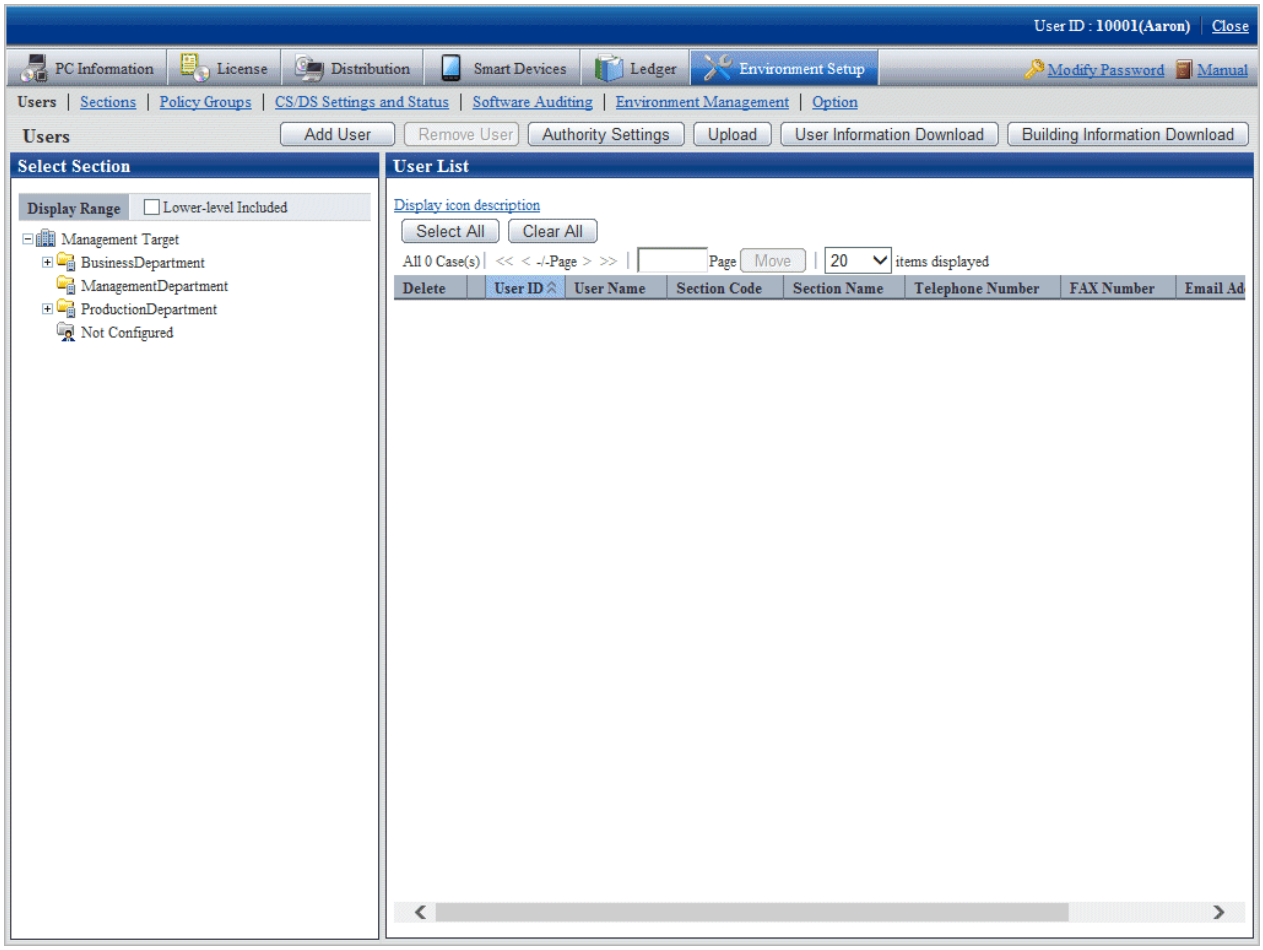
The method of new registration from the main menu is as follows.

1. Log in to the main menu and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

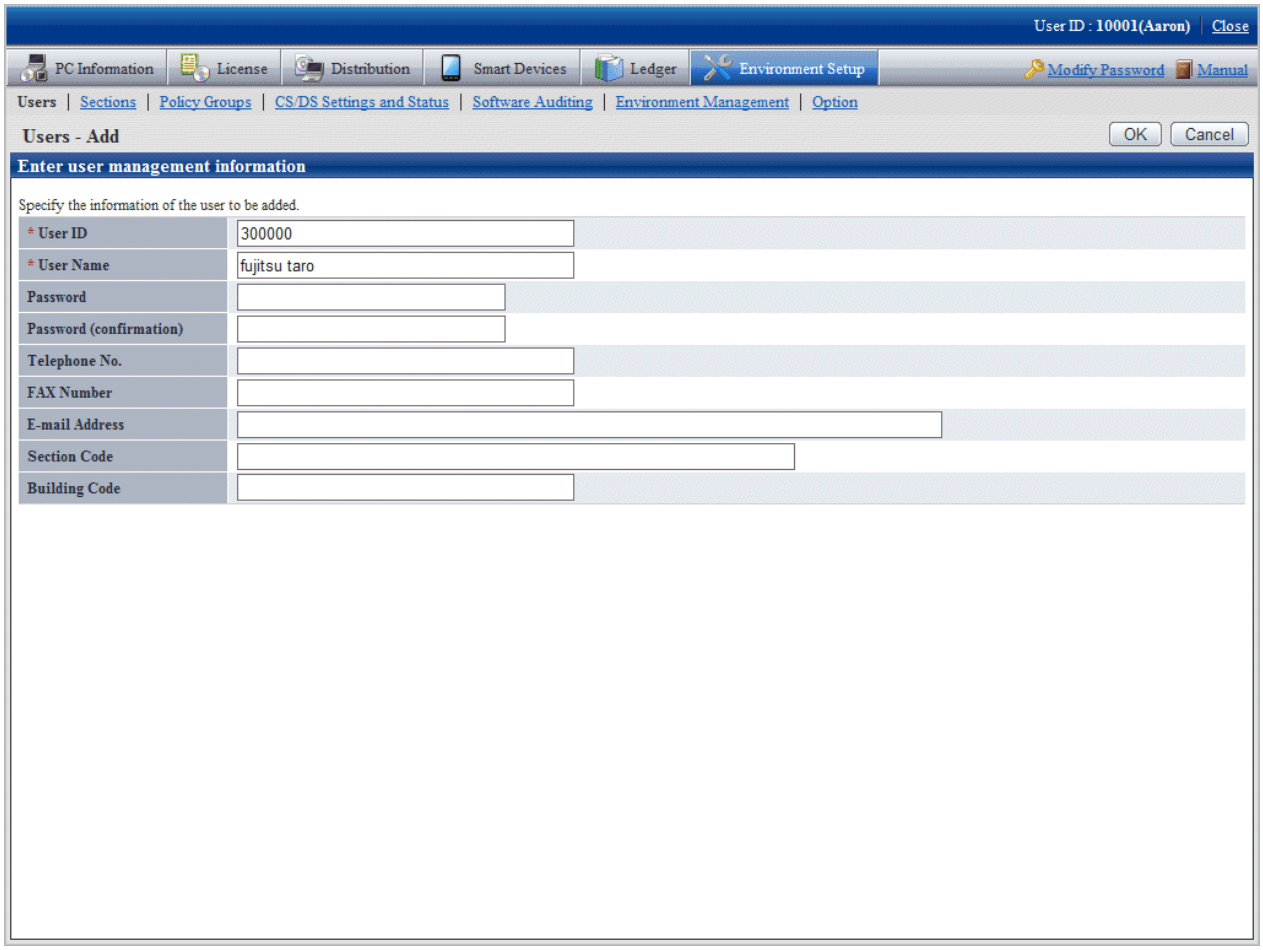
2. Click **Users**.

   The **Users** window will be displayed.



3. Click **Add User**.

   The **Users - Add** window will be displayed.



4. Set the following items:

Item	Description
User ID	Specify the ID number that identifies the user. Use up to 20 halfwidth alphanumeric characters and the following halfwidth symbols: . - @ _ Alphabetic characters are case-sensitive. This item cannot be omitted.
User Name	Specify a user name. Use up to 30 fullwidth or 60 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - @ . ( ) [ ] { } < > : ; Alphabetic characters are case-sensitive. This item cannot be omitted.
Password (*1)	Specify a password. Use from 4 to 12 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ] | < > { _ }

Item	Description
	Alphabetic characters are case-sensitive.
Password (confirmation)	Reenter the password you specified for **Password**.
Telephone number	Specify a telephone number. Use up to 20 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: * + , - . / # ( ) _ Alphabetic characters are case-sensitive.
FAX Number	Specify a fax number. Use up to 20 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: * + , - . / # ( ) _ Alphabetic characters are case-sensitive.
Email Address	Specify an email address. Use up to 50 halfwidth alphanumeric characters and the following halfwidth symbols: . - @ _ * The leading character must be a halfwidth alphanumeric character. No more than one "at" sign (@) can be used.
Section Code	Specify the section code of the section to which the user belongs. Use up to 36 halfwidth alphanumeric characters and the halfwidth symbol "-". If the section code contains alphabetic characters, use uppercase characters. A code specified in lowercase alphabetic characters will be registered in uppercase characters.
Building Code	Specify the code indicating the workplace to which the user belongs. Use up to 4 halfwidth numeric digits.

*1: A password is required for logging in to the main menu.

5. Click **OK**.

   The user will be added and the display returns to the **Users** window.

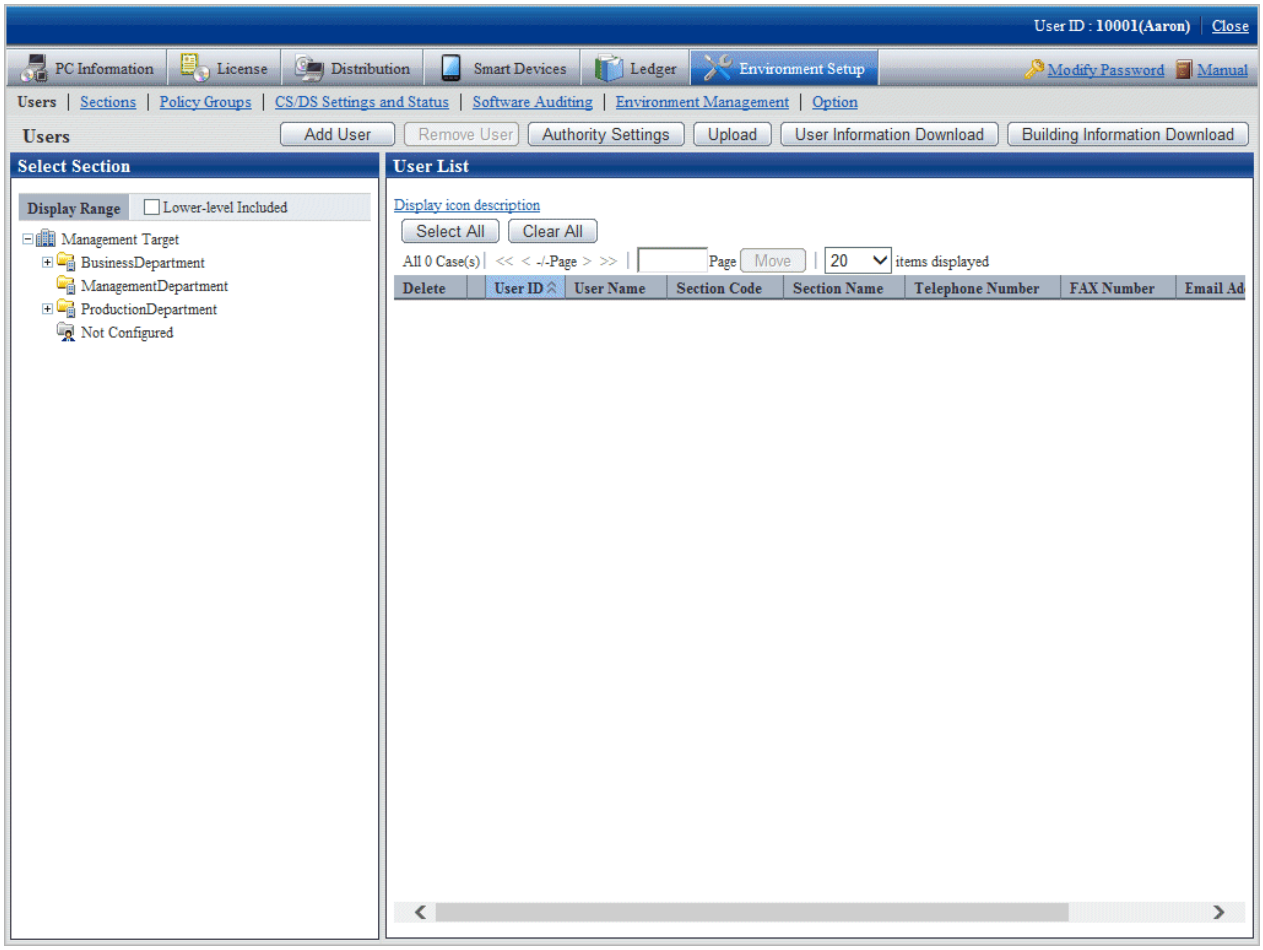
Change a user from the main menu

1. Log in to the main menu and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

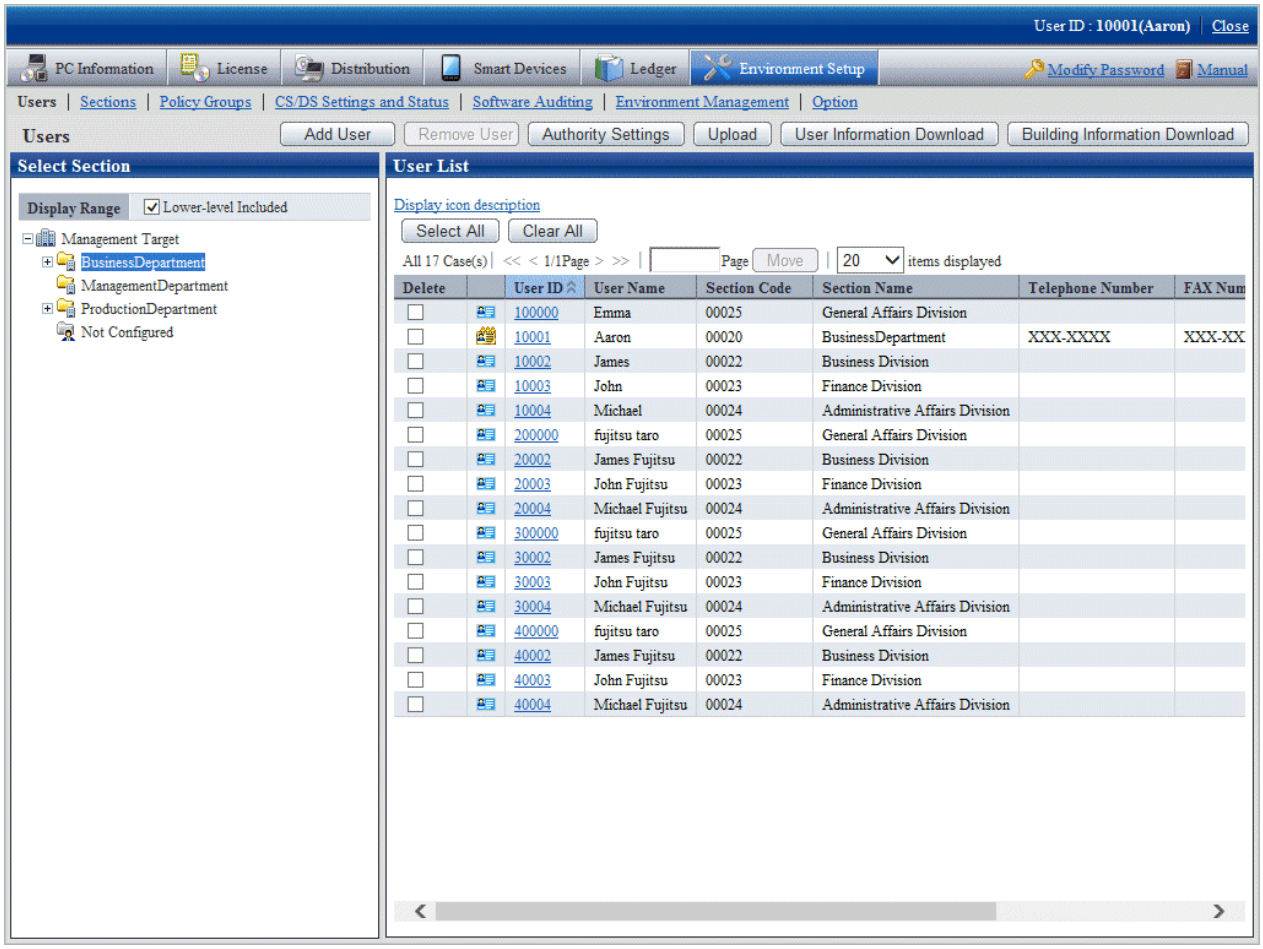
2. Click **Users**.

   The **User** window will be displayed.



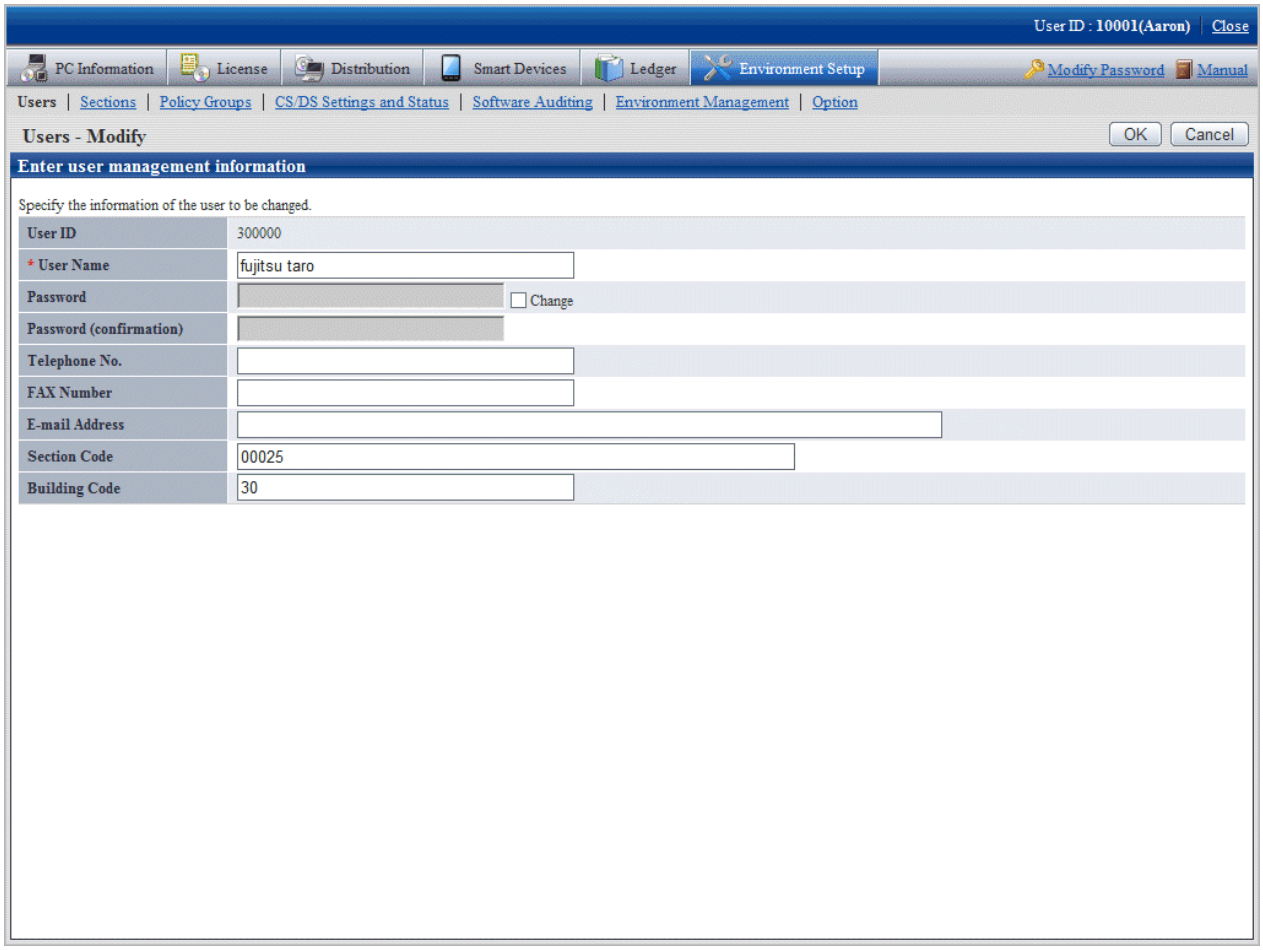
3. Select a section from the section tree in the left pane.

   The users in the selected section are displayed in the right pane.



4. Click the user ID link of the user you want to change.

   The **Users - Modify** window will be displayed.



5. Reenter the following items that you want to change.

Item	Description
User Name	Specify a user name. Use up to 30 fullwidth or 60 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - @ . ( ) [ ] { } < > : ; Alphabetic characters are case-sensitive. This item cannot be omitted.
Password (*1)	If changing the password, select **Change**. Use between 4 and 12 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ] | < > { _ } Alphabetic characters are case-sensitive.
Password (confirmation)	Reenter the password you specified for **Password**.
Telephone number	Specify a telephone number. Use up to 20 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: * + , - . / # ( ) _

Item	Description
	Alphabetic characters are case-sensitive.
FAX Number	Specify a fax number. Use up to 20 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: * + , - . / # ( ) _ Alphabetic characters are case-sensitive.
Email Address	Specify an email address. Use up to 50 halfwidth alphanumeric characters and the following halfwidth symbols: . - @ _ * The leading character must be a halfwidth alphanumeric character. No more than one "at" sign (@) can be used.
Section Code	Specify the section code of the section to which the user belongs. Use up to 36 halfwidth alphanumeric characters and the halfwidth symbol "-". If the section code consists of alphabetic characters, use upper case. A code specified in lowercase alphabetic characters will be registered in uppercase characters.
Building Code	Specify the code indicating the workplace to which the user belongs. Use up to 4 halfwidth numeric characters.

*1: A password is required for logging in to the main menu.

6. Click **OK**.

   The user information is changed and the display returns to the **Users** window.

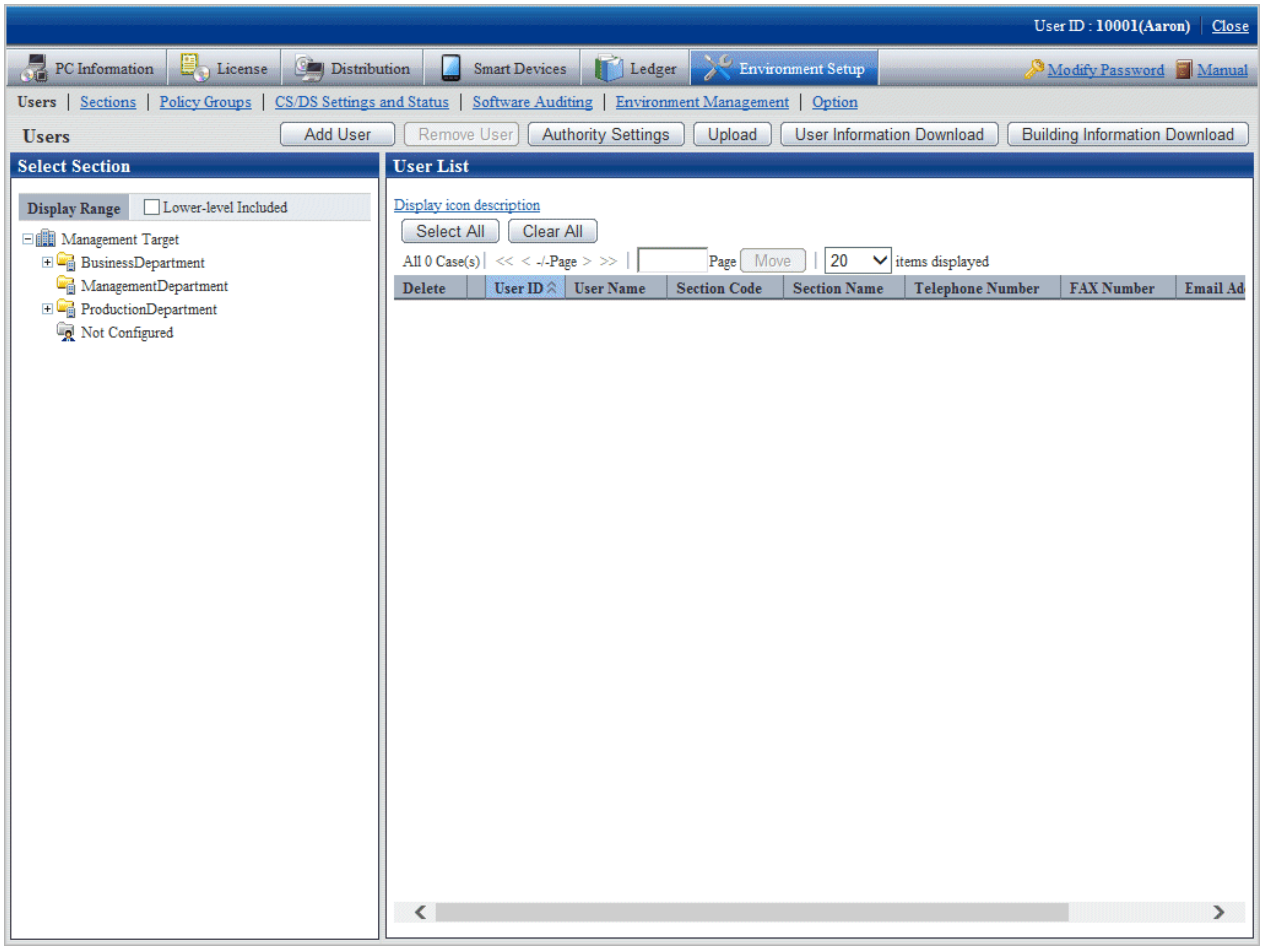
Delete a user from the main menu

1. Log in to the main menu and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

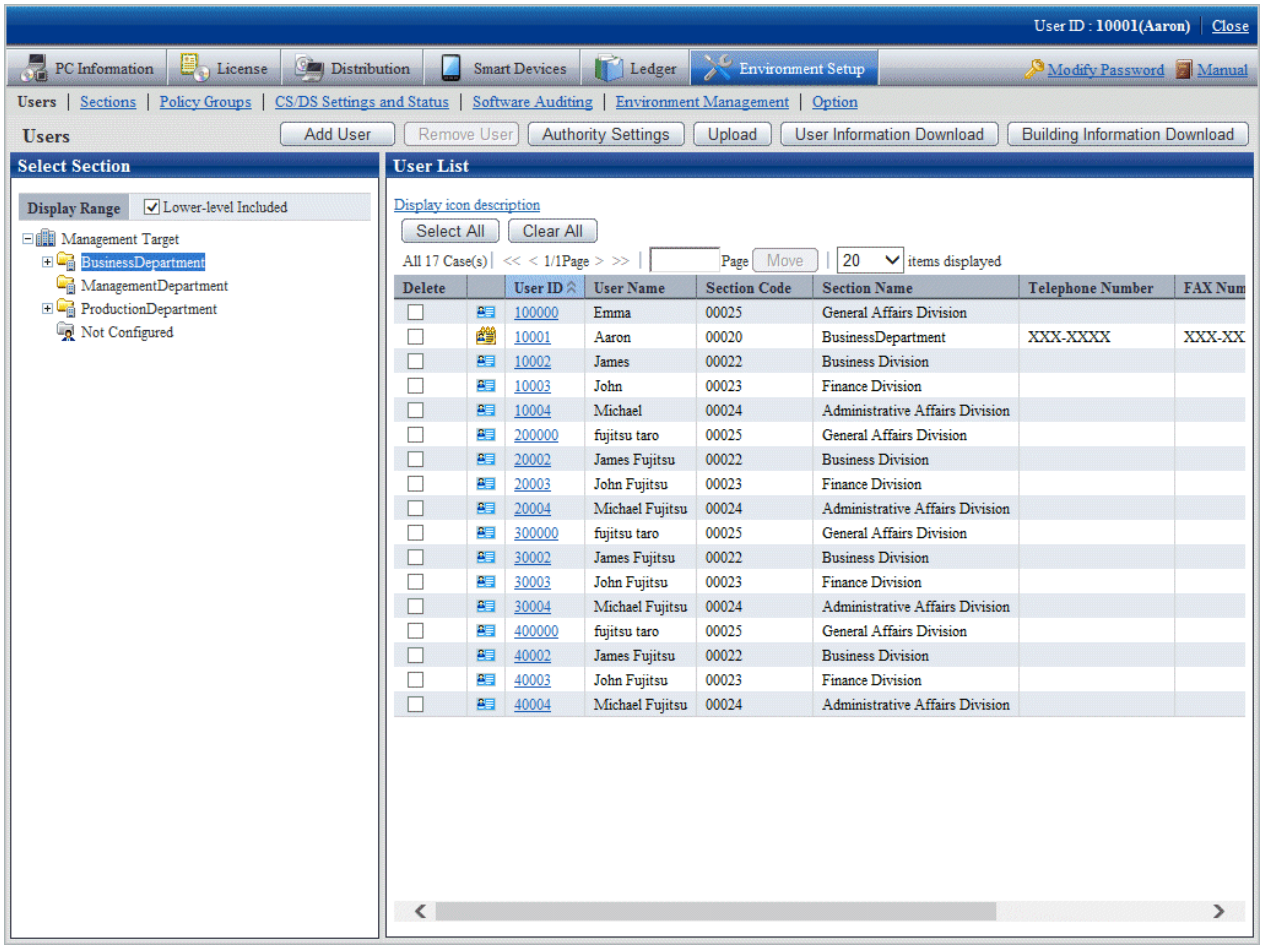
2. Click **Users**.

   The **Users** window will be displayed.



3. Select a section from the section tree in the left pane.

   The users in the selected section are displayed in the right pane.

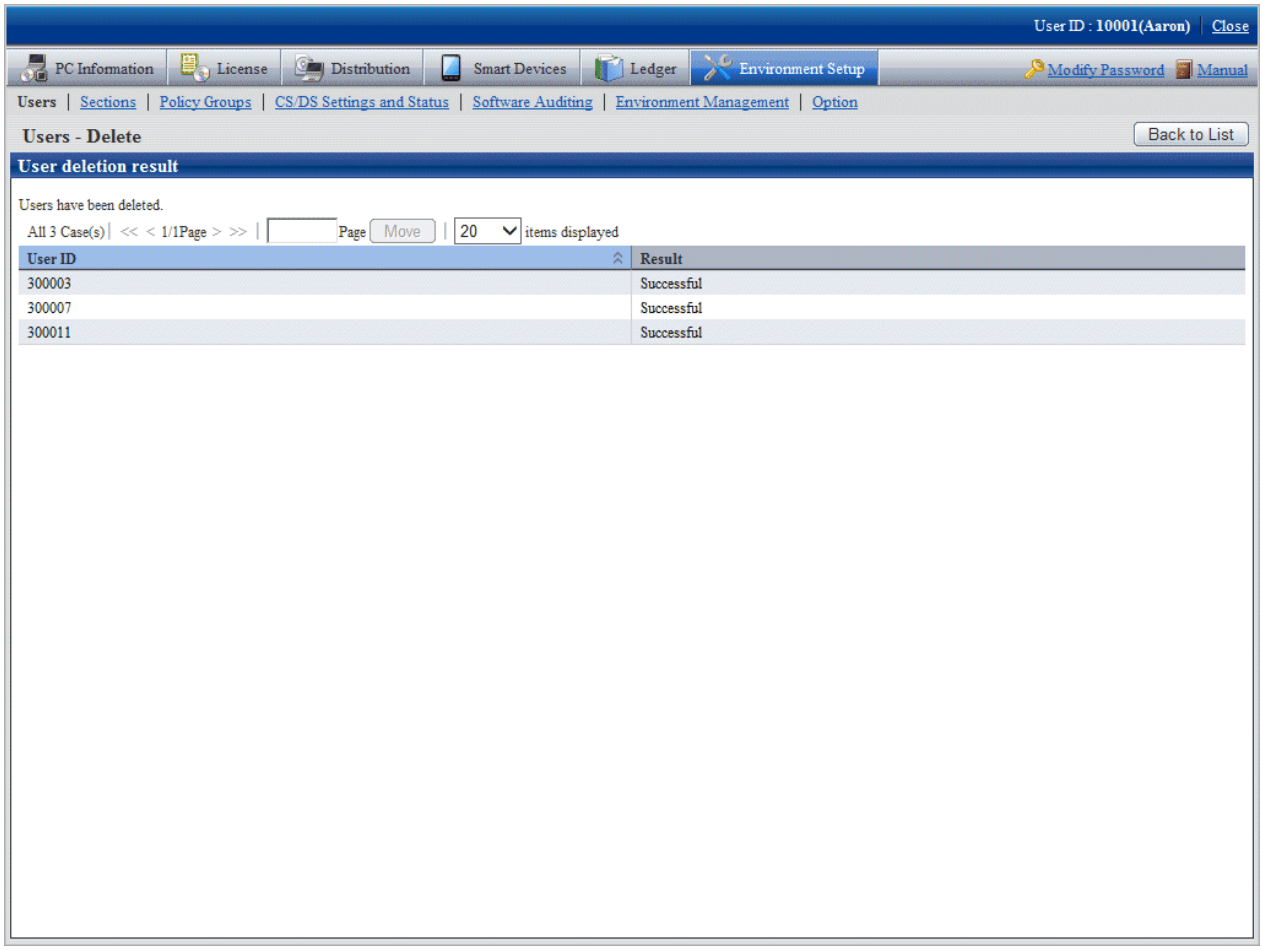


4. Select the check box next to the user you want to delete from **User List**, and click **Remove User**.

   A deletion confirmation message will be displayed.

5. Click **OK**.

   Navigate to the **Users - Delete** window. The deletion result will be displayed.



2.1.5.2 Set the Operation Authority

Operation authority is assigned to users.

Operation authority has the following three types. For details, refer to "1.1 Operation Authority".

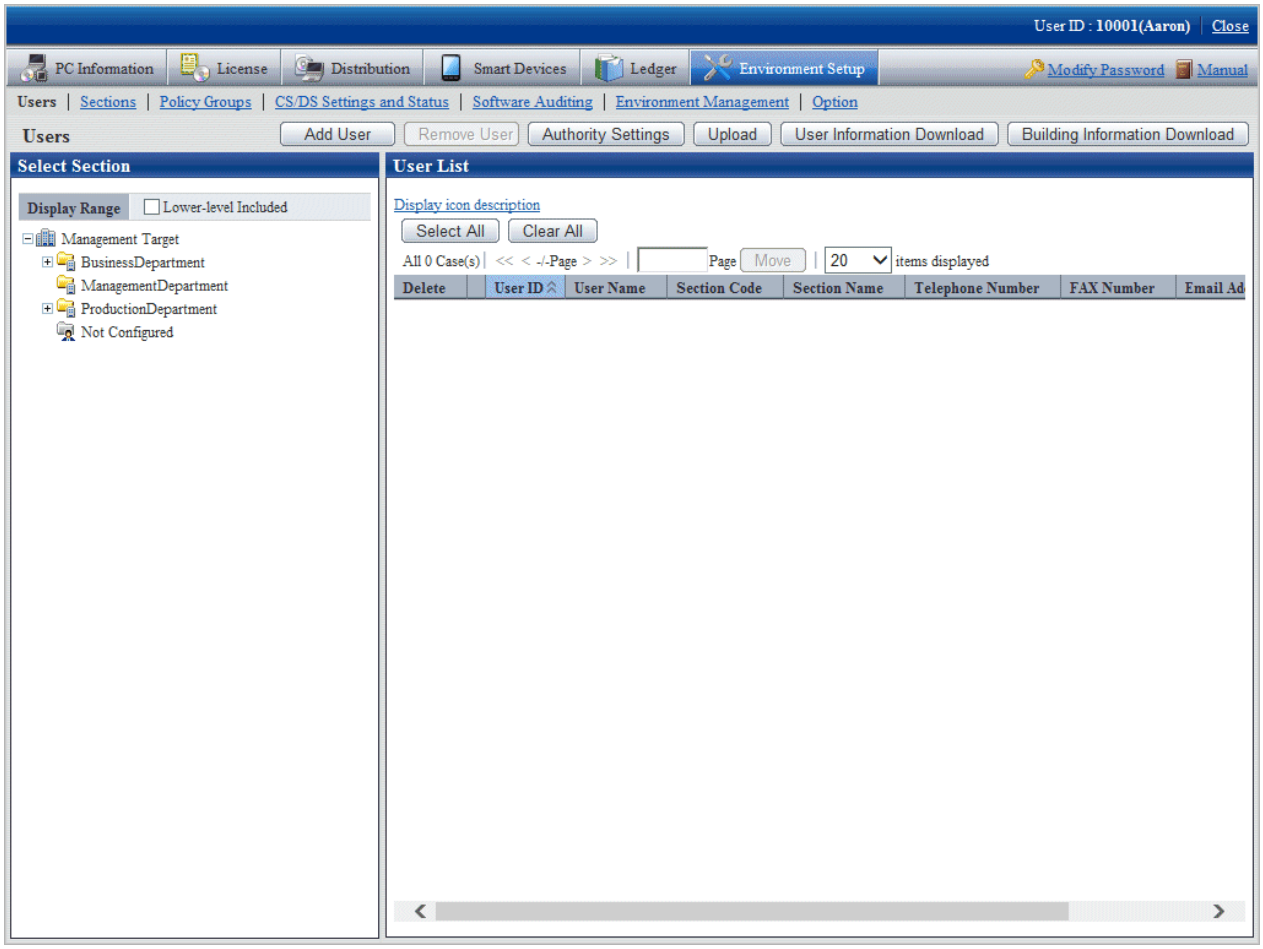
- System account
- Section management account
- User account

In addition, authority setting of system account can only be performed when login with system account.

The procedure is as follows.

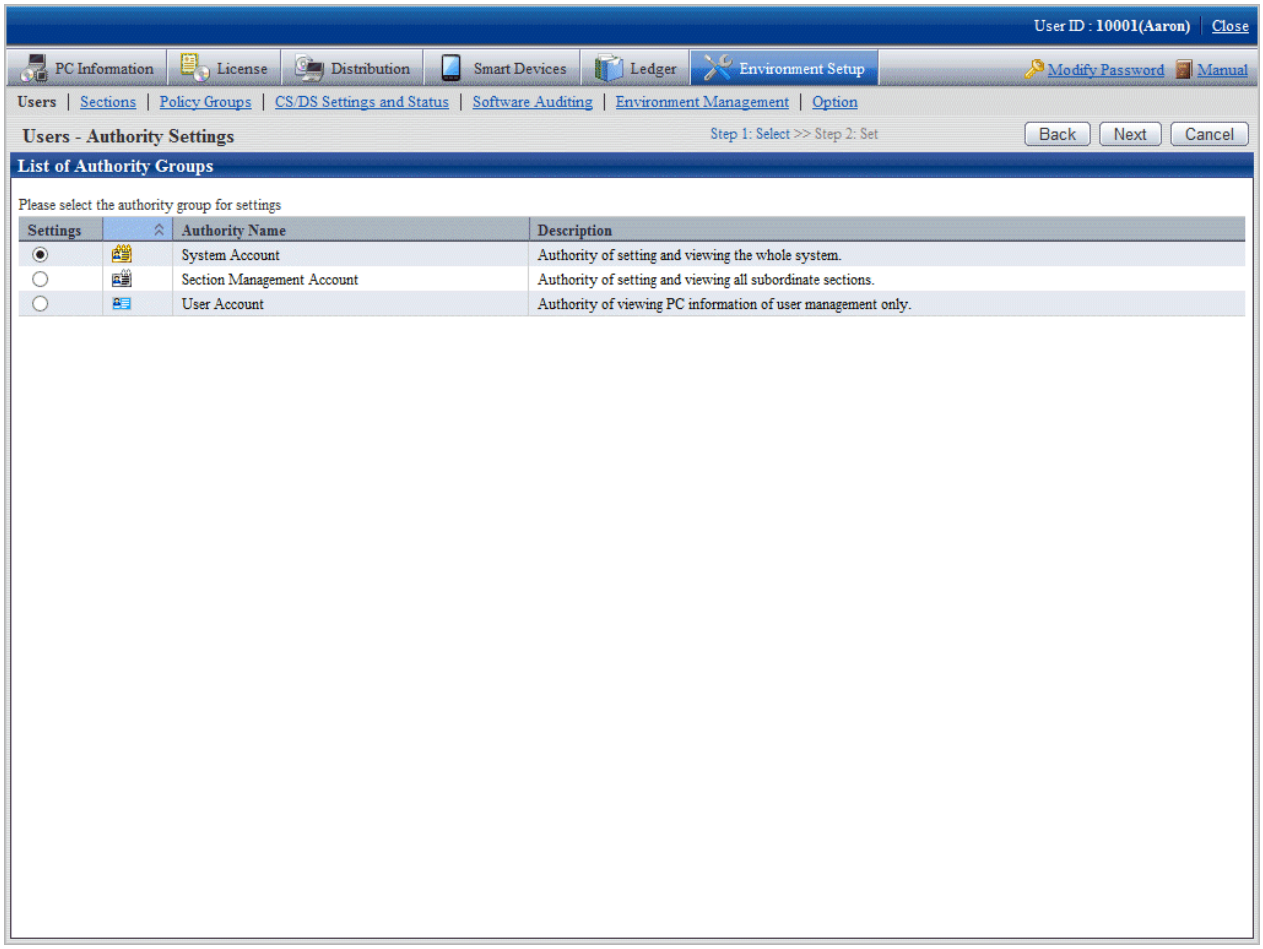
1. Login to the main menu and click **Environment Setup**.

   The following window is displayed.



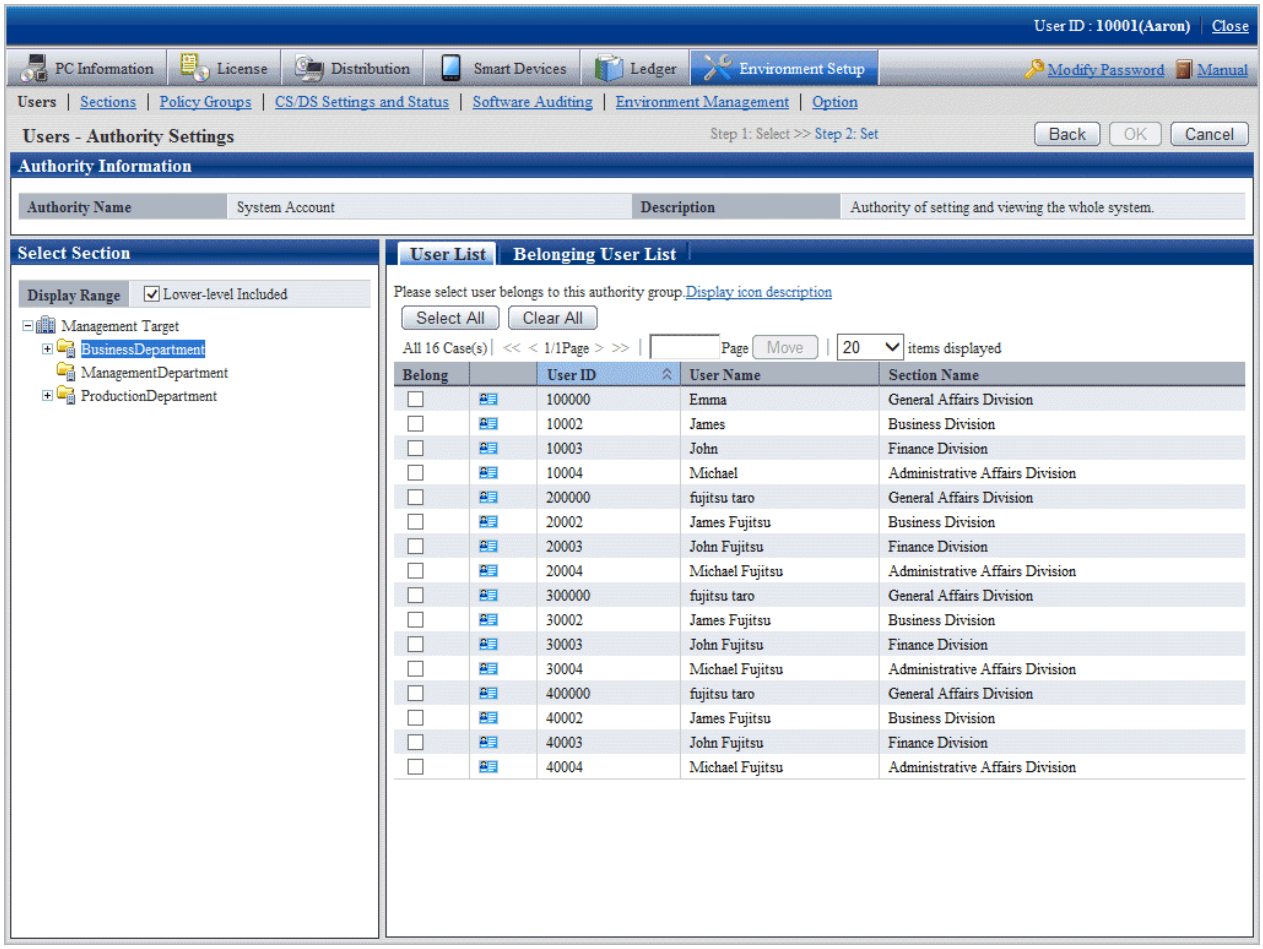
2. Click the **Authority Settings** button.

   The following window is displayed.



3. Select the authority of the setting target, and then click the **Next** button.

   The following window is displayed.



4. Select a section in the tree view of the left field.

   The users that belong to the selected section are displayed in the right field.

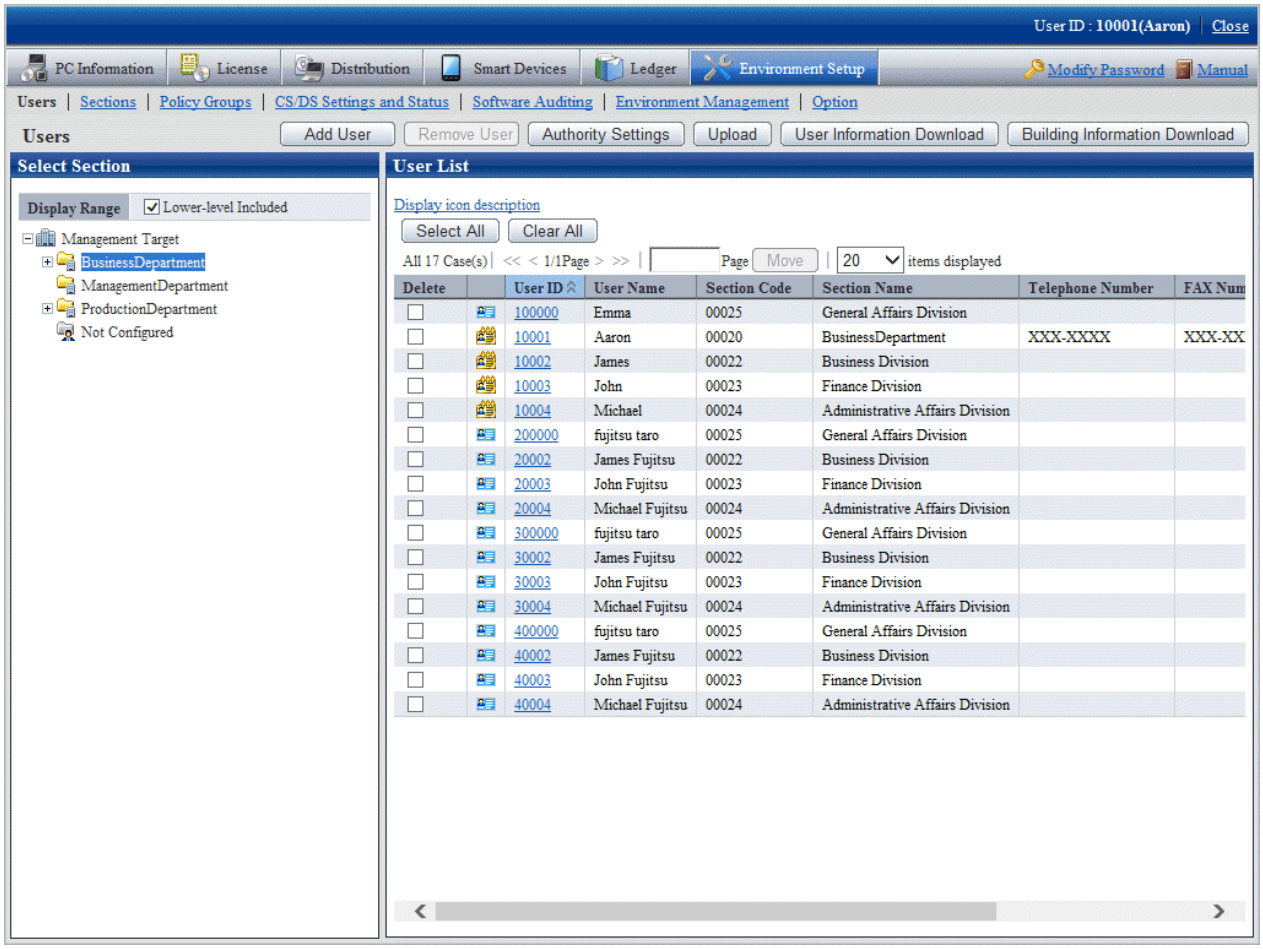
   In addition, the user without a password will not be displayed.

5. Select the user to perform authority setting, and click the **OK** button.

   The user authority will be set.

6. When confirming the users with authority set, go to step "3." again to operate, and click the **Belonging User List** tab to confirm.

   The List of Belonging Users is displayed.



2.2 Set Auditing Software

The "Support Center Definition" distributed from Systemwalker support center by E-mail and software search conditions of user itself are called "Software Dictionary".

Here describes the setting of software dictionary.

2.2.1 Select Software from Support Center Definition

The support center definition is distributed from the Systemwalker support center by E-mail. It covers typical software and is revised at any time. The support center definition cannot be modified for users.

Before starting the operation, it is necessary to select auditing software from the support center definition.

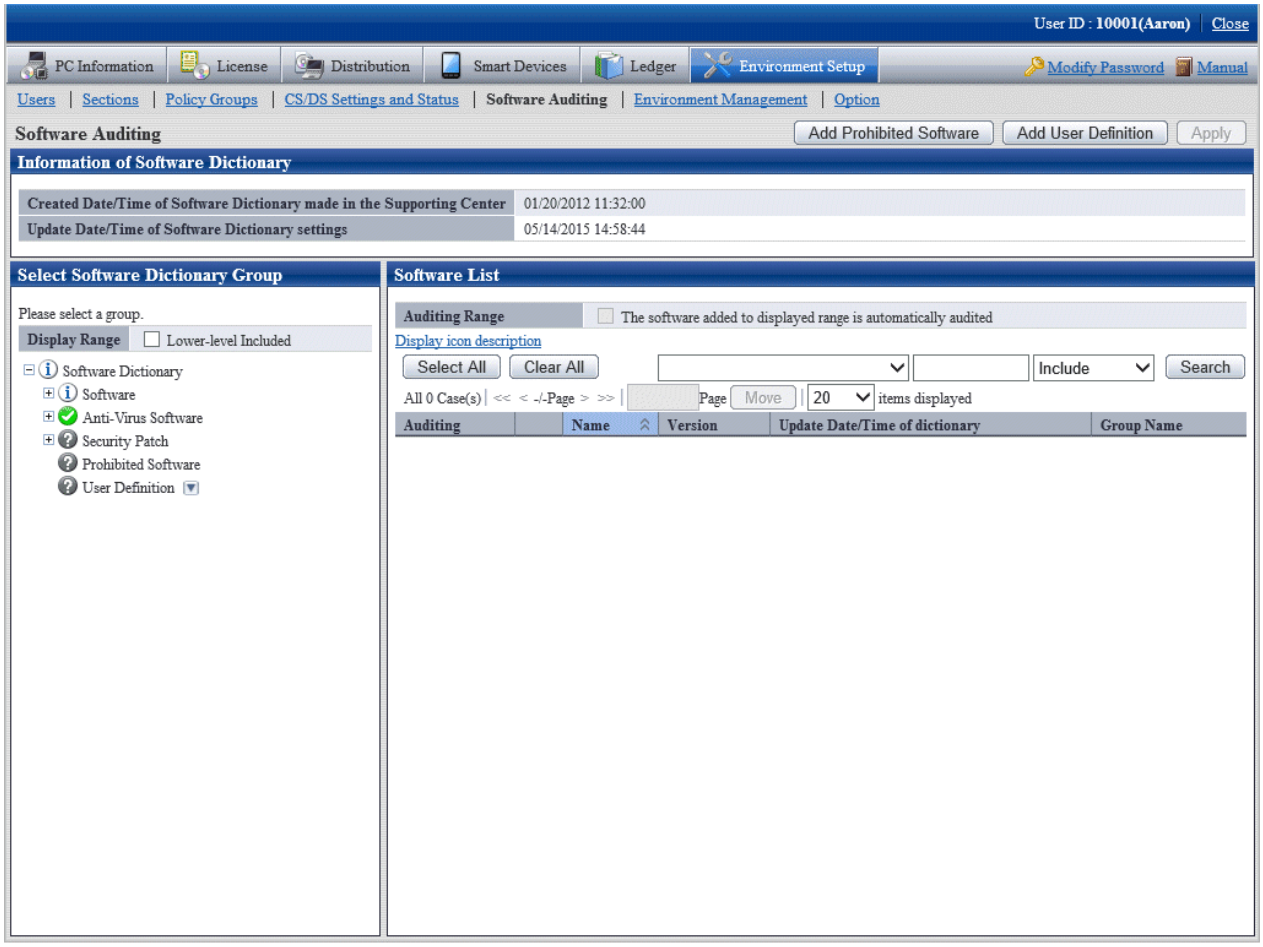
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **Software Auditing**.

   The following window is displayed.



   The meaning of icons in the **Select Software Dictionary Group** is shown as follows.

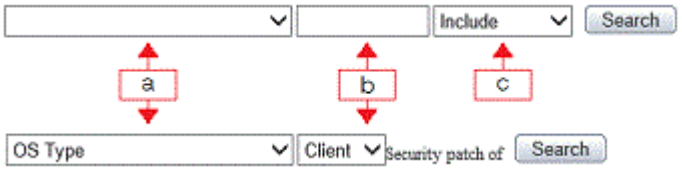
Icon	Description
	All software will be audited.
	Part of software will not be audited.
	No software will be audited.

3. Select **Software** in the tree on the left of window.

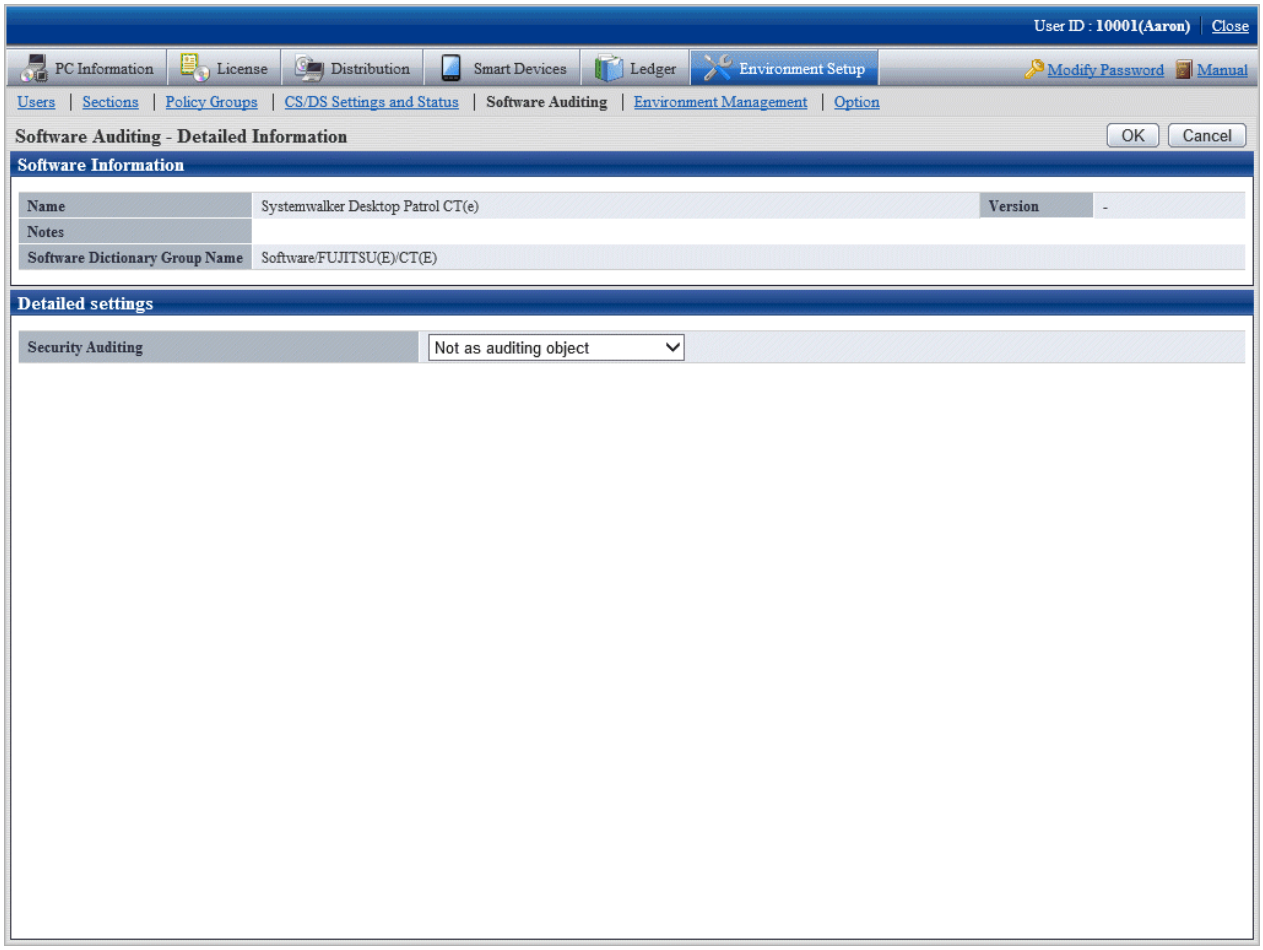
   The selected software is displayed in the right field.

Item	Description
The software added to displayed range is automatically audited	After selecting this item, even if the software is added to the group selected in **Select Software Dictionary Group** automatically in the future, it will be audited by auditing software. This check box is only effective in the following groups. - Software - Anti-Virus Software - Security Patch
Search button	Narrow down the content displayed in software list.

Item	Description

	
	Select the element to be narrowed down in "a". The item name, **OS Name**, **OS Type** can be selected. In addition, OS type can be specified in case of Security Patch.
	In "b", "c", specify the condition of elements set in "a".
	- When the items name or **OS name** in "a" is selected
	  - Specify the string to be narrowed down in "b". The string can be specified according to partial match.
	  In addition, when "a" is **OS name**, specify the string without "Windows" and Edition in "b". (Even if "Windows" and Edition are specified, they cannot be considered as the conditions for narrowing down)
	  In Windows (R) 8 only, you can filter the content by specifying "Windows 8".
	  - Select **Include** or **Not included** in "c".
	- When **OS type** is selected in "a"
	  - Select **Client** or **Server** in "b".

Click the link of software name, and details can be confirmed.



4. Refer to the following points and select the software name to be audited.

   - When it is expected to perform license management

     - Select **Software** in the tree on the left of the window, and the software to manage license can be selected in the right field of the window.

   - When it is expected to perform security audit

     - Select **Software** in the tree on the left of window, and the software to audit can be selected in the right field of the window.
     - Select **Anti-Virus Software** in the tree on the left of window, and the software to audit and virus pattern can be selected in the right field of the window.
     - Select **Security Patch** in the tree on the left of window, and the security patch to audit can be selected in the right field of the window.

   After the number of software to be audited is increased through clicking the **Select All** button, the data communication volume between CS/DS and CT will increase. Select the necessary software only.

   In addition, the software that disables the check box is the software to be distributed, so it cannot be removed from the auditing target.

5. Click the **Apply** button and save the check status.

2.2.2 Create User Definition

If the user wishes to audit the software that is not defined in support center definition, it is required to create user definition.

The following software search conditions can be defined in user definition.

- Search product information

  From **Control Panel**, click either **Add or Remove Programs** or **Programs and Features** > **Uninstall a program**, and search using a name specified in the user definition window.

- Search file

  Search by the file name, file size, file update time or version information of software.

- Search registry - Search any key and value

  Search by the specific information set in the registry.

- Combined condition

  Multiple software definition can be combined and registered as one software definition. More specific software management can be performed through the combination of software definition.

- Software operation status

  Search the operation status of "Executable file".

Do not perform circulated definition in user definition.

The procedure of creating user definition is as follows.

1. Add software dictionary group (optional)
2. Define the search condition of software
3. Put a check in the check box in front of the added user definition

Add software dictionary group (optional)

Add software dictionary group in the user definition tree.

Through adding software dictionary group, the dictionary code can be managed in groups.

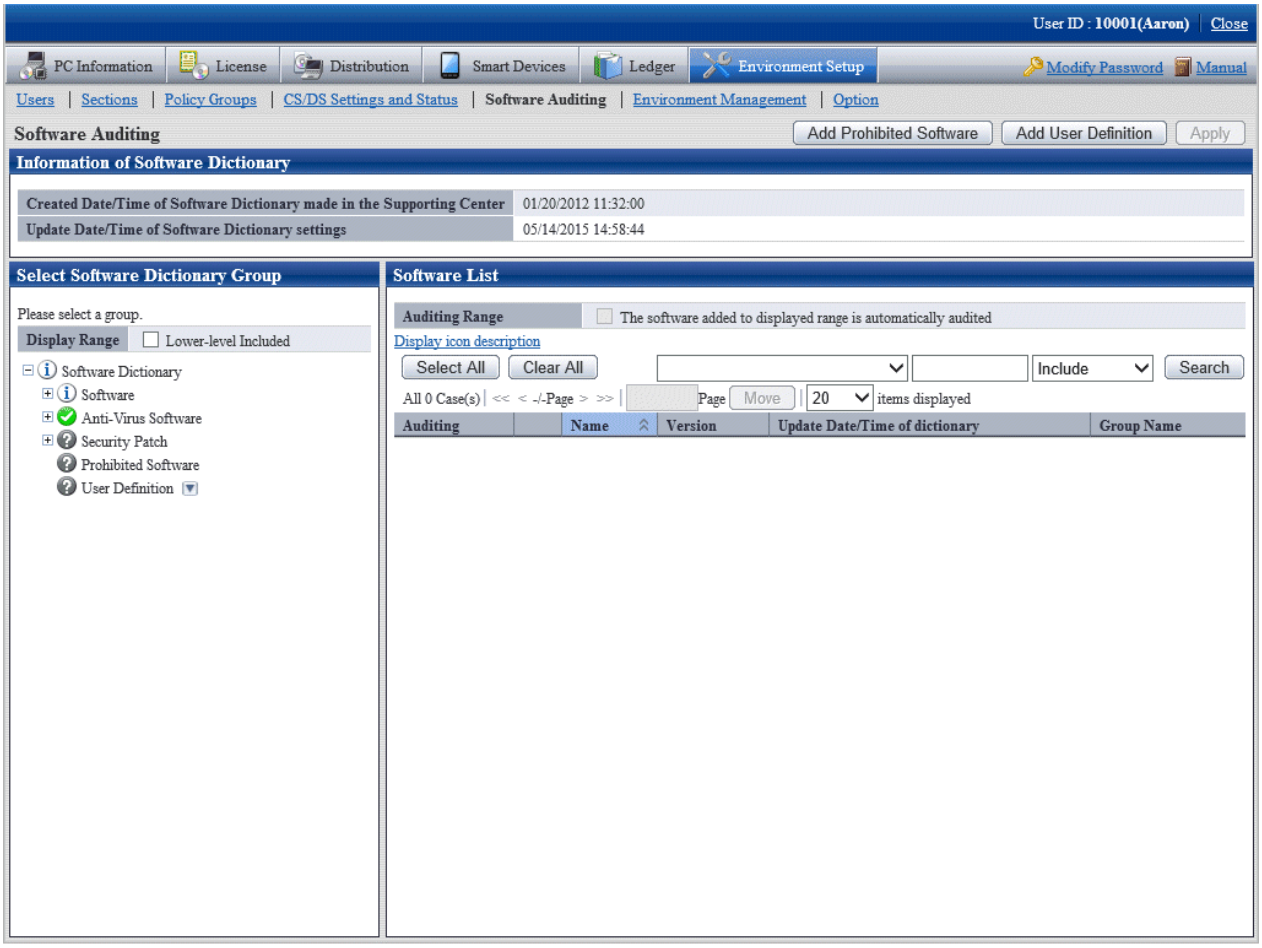
The procedure is as follows.

1. Login to the main menu and click **Environment settings**.

   The **Environment Setup** window is displayed.

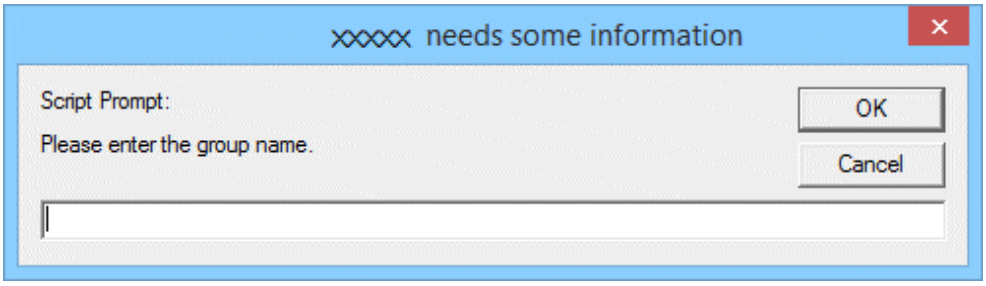
2. Click the **Software Auditing**.

   The following window is displayed.



3. Click the button on the right of **User Definition** in the tree on the left, and select **Add Group** from the menu.

   The following window is displayed.



4. Enter the group name and click the **OK** button.

   The created software dictionary group name will be added.

5. When performing operation for the added group, click the button on the right of the added group to display the menu.

   Description of the displayed menu is as follows.

Setting	Description
Add Group	Specify it to create a group in user definition. Specify a group name using up to 30 fullwidth or 60 halfwidth characters.
Delete Group	Specify it to delete the group that has been created in user definition. All of the lower-level group and user dictionary will be deleted.
Move Group	Specify it to move the group that has been created in user definition. All of the lower-level group and user dictionary will be moved.
Rename Group	Specify it to modify the group name that has been created in user definition. Specify a group name using up to 30 fullwidth or 60 halfwidth characters.

Define search condition of software

Define the search condition of software.

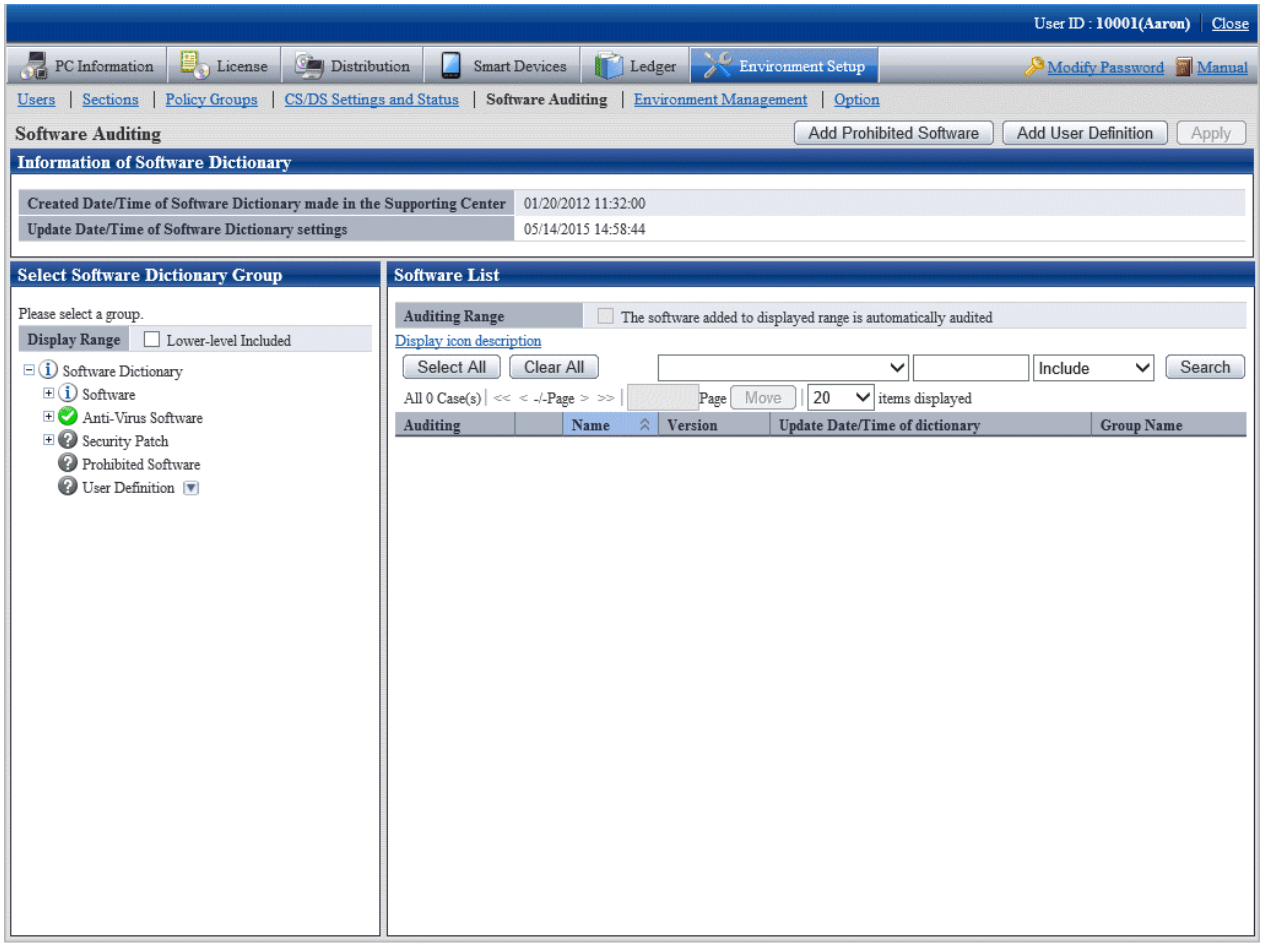
The procedure is as follows.

1. Login to the main menu and click **Environment settings**.

   The **Environment settings** window is displayed.

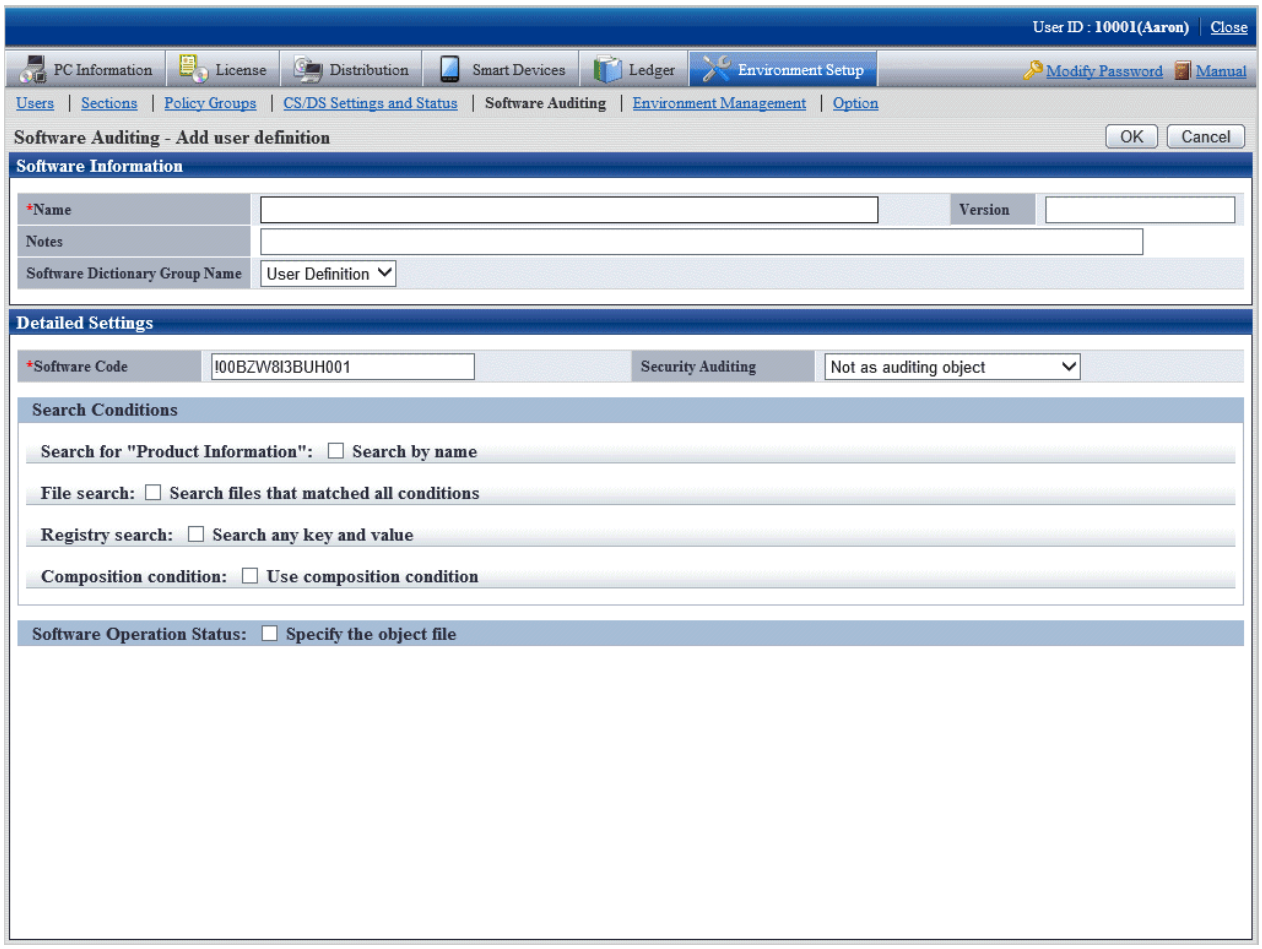
2. Click the **Software Auditing**.

   The following window is displayed.



3. Click the **Add user definition** button.

   The following window is displayed.



4. Define the following information.

Software Information

Item	Description
Name	Specify the name of software to be audited, using up to 128 fullwidth characters or 256 halfwidth characters. This item cannot be omitted.
Version	Specify the version using up to 32 fullwidth characters or 64 halfwidth characters.
Notes	Enter the remarks. Enter with 128 multi-byte characters or 256 single-byte characters.
Software Dictionary Group Name	Select the software dictionary group name to be added into user definition.

Detailed Settings

Item	Description
Software Code	It is generated automatically at new registration. To modify, specify with 15 single-byte alphanumeric characters. However, "@" cannot be specified at the beginning.
Security Auditing	Select whether to set this software to the target of security audit from the following.

Item	Description
	- **Not to be audited** (default) This software will not be the target for security audit. - **Audit as Anti-Virus software** This software will be set as the target for security audit of Anti-Virus software. - **Audit as encryption software** This software will be set as the target for security audit of encryption software.

Search Condition

Specify the search condition of this software.

As the search condition, it involves search from product information, search according to files, search from registry, combined search condition of defined auditing software.

When a certain condition is satisfied, this software will be detected.

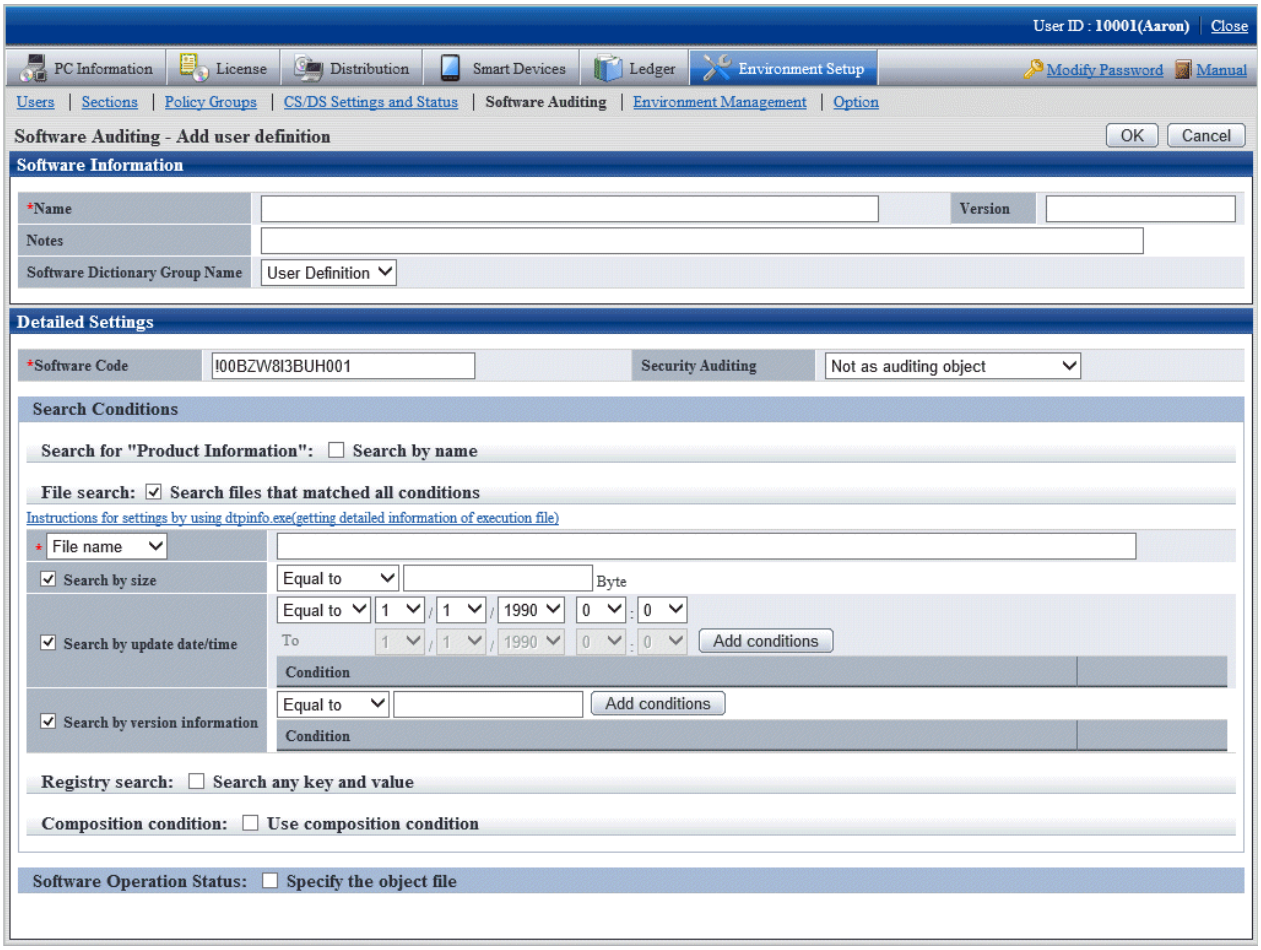
- Search for **Product Information**

  After **Search by name** is selected, search will be performed in product information according to the name specified in Name.

- File search

  After **Search files that matched all conditions** is selected, setting of file search can be performed.

Each item of file search condition not only can be set manually, but also can be set automatically through command. For details on the command, refer to "dtpfinfo.exe (obtain details of executable file)" of *Systemwalker Desktop Patrol Reference Manual*.



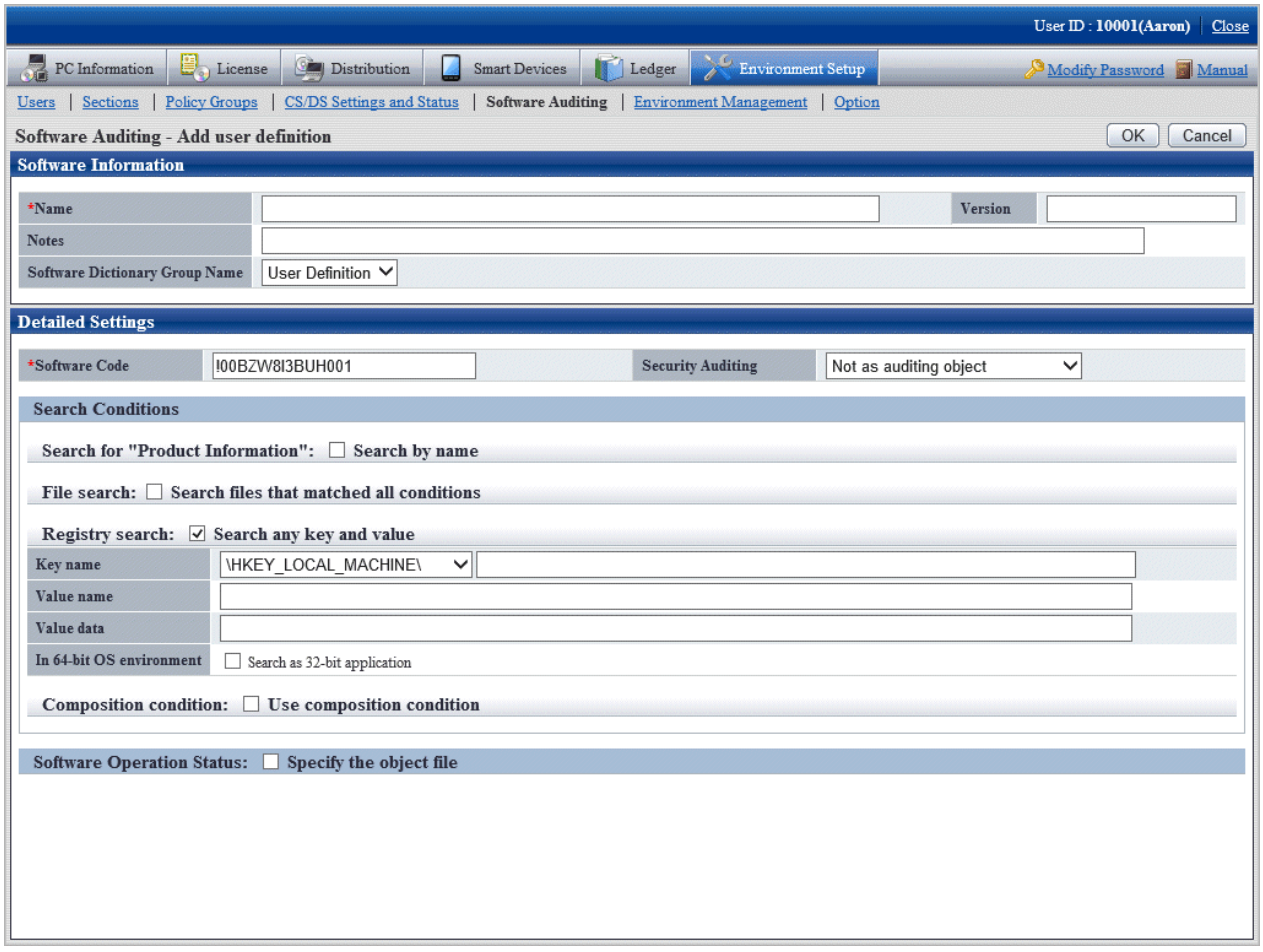
Specify the search condition of file.

Item	Description
File name/Folder name	Select **File name** or **Folder name** from the list and specify the name to be searched using up to 129 fullwidth characters or 259 halfwidth characters. This item cannot be omitted. The following characters cannot be specified. ":", "\", "*", """, "<", ">", "|", "?", "/"
Search by size	This item is effective when **File name** is specified, select it when adding the file size as search condition. When specifying the file size in **File name**, specify a number of up to 13 digits, and select one of **Equal**, **Larger than** or **Smaller than** as the comparison condition of file size.
Search by update date/ time	Select it when adding file update time as the search condition. Specify the update time of file in **File name** and select one of **Equal to**, **Above** or **Below** as the comparison condition of update time. When **From** is selected in the comparison condition, it is required to specify the end date of that period. The date that is larger than the start date of the period should be specified.

Item	Description
	When **Equal to** is selected in comparison condition, up to 10 conditions can be registered. The same date and time cannot be specified.
Search by version information	Select it when adding the version information of file as search condition. The numeric value from 0 to 2147483647 and "." can be specified. In the comparison condition of version information, select one of **Equal to** or **Larger than**. When the comparison condition is specified to **Equal to**, up to 10 conditions can be registered. The same version cannot be specified. In the properties of search file displayed in Windows Explorer, the version information will be displayed in **File Version** in the **Version Information** tab. Set the value of version information displayed as above here.

- Registry Search

  After **Search any key and value** is selected, setting of registry search can be performed.



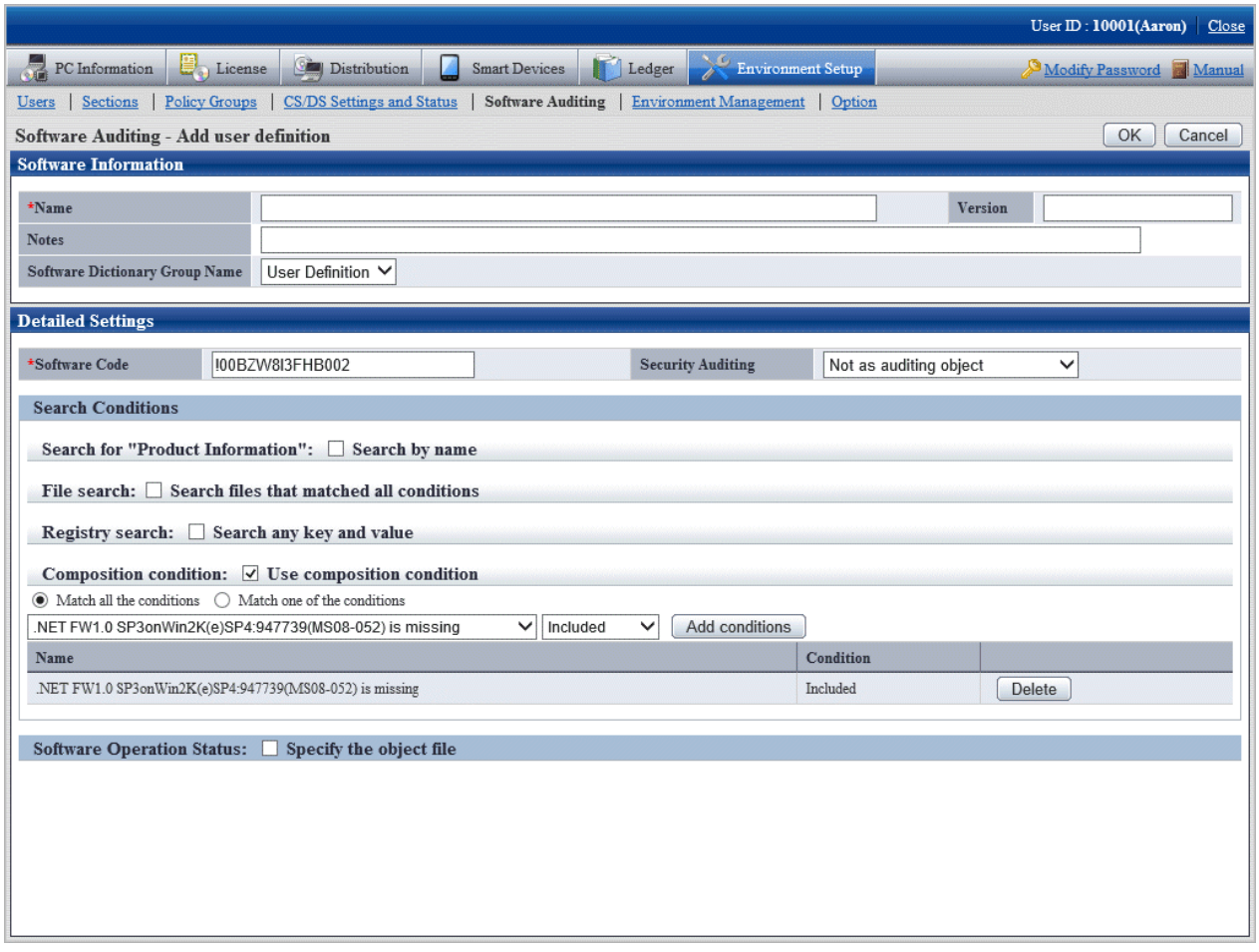
Specify the search condition of registry.

Item	Description
Key name	Specify the key name of registry using up to 116 fullwidth characters or 233 halfwidth characters. Select the beginning of key name from the list. - **\HKEY_LOCAL_MACHINE**

Item	Description
	- **\HKEY_CLASSES_ROOT** - **\HKEY_USERS**
Value name	Specify the value name of registry using up to 128 fullwidth characters or 256 halfwidth characters. When omitted, search by key name only.
Value data	Specify the data of registry value using up to 128 fullwidth characters or 256 halfwidth characters. The searchable registry value types are as follows: - **REG_DWORD** - **REG_SZ** When omitted, search by key name and the name of key value only.
In 64-bit OS environment	Specify registry search operation on the 64-bit OS. - When selected When search registry on 64-bit OS, refer to the registry under "HKEY_LOCAL_MACHINE\Software\Wow6432Node". On the 32-bit OS, refer to the specified registry. - When not selected Refer to specified registry for both 32-bit OS and 64-bit OS.

- Composition condition

  Select **Use composition condition**, combined condition can be set.

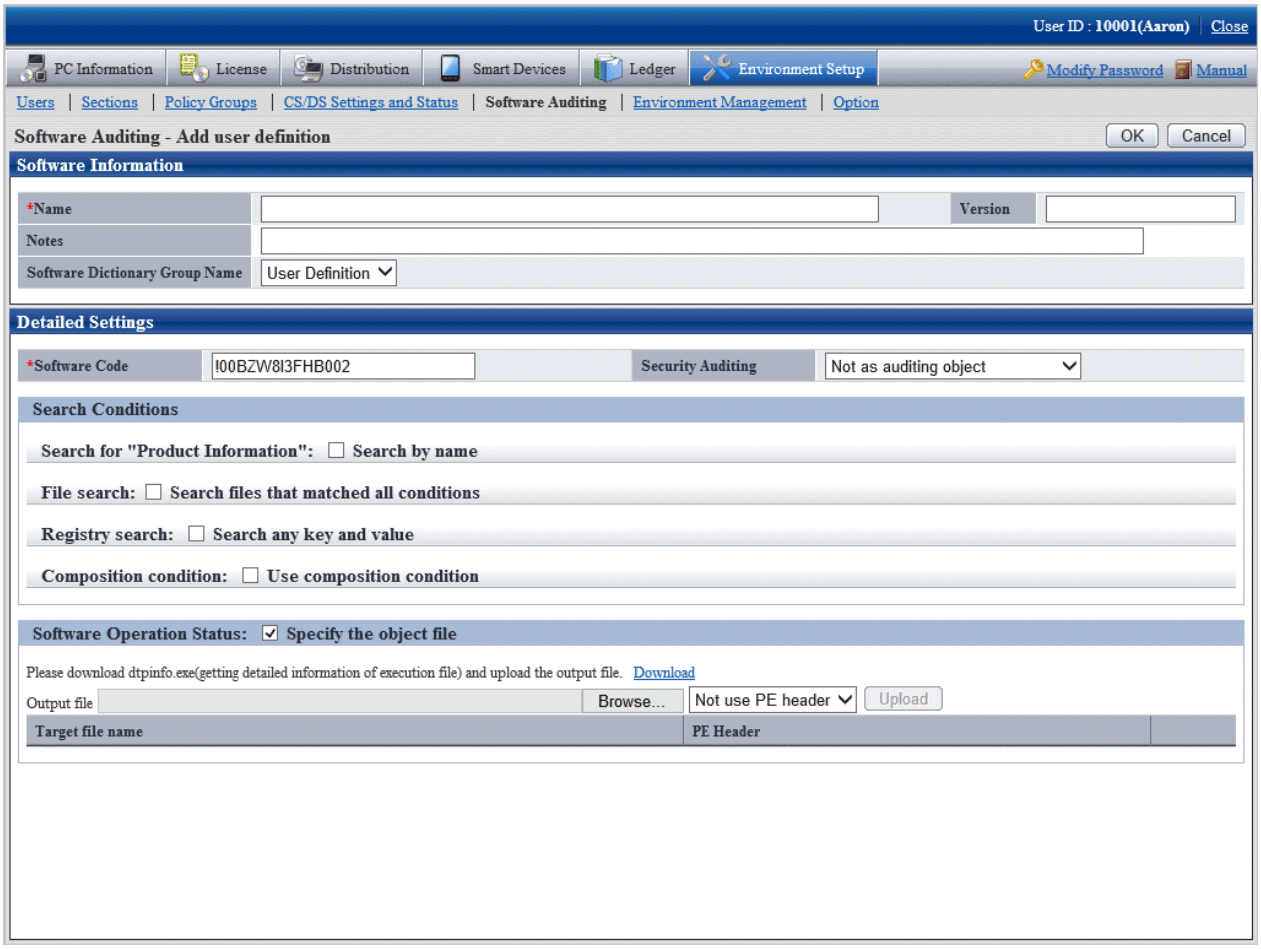


Select the software to be combined from the list, and specify **Include** or **Not Include** for the selected software to determine combined condition. Up to 10 combined conditions can be specified.

Item	Description
Adding conditions button	Add one line of field that can select software.
Delete button	Delete the software where the line of delete button is located from the combined condition.

Software Operation Status

Select **Specify the object file**, the setting of software operation status can be performed.



Register the result file of command output to server and software can be registered.

For details on the command, refer to "dtpfinfo.exe (Obtain details of executable file)" of *Systemwalker Desktop Patrol Reference Manual*.

Item	Description
Upload button	Register the file specified in the output result file to server. During registration, select whether to specify PE Header for target file to register. - **Not use PE header** - **Use PE header**
Delete button	Delete the file of the line where the delete button is located from the server.

Item	Description
Target file name	The name of target file to be audited as operation status of software is displayed.
PE Header	When registering target file according to specified PE Header, it is displayed as **Registered**.

In addition, the operation status of the following software cannot be collected.

- Software without fixed file name
- Software with extension apart from "exe"
- Resident software and software without window that is started in service of Windows, etc

5. Click the **OK** button.

Put a check in the check box in front of the added user definition

Select the added user definition.

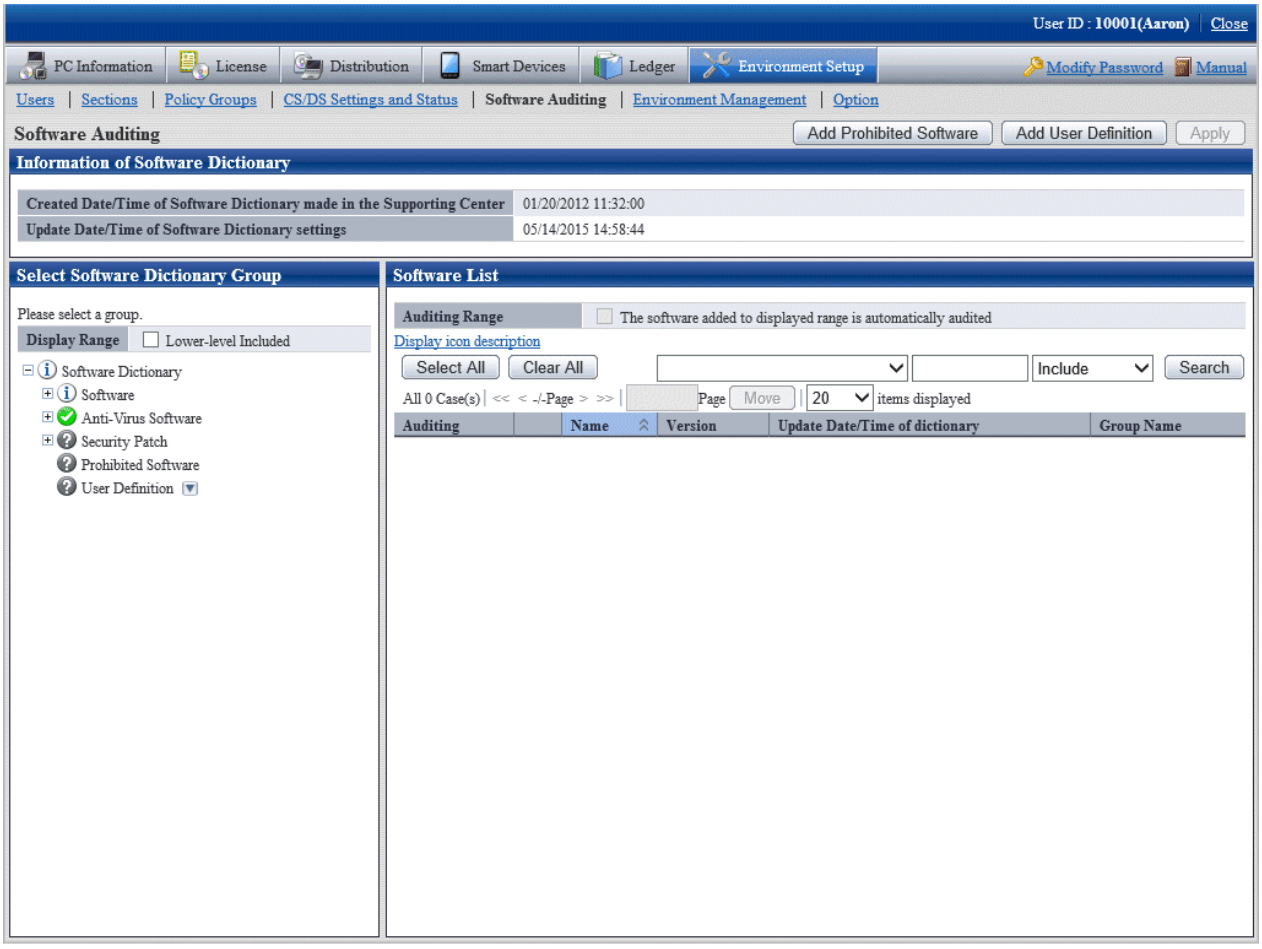
The procedure is as follows.

1. Login to the main menu and click **Environment settings**.

   The **Environment settings** window is displayed.

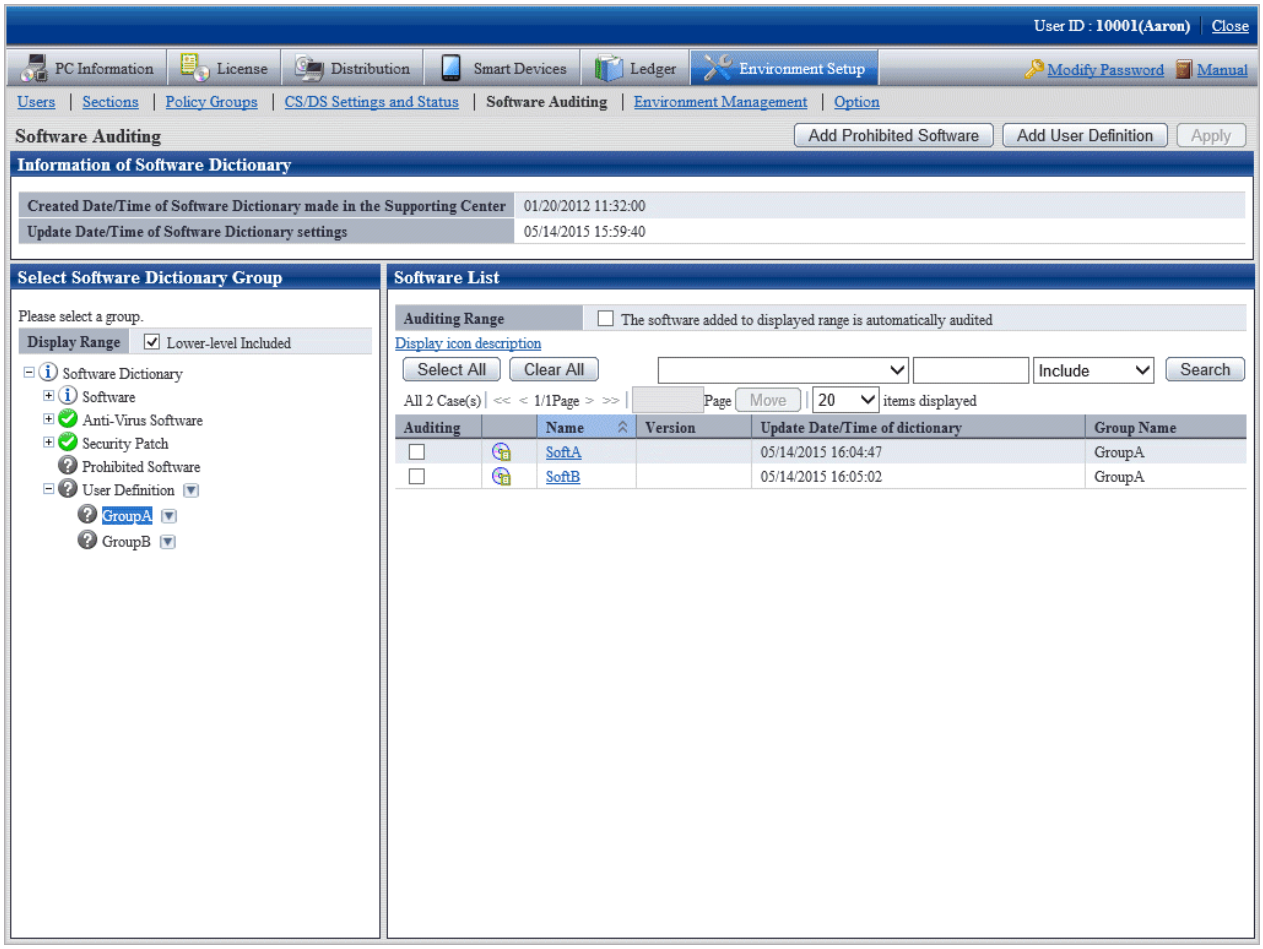
2. Click the **Software Auditing**.

   The following window is displayed.



3. In the field on the left, select **User Definition**.

   The added user definition is displayed in the field on the right.



4. Select the software name to be audited.
5. Click **Apply** button, save the selected status.

2.2.2.1 Create User Definition from Inventory Information

"User Definition of software dictionary can be created automatically from the information of "Product Information" collected as inventory information from CT.

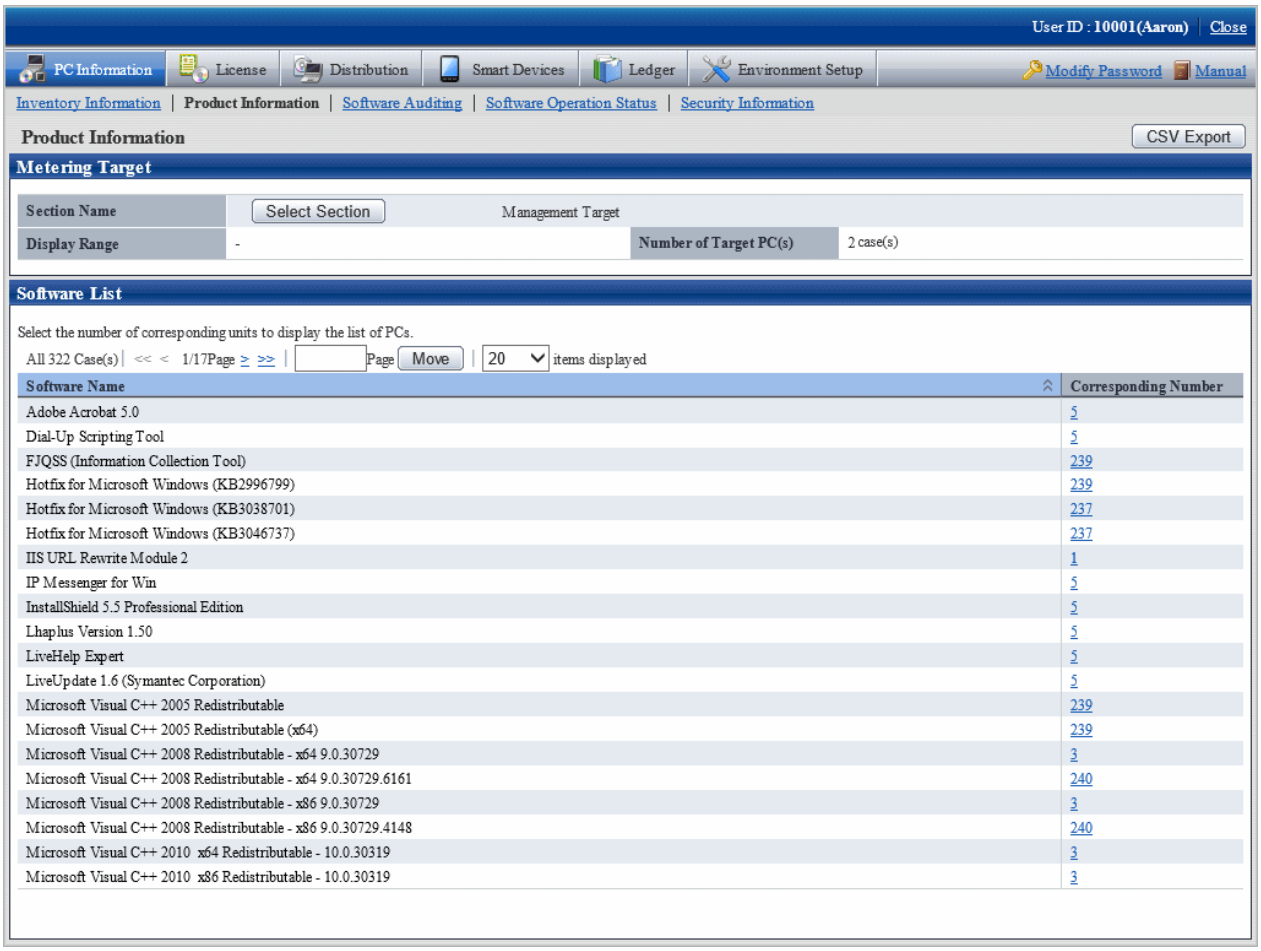
This "User Definition" is called "User Asset Software Dictionary". "The procedure of creating "User Asset Software Dictionary" is shown as follows.

1. Confirm the software product that has been installed
2. Execute the user asset software dictionary creation command
3. Set user definition of software dictionary

Confirm the software product that has been installed

Confirm the installation status of software product to be audited from the main menu.

Select **PC Information** > **Product Information** of the main menu, and refer to the list of software collected from each PC to confirm whether the software product to be audited is displayed.



If the software product needs to be audited is not installed, perform the one of following actions.

- Install this software product on the PC with CT installed, and collect inventory information.
- Install CT on the PC with this software product installed, and collect inventory information.

Execute the user asset software dictionary creation command

Execute the dtplocaldic.exe (user asset software dictionary creation) command.

For details on the dtplocaldic.exe (user asset software dictionary creation) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

It is recommended to set the following according to operation method for the timing of command execution.

- When creating software dictionary from the inventory information after refining by user ID or PC name

  Create the model PC of license management, and execute this command when the **Product Information** installed to the specified user ID or PC name is modified.

- When creating software dictionary from the inventory information of all PCs

  Since it is possible to install new software, it is required to register command to the task of Windows and execute the command regularly.

Point

The so-called license management model PC

It indicates that the software product that requires license management has been installed.

Install the software product that requires license management to the specified PC again to collect inventory information. Specify this PC name to execute the user asset software dictionary command and the information volume of user information that requires license management can be reduced.

Set the user definition of software dictionary

Through executing the user asset software dictionary command, the software product displayed in **Product Information** will be added to the user definition of software dictionary.

The administrator selects the software added to user definition.

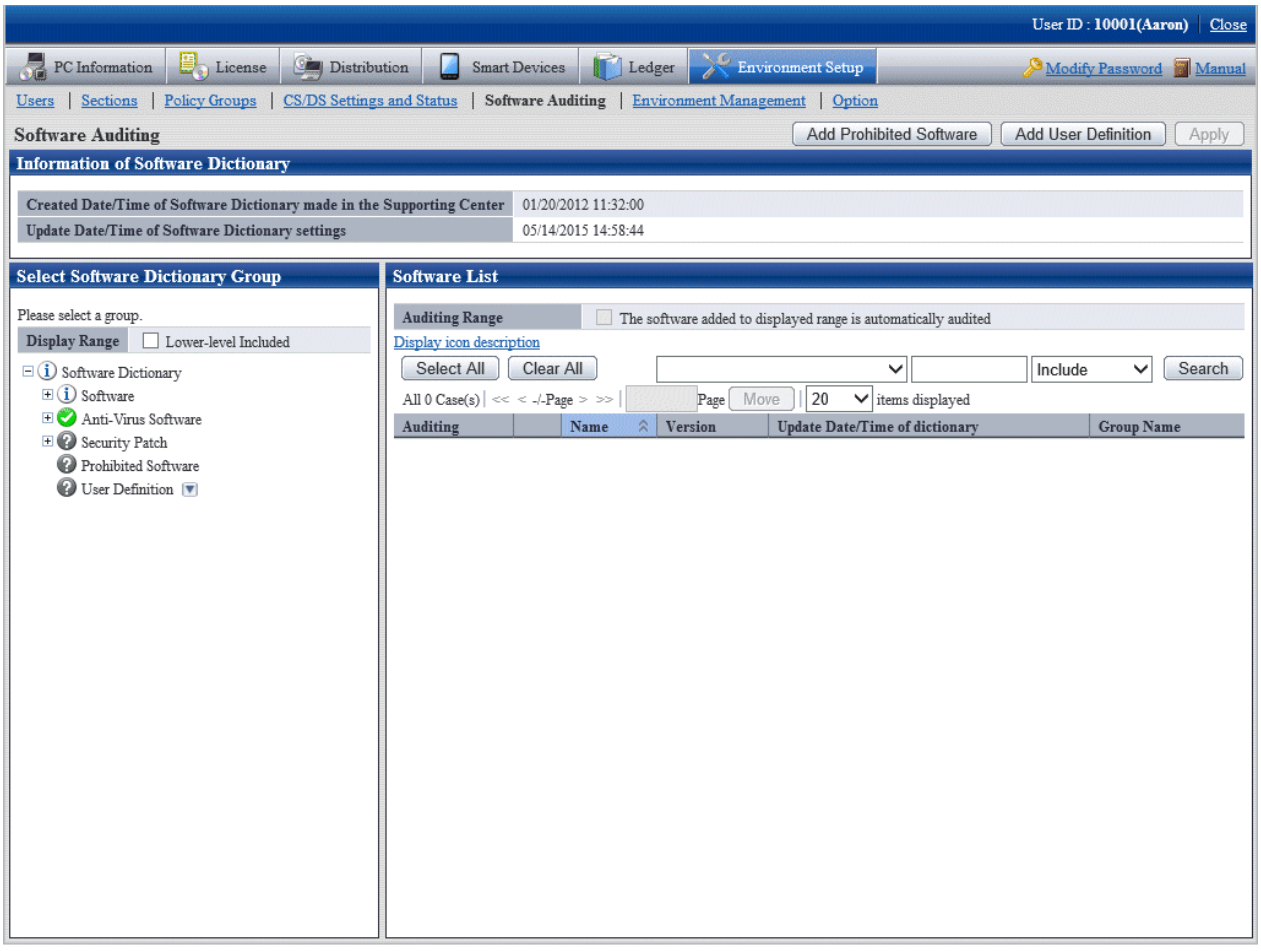
Select software product of user definition

The list of added software products will be added to the following location of the main menu in default setting.

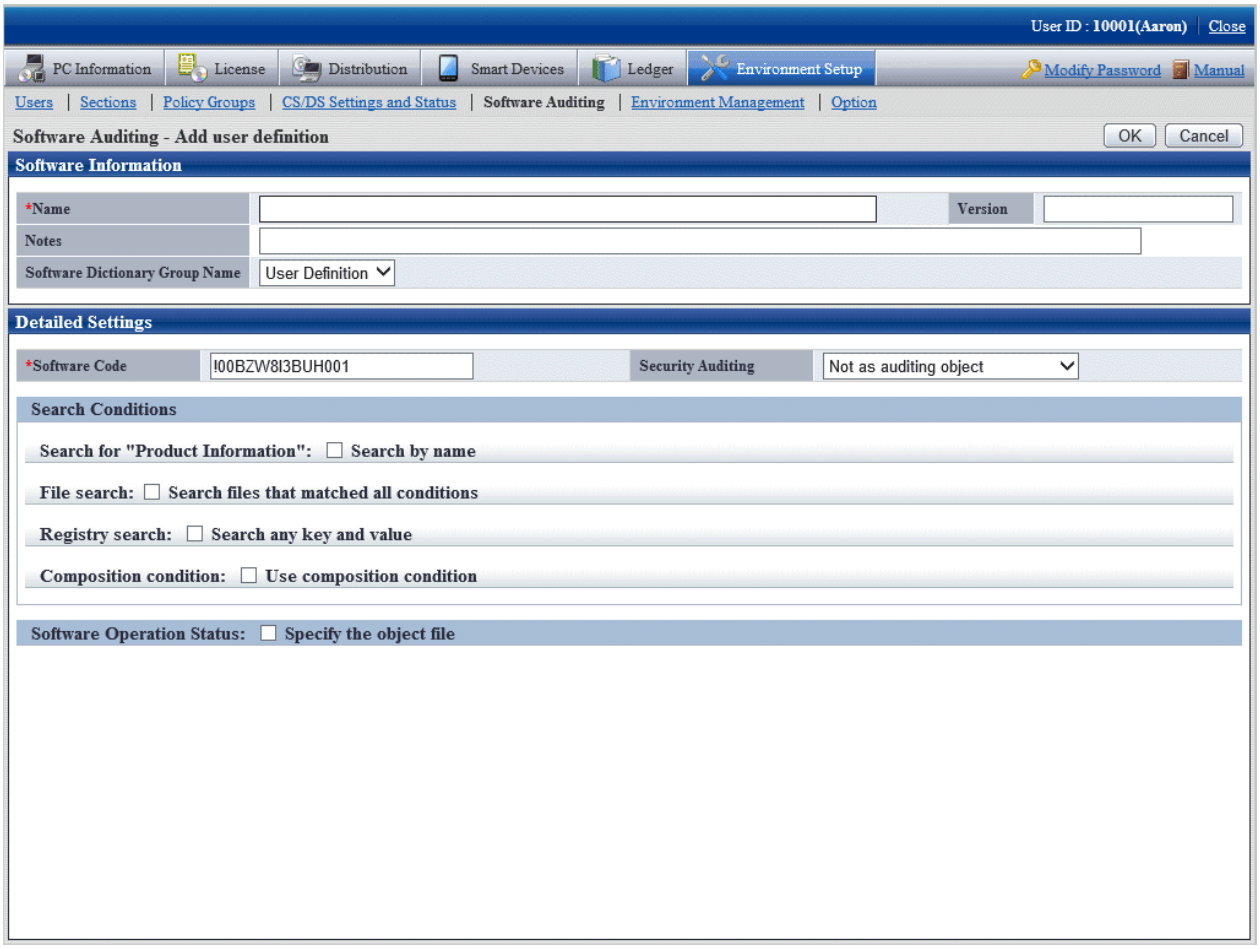
Environment Settings > **Software Auditing** > **Software Dictionary** > **User Definition** > **Installed Software** (Note)

The software product needs to be audited by the administrator.

Note) The location to add software definition is specified in the dtplocaldic.exe (user asset software dictionary creation) command.



The value set for each items of added software definition is shown as follows.



Item	Description
Name	Software name displayed in **Product Information**.
Version	Set **VERSION** as the initial value.
Software Dictionary Group Name	In default setting, **User Definition** (Note) is used as software dictionary group.
Software code	The code that is generated automatically is set. Format: LLMMDDYYYYIIIII LL: Indicates it is created at user definition creation YYYY: 4 digits of western calendar MM: Month (01~12) DD: Date (01~31) IIIII: Increment value (00000~99999)
Search for "Product Information"	The **Search by Name** check box is selected. The result of search by software name according to this setting will be collected as inventory information.
Other items	They are not set as initial value.

Note) The software dictionary group name is specified during the execution of the dtplocaldic.exe (user asset software dictionary creation) command.

Since license management is managed according to the software name displayed in **Product Information**, if the software product for which the version, license and license form cannot be determined exists in the name displayed in **Product Information**, this name cannot be used in software license management.

At this time, this situation can be changed through additional setting for other items of the software license definition. For details, refer to "2.2.2 Create User Definition".

Note

The notes for the user definition creation function are shown as follows.

- User definition of the software product that is not displayed in **Product Information** cannot be created.
- In following cases, software license definition cannot be created through the user asset software dictionary creation command.
  - In software dictionary service, when the software license definition of software product with same name exists in "Support Center Definition"
  - In the previous process of executing the user asset software dictionary creation command, when the software license definition of software product with same name exists in **User Definition**.
- When the software dictionary is provided through software dictionary service, if the software license definition of software product with same name is contained, the software name of **User Definition** will be renamed.

  "Software Name" -> "Software Name (Duplicate)"

2.2.3 Import the SAMAC Software Dictionary

This section explains how to import data registered in the SAMAC Software Dictionary to CS.

Perform the following procedure to import the software dictionary:

1. Stop the CS "ITBudgetMGR (INV)" service.
2. Edit and save the following file:

   ```
   csInstallDir\FJSVsbtrs\etc\jreoption.inf
   ```

   Example: C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbtrs\etc\jreoption.inf

   - Before

     -Xmx640m -Xmx640m

   - After

     -Xmx1024m -Xmx1024m
3. Start the CS "ITBudgetMGR (INV)" service.
4. Execute dtplocaldic.exe (creating user asset software dictionary command) and export the data registered in the SAMAC Software Dictionary to CS.

   Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on dtplocaldic.exe.

Point

- More than 70,000 items of software information are registered in the SAMAC Software Dictionary. It is therefore recommended that you filter the software information by the following categories before importing it.
  - Vendor name
  - Software type
    - Commercial software
    - Freeware
    - Drivers, utilities and so on.
    - Hotfix

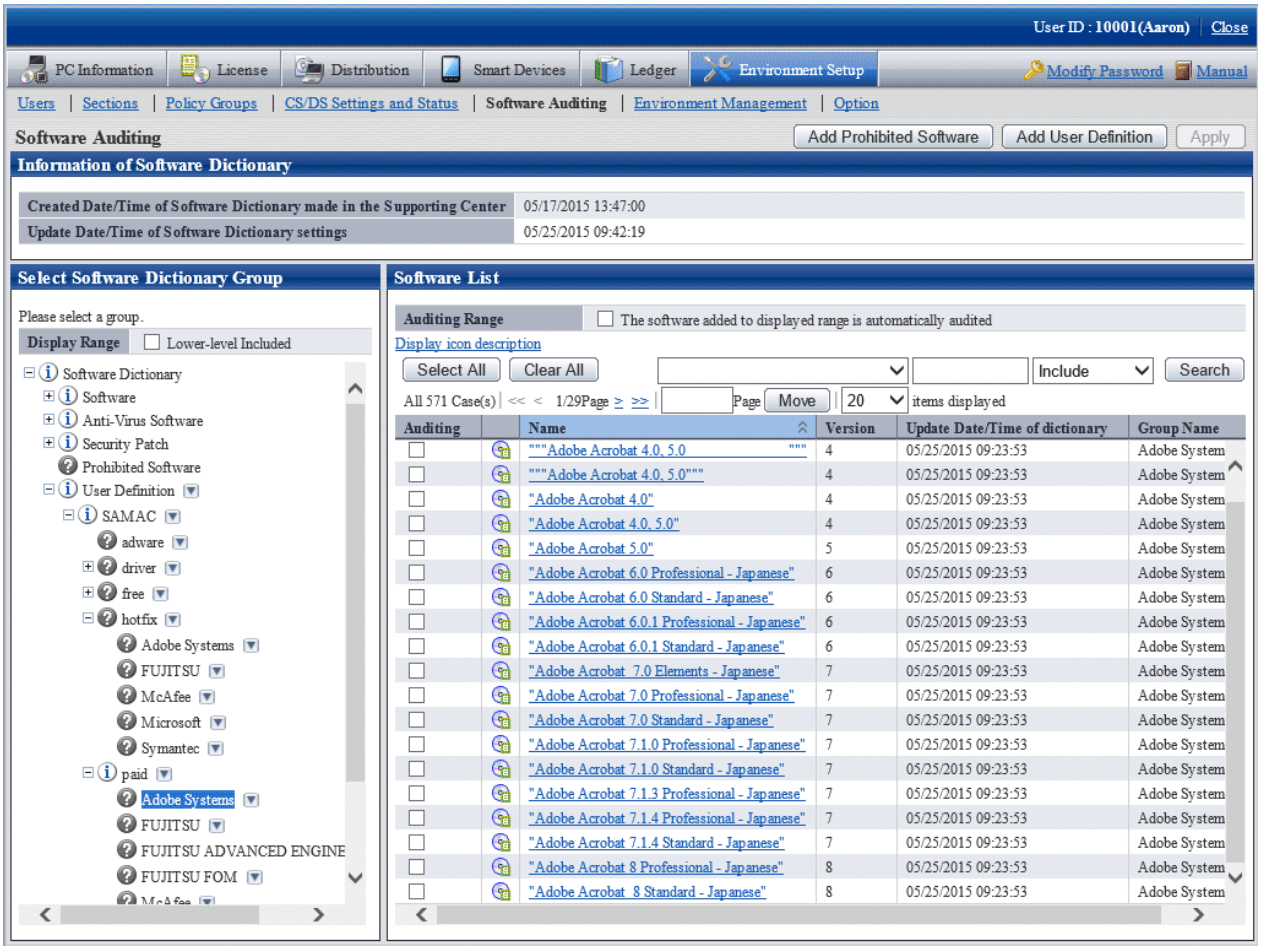
  - Adware
  - Unknown
- After you import the SAMAC software information, **Search by name** is selected when you search **Product Information**.
- You can detect the software installation status and manage licenses by selecting the software to be monitored and specifying the search conditions.

Import destination of SAMAC software information

The import destination for SAMAC software information is in **User Definition** > **SAMAC** > **Software Type** > **Vendor Name**. Vendor name groups can be created only for the following vendors:

- Adobe Systems
- Microsoft
- McAfee
- Symantec
- TREND MICRO
- Vendor name containing "FUJITSU"

Software information for vendors other than the above is added in **User Definition** > **SAMAC** > **Software Type**.



2.3 Set Client Policy

Information about the operation of each function in Systemwalker Desktop Patrol is recorded in enacted rules, and the set of this information is called policy. Policy has the following types.

- Client Policy

  This policy is used to manage the application of CT.

  There are following two methods to manage client policy, you can apply them according to the application pattern or apply them after combination.

Policy application of DS unit

Regard the CT configured as a subordinate of a higher server as a management unit, and the client policy is applied by each management unit.

To classify the settings of client policy, install DS in each management unit.

Since the management unit is composed of a network connection between client PC and a higher server, the policy that has considered the transfer rate and the communication load of the network can be operated. In addition, since the policy of DS unit will be applied automatically when the new client PC is connecting with the higher server, the administrator can do the daily operation more easily.

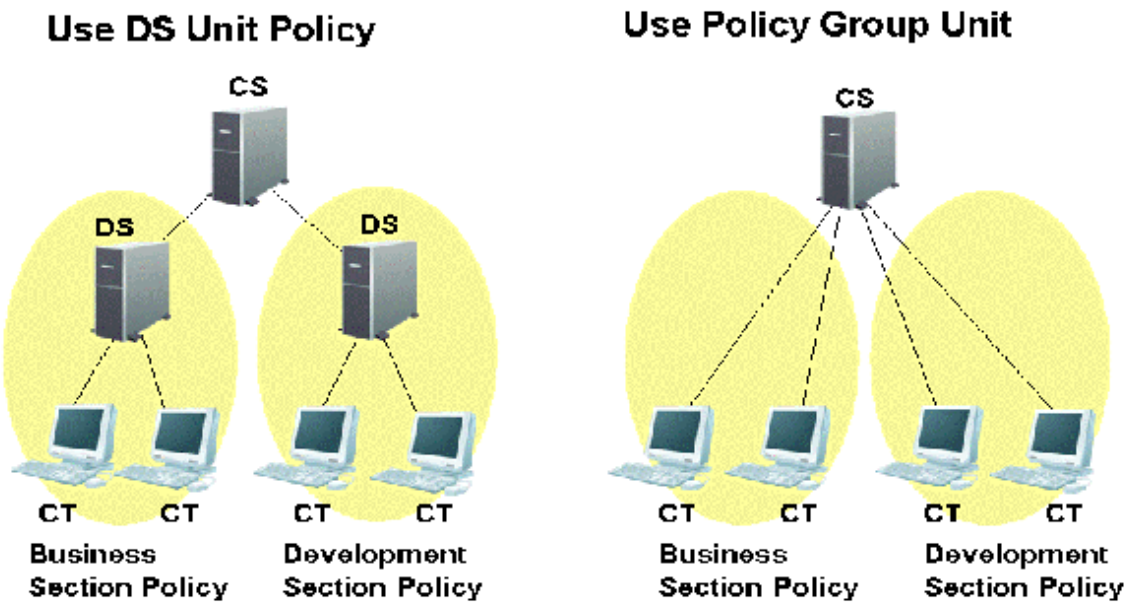
Application of policy group unit

Create a logical group and apply the client policy in this group unit. To classify the settings of policy settings, the administrator creates a policy group and registers each client PC in this group.

Groups can be freely defined without being confined by the physical network configuration, so policy of any PCs can be managed across the higher server.

In addition, the PC that does not belong to a policy group and the PC with CT prior to V13.0.0 are operated according to the policy of DS unit.

The policy application of DS unit and the application of policy group unit are shown in the diagram below.



Setting methods

CT runs according to the policy of DS unit or policy group.

Under the initial status of CT, it will belong to the "Default Group" automatically. The CT that belongs to the "Default Group" will run according to the policy of DS unit (in initial status, it runs according to the client policy set in the DS unit of higher server.)

The CT that belongs to the policy group is the CT that is registered automatically to CS during inventory collection. In addition, at the installation stage of Systemwalker Desktop Patrol and before network connection, etc, the CT that is not registered to CS can be classified to the belonging policy group through the following approaches.

- Register PC using the dtppcmst.exe (PC registration) command

  For details on the dtppcmst.exe (PC registration) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

A new policy group is created and the PC that belongs to the default group is changed to the new group, and the CT will run according to the client policy set in the policy group it belongs.

The tiny operations such as "Install security patches automatically in the general PCs but not install in server PC" can be performed by simultaneously using the policy application of DS unit and of policy group.

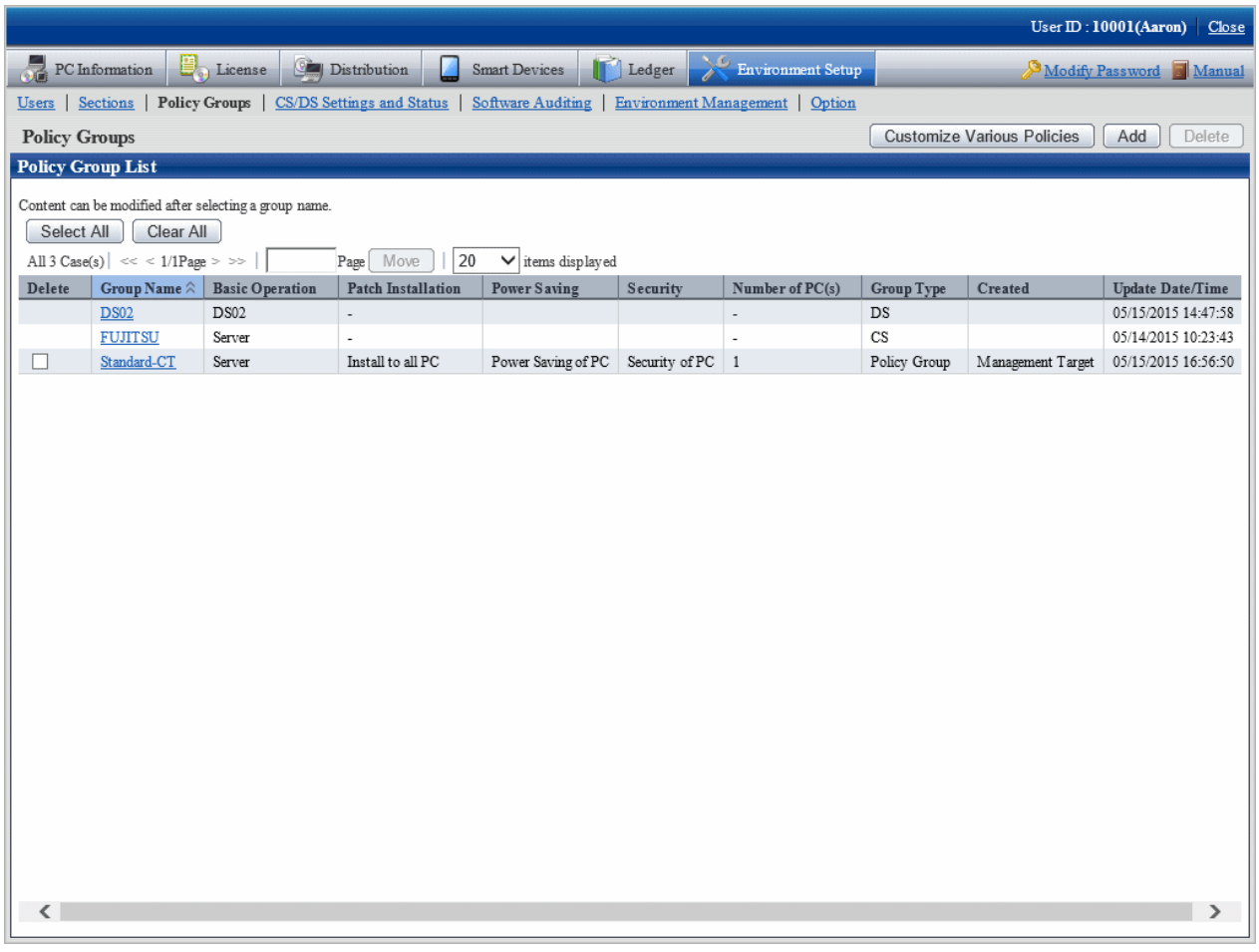
The procedure of setting policy group is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **Policy Groups**.

   The following window is displayed.



   The meaning of each item in this window is as follows.

Item	Description
Delete check box	A group will be deleted by selecting this check box and clicking the **Delete** button. When the group type is CS/DS, it cannot be deleted. After a group has been deleted, the PC that belongs to the group will run according to the policy setting of the server it connects to.
Group Name	The group name created by CS name, DS name or user is displayed. By clicking the link, the group name information and PC in a group can be modified.
Basic Operation	The basic operation setting name used in a group is displayed.
Patch Installation	The patch installation setting name used in a group is displayed.
Power Saving	The power-saving setting name used in a group is displayed.
Security	The security setting name used in a group is displayed.
Number of PC(s)	The number of PCs belong to the group is displayed. It is not displayed in case of the group that is not for operation settings.
Group Type	Display the type of group. - **CS** It is the group for CT to connect to CS. - **DS** It is the group for CT to connect to DS. - **Policy group** It has nothing to do with the connected server, and it is the policy group that specifies a particular PC. - **Command mode CT** It is the group used by command mode CT.
Created	The section in which the policy group was created is displayed. All policy groups will be displayed when logging in using system administrator. Only the policy group within the section will be displayed when logging in using section administrator.
Update Date/Time	The date and time when policy group and settings are updated is displayed. When the group type is CS/DS, the date and time relating to PC increment/decrement will not be displayed.

3. Click the following button to operate policy.

Button Name	Description
Customize Various Policies button	Customize the settings of various policies.
Add button	Create one group that uses various settings.
Delete button	Delete policy group.

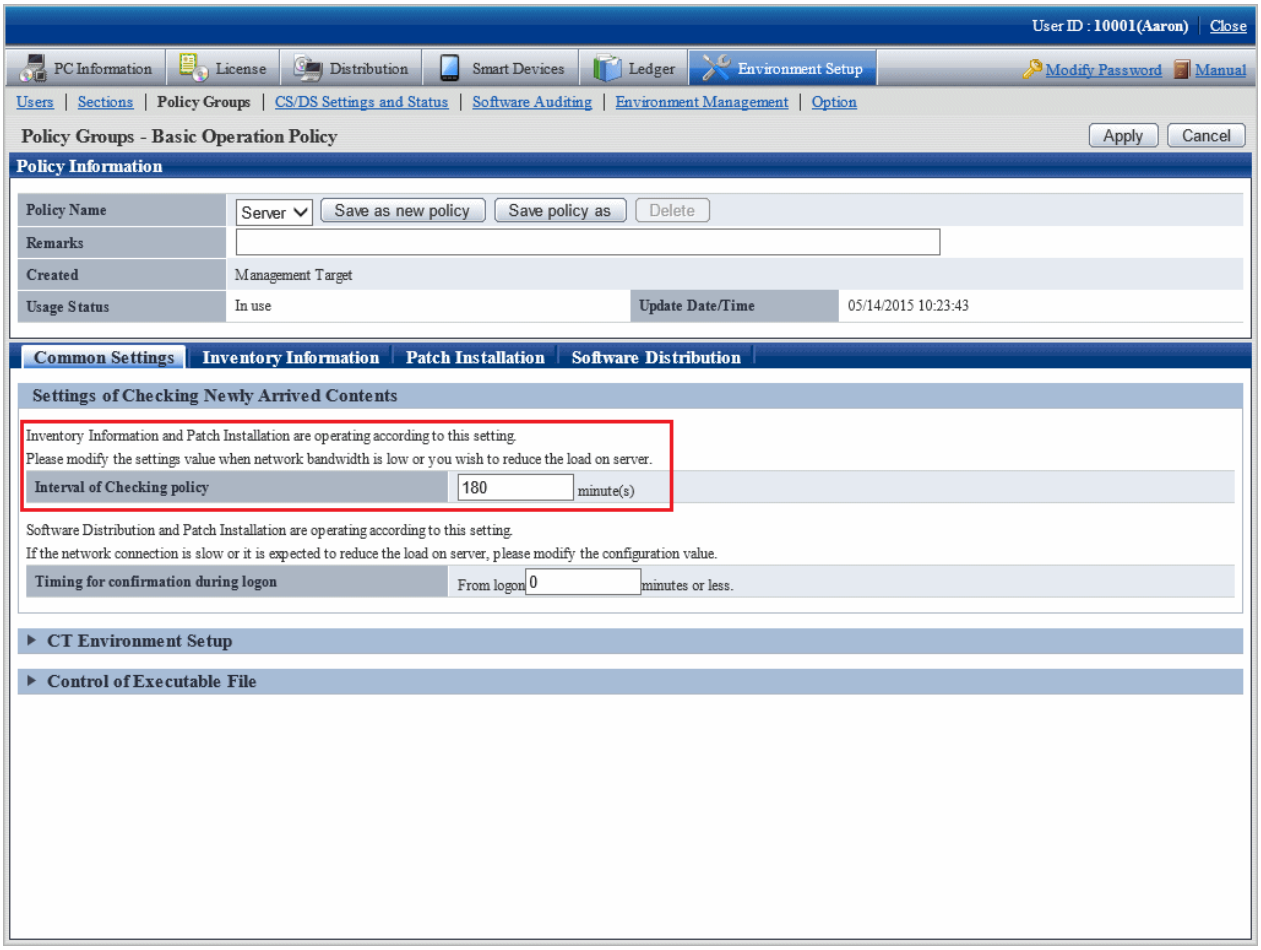
Timing of policy reflection

The policy will be reflected to CT at the timing set in the following window.

- Select **Interval of Checking policy** of **Environment Setup** > **Policy Groups** > **Basic Operation Policy** tab > **Common Settings** tab of the main menu.

After distributing within the time set in the **Interval of Checking policy** window, and confirm to the higher server using a random number.

If there is an updated client policy, the client policy will be reflected to CT after it is received.



2.3.1 Create Policy Group

It describes how to create policy group.

2.3.1.1 Add Policy Group

Add a policy group.

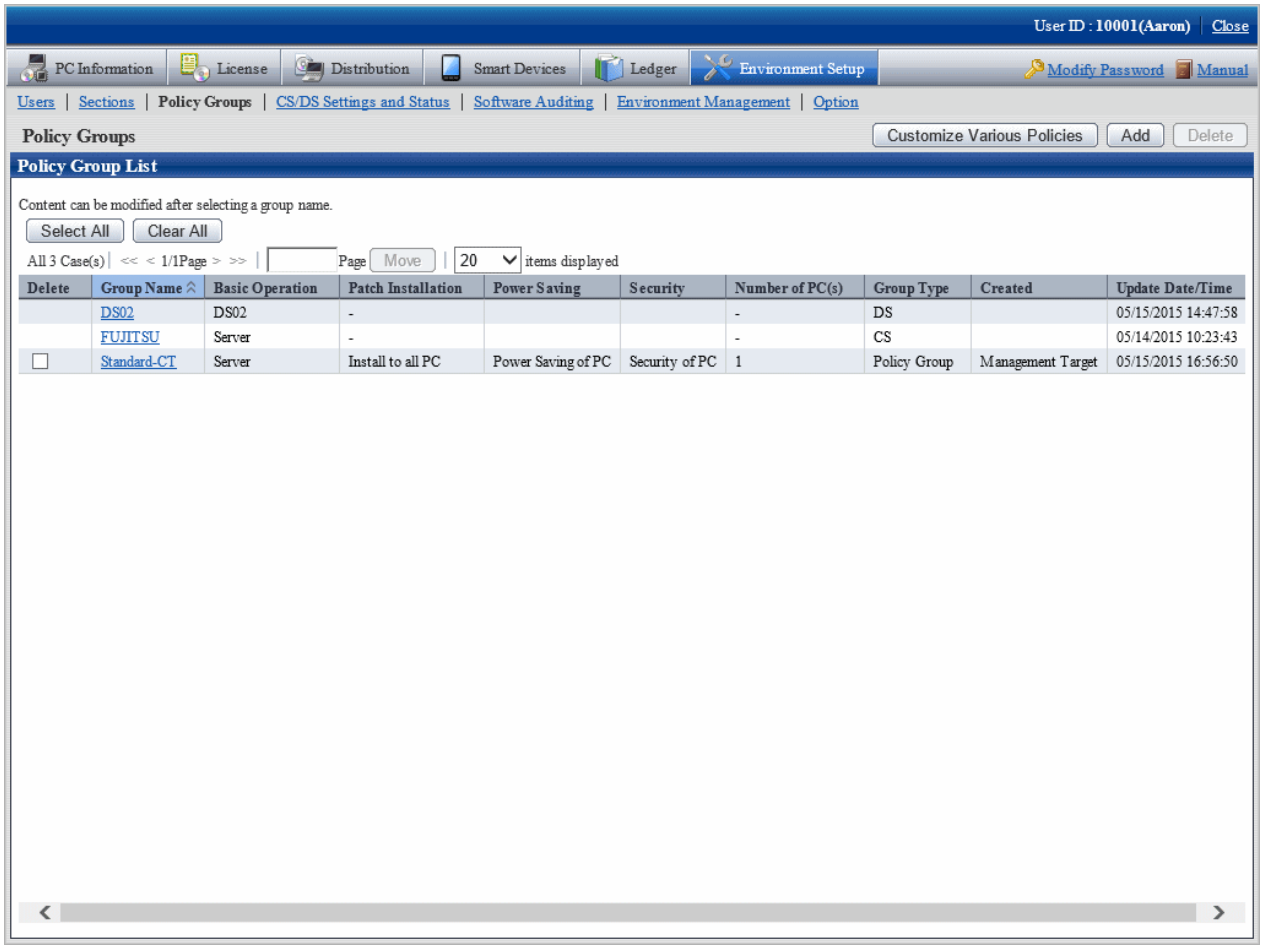
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

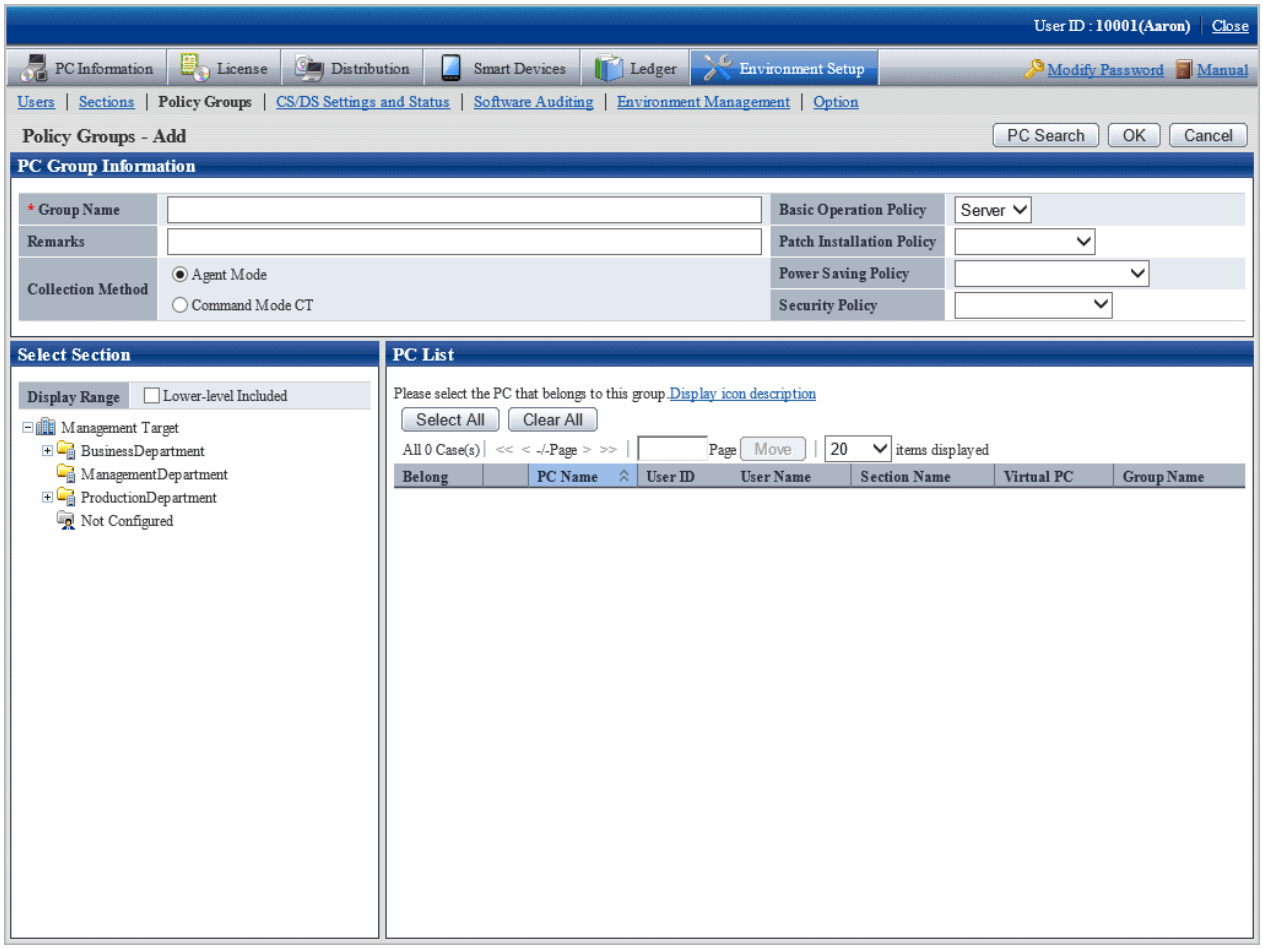
2. Click **Policy Groups**.

   The following window is displayed.



3. Click the **Add** button.

   The following window is displayed.



4. Enter the following items.

Item	Description
Group Name	Enter the name of policy group. Up to 60 characters can be entered. Characters can be specified include alphanumeric characters and the following single-byte symbols. ("-""@"".""("")""["]""{"}""<"">"":";")
Remarks	Enter the remarks. Up to 256 characters can be entered.
Basic Operation Policy	Select the basic operation setting used in this group from the pull-down menu.
Patch Installation Policy	Select the excluded patch setting used in this group from the pull-down menu. Select "-" when the operation of excluded patch is not performed.
Power Saving Policy	Select the power saving setting used in this group from the pull-down menu. Select "-" when the operation of power saving setting is not performed.
Security Policy	Select the security setting used in this group from the pull-down menu. Select "-" when the operation of security setting is not performed.
Collection Method	Select the collection method of this group. - Agent mode

Item	Description
	Specify when creating the group for agent mode. - Command Mode CT Specify when creating the group for command mode CT.

5. Register PC to policy group.

   Select the PC to be registered through one of the following method.

   a. Select a section from the section tree in the field on the left.

      The PC under the selected section will be displayed in the field on the right.

      - If the words such as PC name are displayed in gray, it indicates that the PC is not running according to policy group. There are following major types.

        In case of command mode CT

        In case of PC of the version prior to V13.0.0

        The PC of versions prior to V13.0.0 can be classified to the policy group. In this case, when the PC is updated to V13.0.0 or later, it will run according to the policy group.

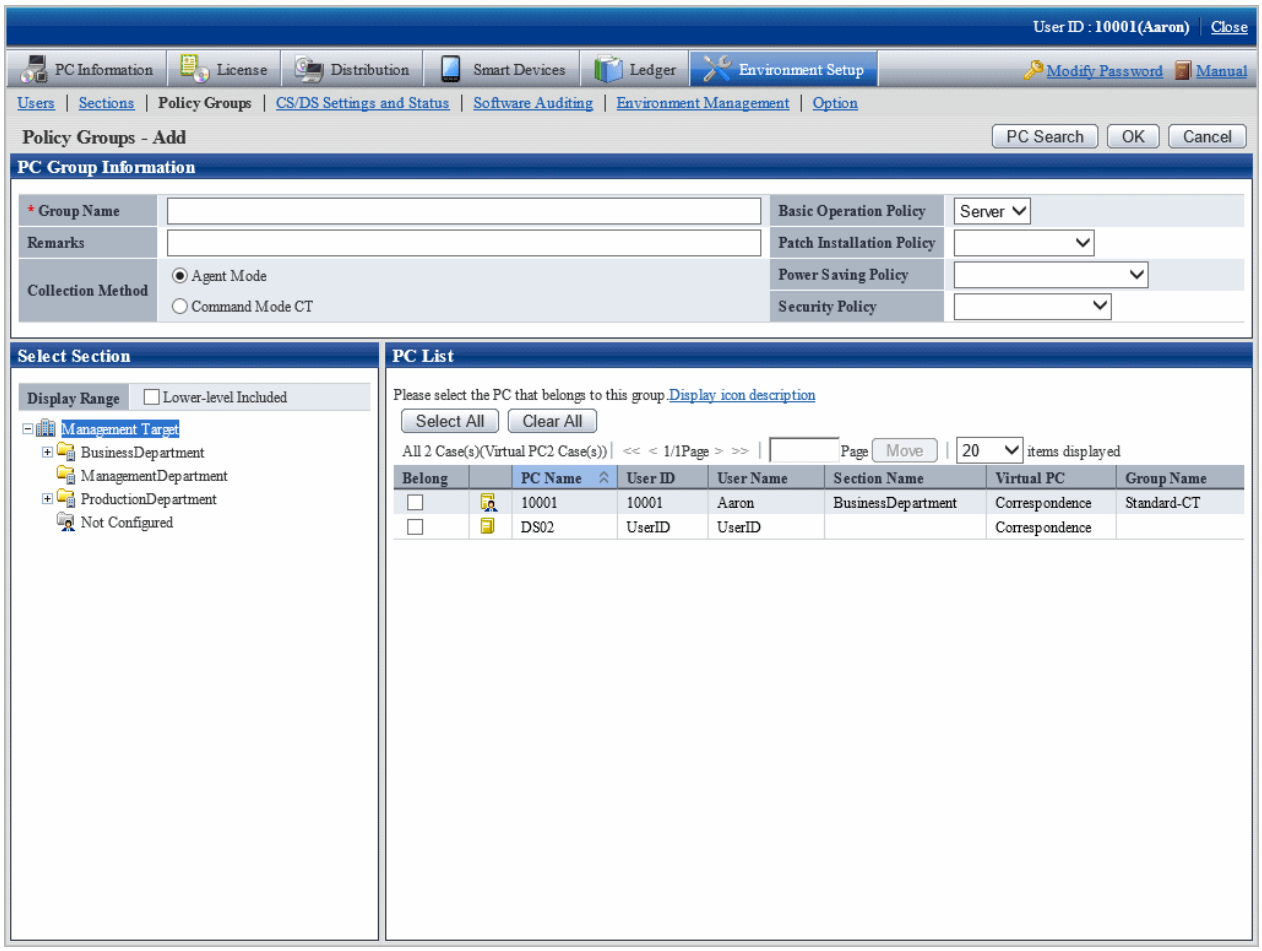
      - The PC registered using the dtppcmst.exe (PC registration) command is displayed using the following dot line icon.

   b. Click the **PC Search** button.

      The window for entering search condition is displayed.

      Enter the search condition and click the **Search** button.

The PC that matches with the search condition is displayed.



6. Select the PC name to be belonging to the policy group and click the **OK** button.

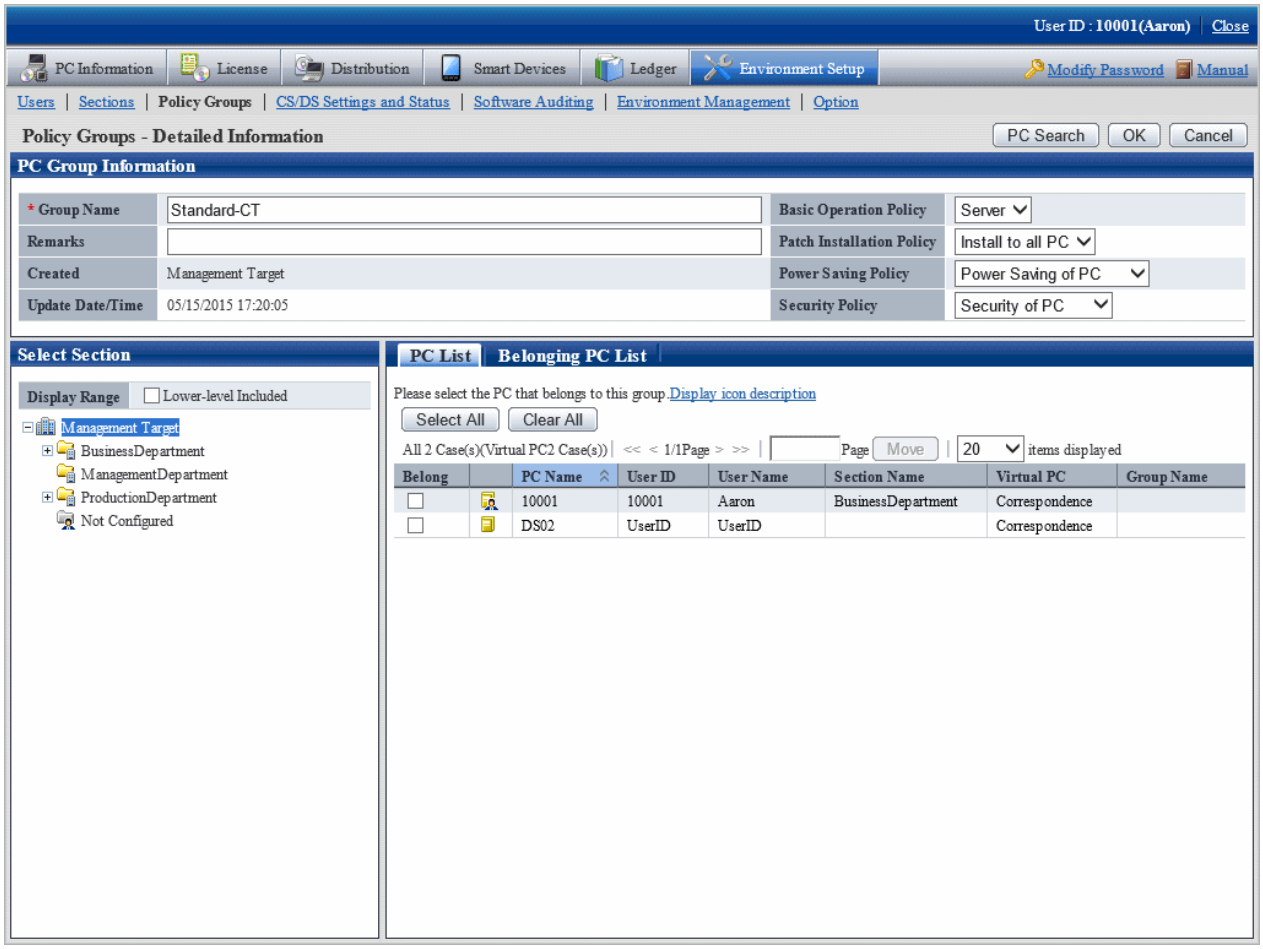
   The PC to be belonging to the policy group is selected.

7. Click the **OK** button.

   The policy group to which the PC belongs is added.

8. To confirm the PC that belongs to the policy group, repeat the operation of step "5.", and click the **PC List** tab to confirm.

   The belonging PC list is displayed.



2.3.1.2 Add Command Mode CT

Add the group used for command mode CT.

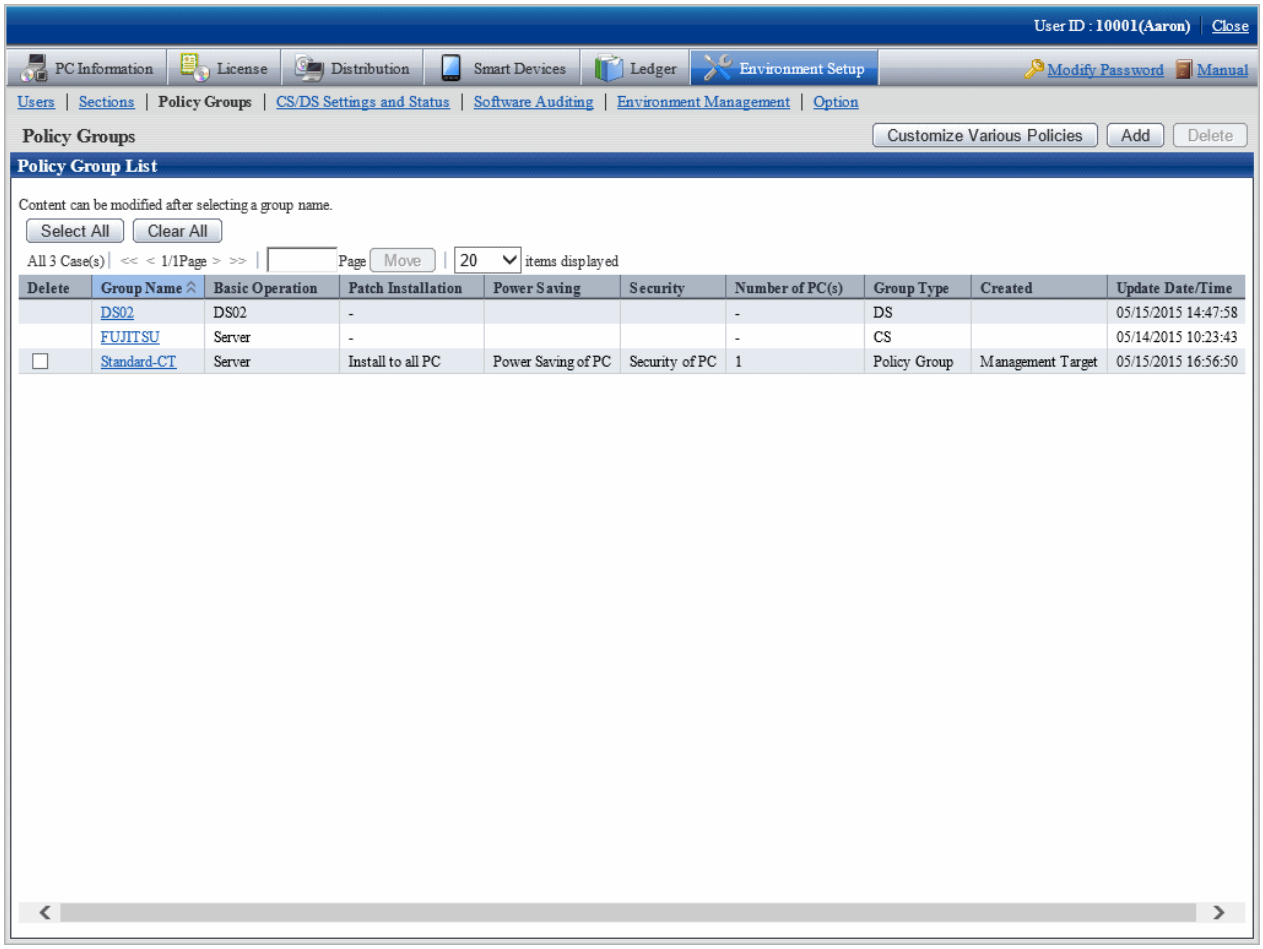
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

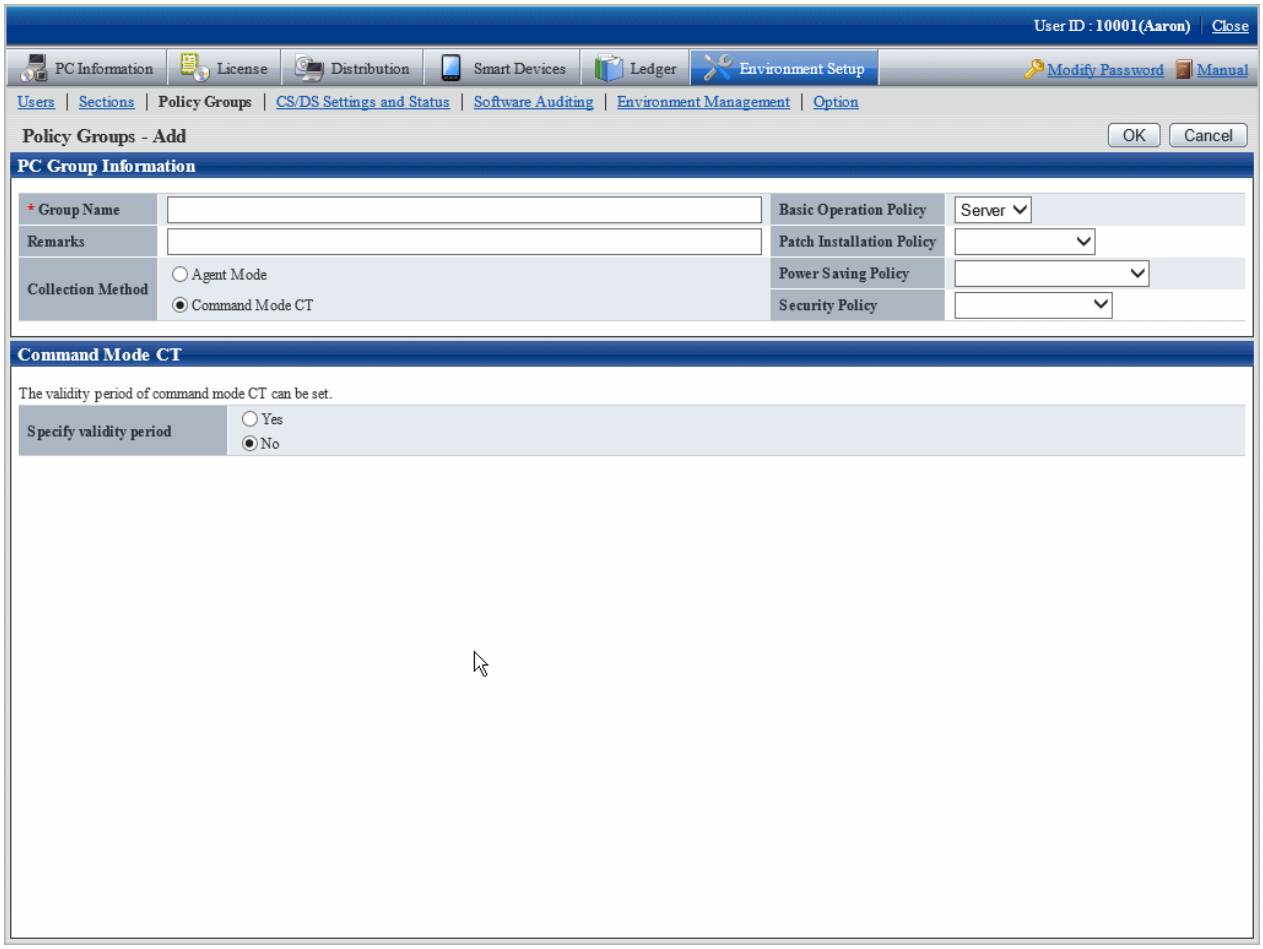
2. Click **Policy Groups**.

   The following window is displayed.



3. Click the **Add** button.

   The following window is displayed.



4. Enter the following items.

Item	Description
Group Name	Enter the name of policy group. Up to 60 characters can be entered. Characters can be specified include alphanumeric characters and the following single-byte symbols. ("-""@"".""("")""["]"{"}""<"">"":";")
Remarks	Enter the remarks. Up to 128 multi-byte characters and 256 single-byte characters can be entered.
Basic Operation Policy	Select the basic operation setting used in this group from the pull-down menu.
Patch Installation Policy	Select the excluded patch setting used in this group from the pull-down menu. Select "- "when the operation of excluded patch is not performed.
Power Saving Policy	Select the power saving setting used in this group from the pull-down menu. Select "- "when the operation of power saving setting is not performed.
Security Policy	Select the security setting used in this group from the pull-down menu. Select "-" when the operation of security setting is not performed.
Collection Method	Select the collection method of this group.

Item	Description
	- **Agent mode** Specify when creating the group for agent mode. - **Command Mode CT** Specify when creating the group for command mode CT.

5. Set the effective period of command mode CT.

Item	Description
Specify validity period	Select **Yes** to set the effective period of command mode CT. Select the number of days from 1 to 60 since creation from the list.

6. Click the **OK** button.

   The group is added.

2.3.1.3 Modify Policy Group Information

Modify the information of registered policy group.

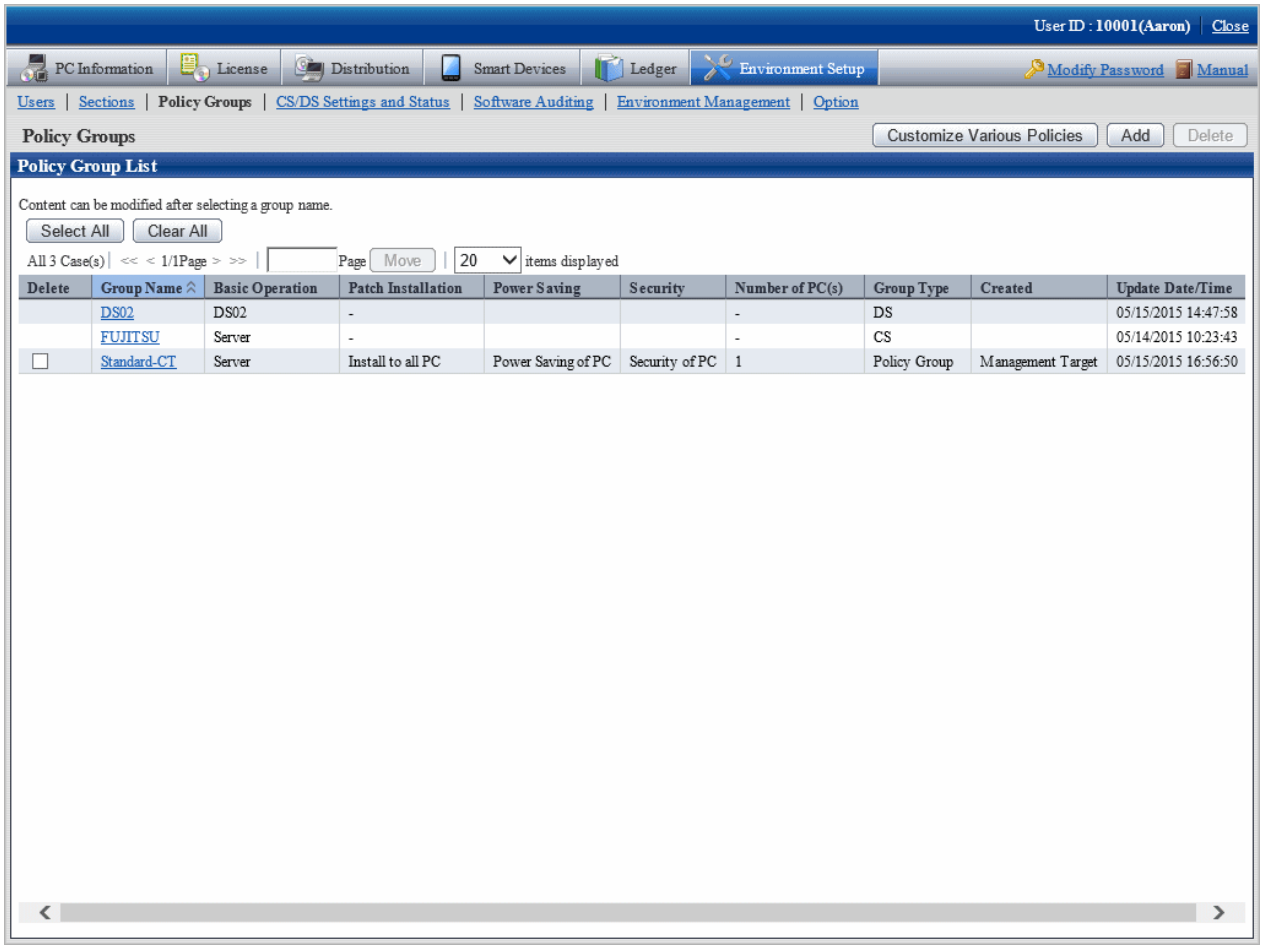
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

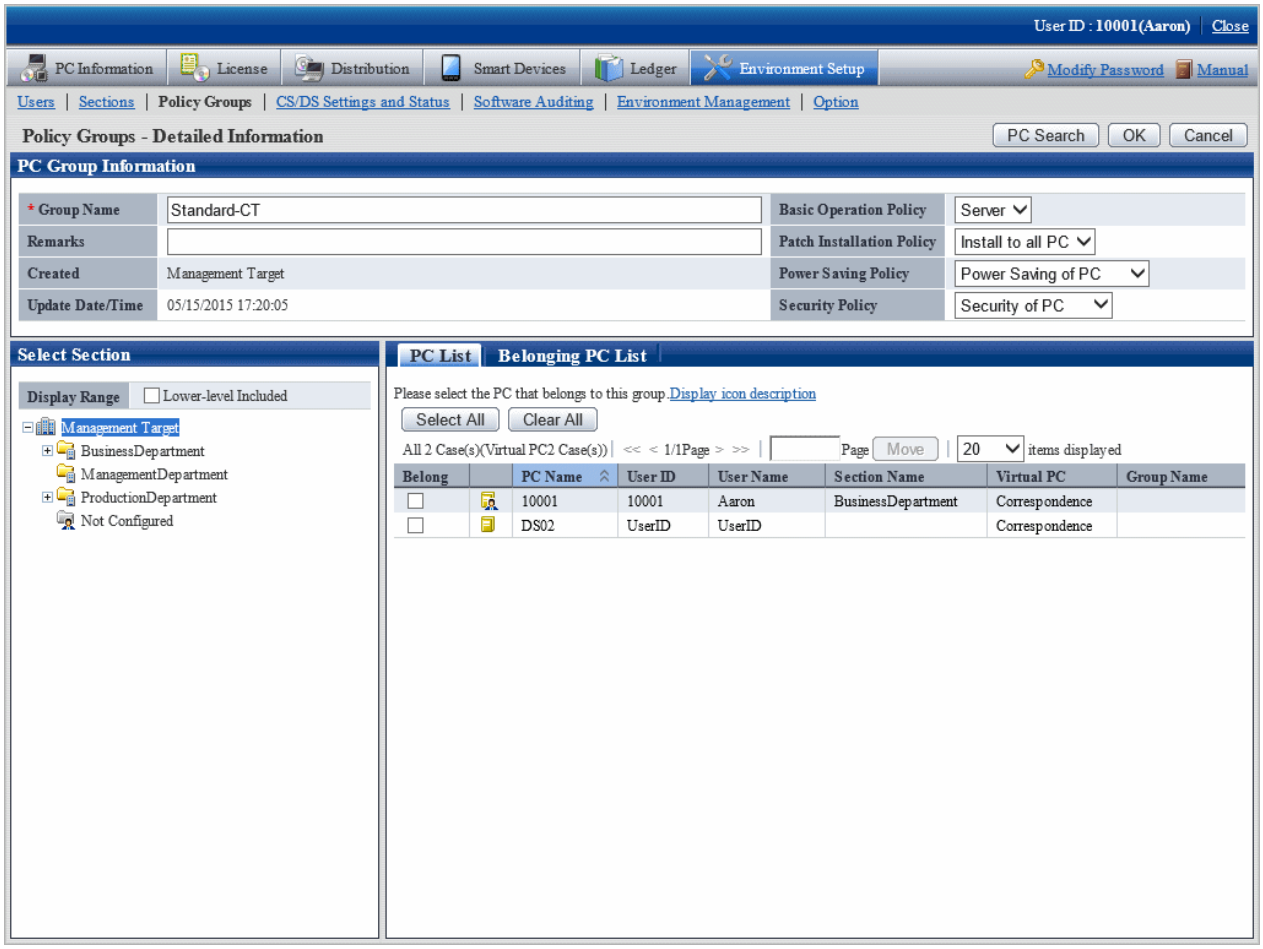
2. Click **Policy Groups**.

   The following window is displayed.



3. Click the link of **Group Name** to modify settings.

   The following window is displayed.



4. Modify the content of each item.

   In addition, when **CS** or **DS** is selected in the type, the group name, Patch Installation Policy and belonging PC cannot be modified.

5. Click the **OK** button.

   The group information is modified.

2.3.1.4 Delete Policy Group

Delete a policy group.

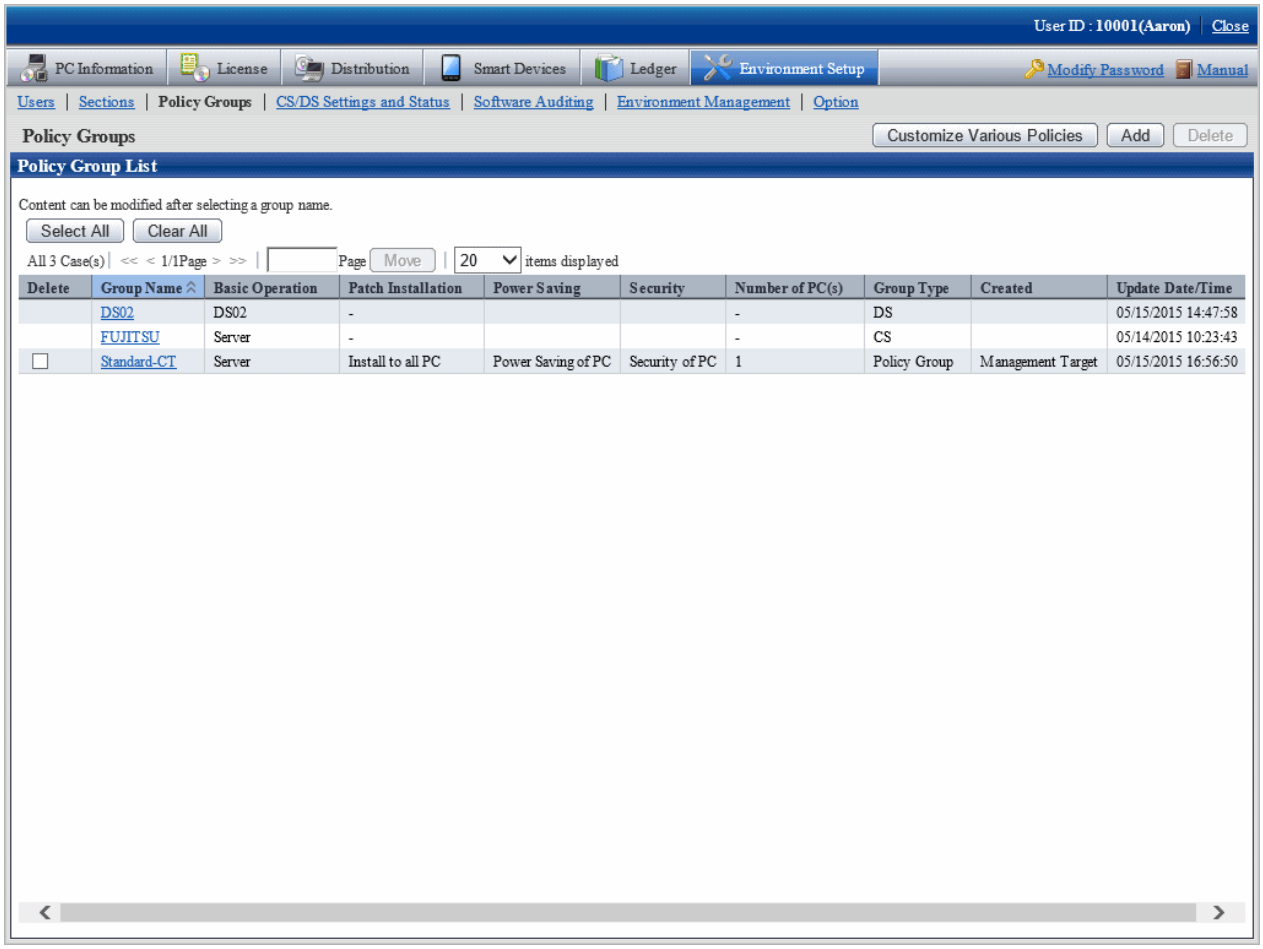
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **Policy Groups**.

   The following window is displayed.



3. Select the policy group to be deleted, and click the **Delete** button.

   The group is deleted.

   After the policy group has been deleted, the PC that belongs to the group will have no affiliation. At this time, the PC will run according to the policy set in CS/DS.

2.3.2 Customize Various Policies

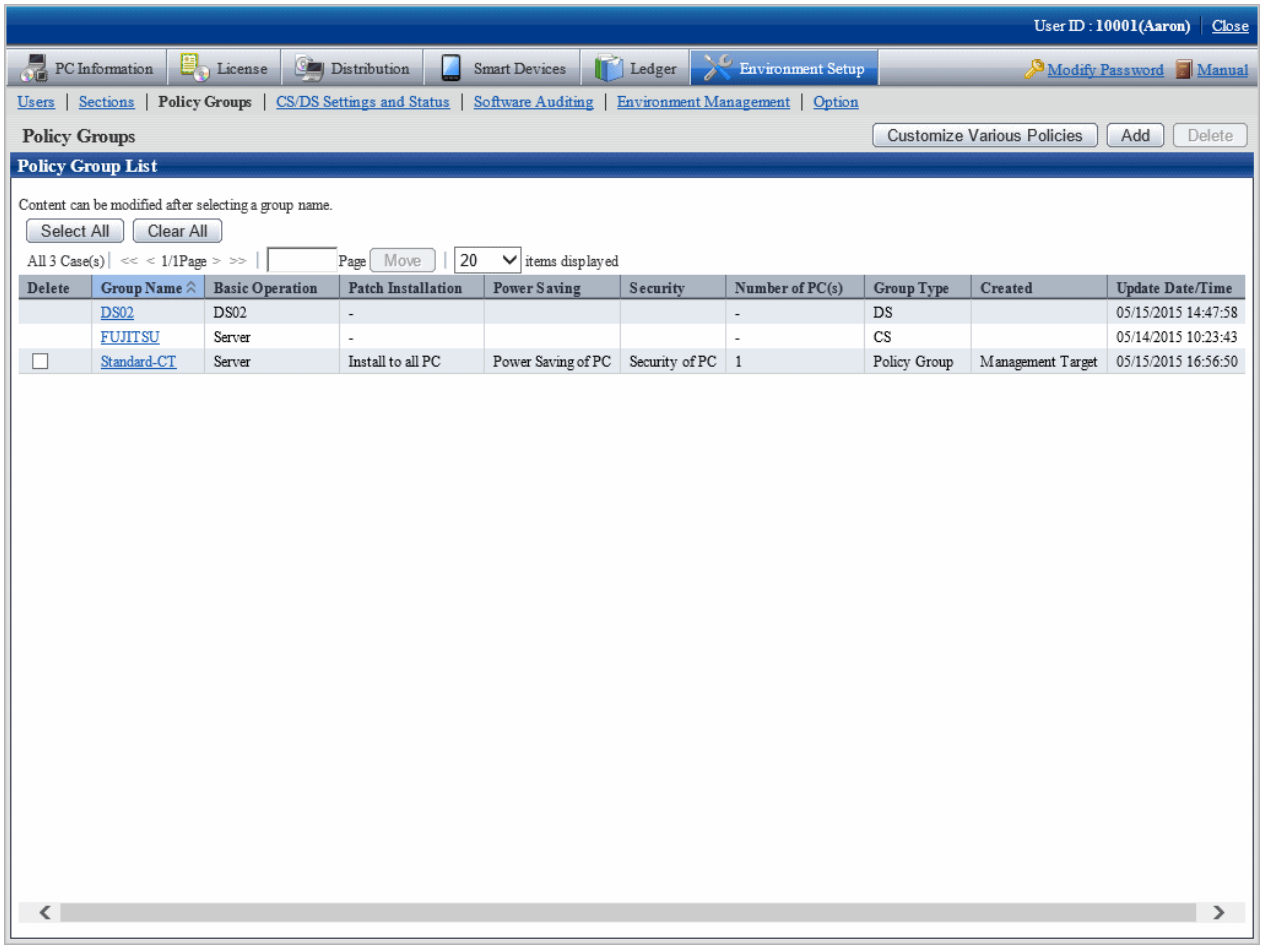
Customize various policies according to the following procedure.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

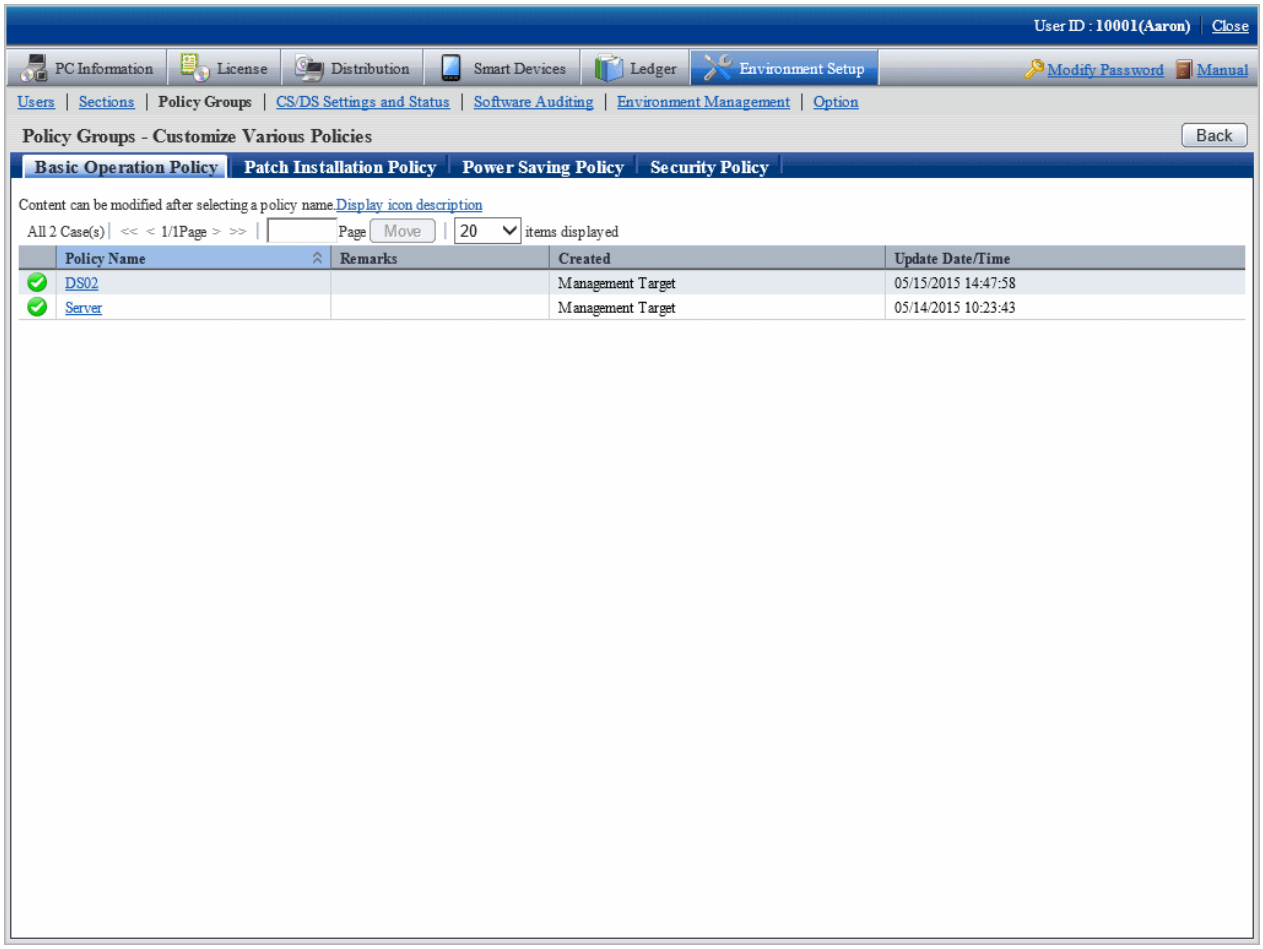
2. Click **Policy Groups**.

   The following window is displayed.



3. Click the **Customize various policies** button.

   The following window is displayed.



   The meaning of each item in this window is shown as follows.

Item	Description
Icon	It shows whether the group that uses the policy exists or not. : The correspondent policy is not used in policy group. : The correspondent policy is being used in policy group.
Policy Name	It shows the policy name. By clicking on the link, the policy content can be modified or copied, and the policy can be deleted.
Remarks	The remarks for the policy are displayed.
Created	The section that created the policy is displayed. When login with system administrator, all policy groups will be displayed. When login with section administrator, only the policy group created within the section will be displayed.
Update Date/Time	The date and time when policy was updated is displayed.

4. Click the following setting tab to be customized.

   - Basic Operation Policy
   - Patch Installation Policy

- Power Saving Policy
- Security Policy

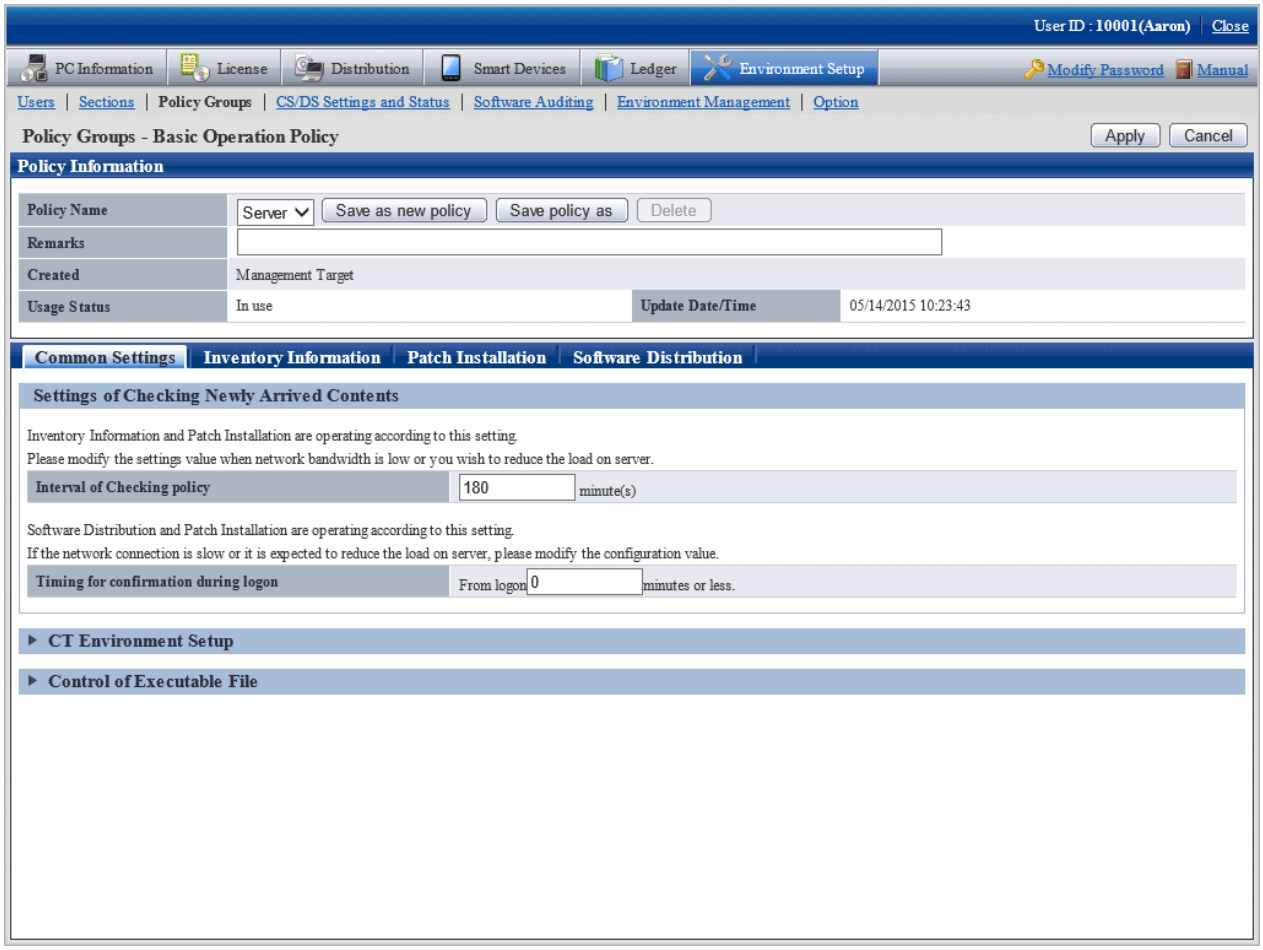
For each window, refer to the following description.

2.3.2.1 Customize Basic Operation Policy

Customize basic operation policy according to the following procedure.

1. Click the **Basic operation policy** tab in the **Customize various policies** window.

   By clicking the link of policy name, the following window is displayed.



2. Enter the setting information.

Item	Description
Policy Name	The policy name of various policies can be selected from the list.
Save as new policy button	Register the content of various policies with new policy names. Up to 30 multi-byte characters or 60 single-byte characters can be entered in policy name. Characters can be specified are alphanumeric characters and the following single-byte symbols. ("-""@"".""(")"["]"{"}"<">":";")
Save policy as button	Modify the selected policy name. Characters can be specified are the same as **Save As**.

Item	Description
Delete button	Delete the policy selected from the list. After policy name has been deleted, the group that uses policy previously will be in the status of not using policy. In addition, if no policy name exists in the various policies, the **Delete** button will be disabled.
Remarks	Enter the remarks. Up to 128 multi-byte characters and 256 single-byte characters can be entered.

3. Set the following items.

   - **Common Settings** tab

     Perform the following common settings for inventory information collection and installation of security patches.

Item	Description
Interval of Checking policy	Set the time interval to perform confirmation of newly arrived information when client PC is connected to the higher server in minutes. Specify a value within 30~1440. The inventory collection function and automatic patch installation function run according to this setting. When the bandwidth of network circuit is small and it is expected to reduce the server load, modify this setting value. When the initial value is 180 minutes. The initial timing of newly arrival confirmation is distributed as the maximum value of this value.
Timing for confirmation during logon	Specify the maximum time from logon to Windows till the newly arrival confirmation in minutes. Specify a value within 0~180. When a value except 0 is specified, the actual time from logon to Windows till the newly arrival confirmation is a random number between 0 and the maximum time. The initial value is 0 minute. -

   - **Inventory Information** tab

     Perform settings related to the collection of inventory information. For details, refer to "Chapter 3 View PC Information".

   - **Patch Installation** tab

     Perform the settings related to the installation of security patches. For details, refer to "Chapter 6 Distribute/Install Security Patches".

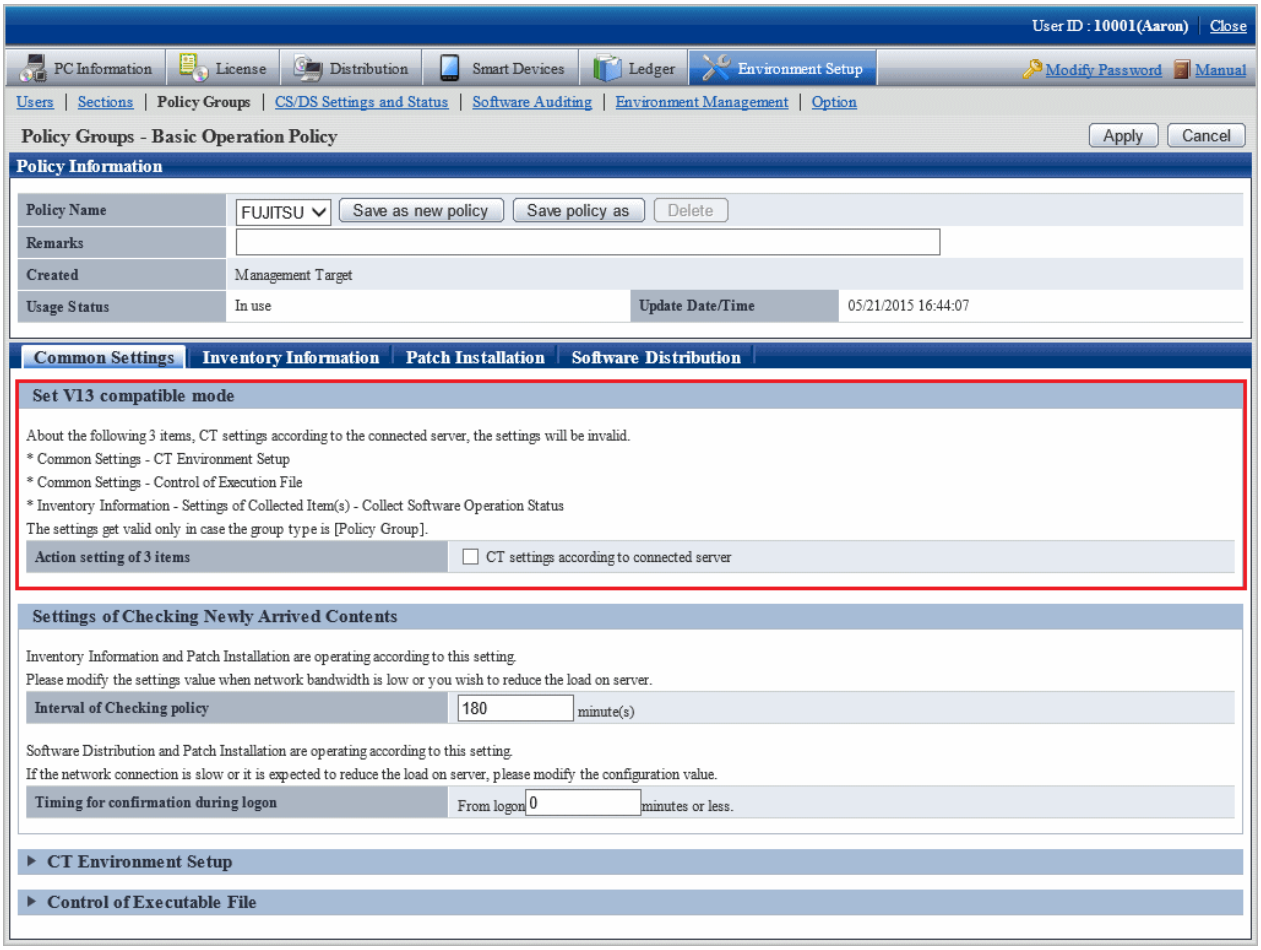
   - **Software Distribution** tab

     Perform settings related to software distribution. For details, refer to "Chapter 8 Distribute Software".

4. Click the **Apply** button, save the settings.

Common setting window at version update from V13

After version update from V13, the following items will be displayed in **Basic Operation Policy** > **Common Settings** tab.



Set V13 compatible mode

Item	Description
Action setting of 3 Items	When the check box is selected, the setting of following three items will follow the setting of server connected with the CT, and the specification in policy group will be invalid. - **Common Settings > CT Environment Setup** - **Common Settings > Control of Executable File** - **Inventory Information > Settings of Collected Item(s) > Collect Software Operation Status** This setting is effective only when the group type is "Policy Group".

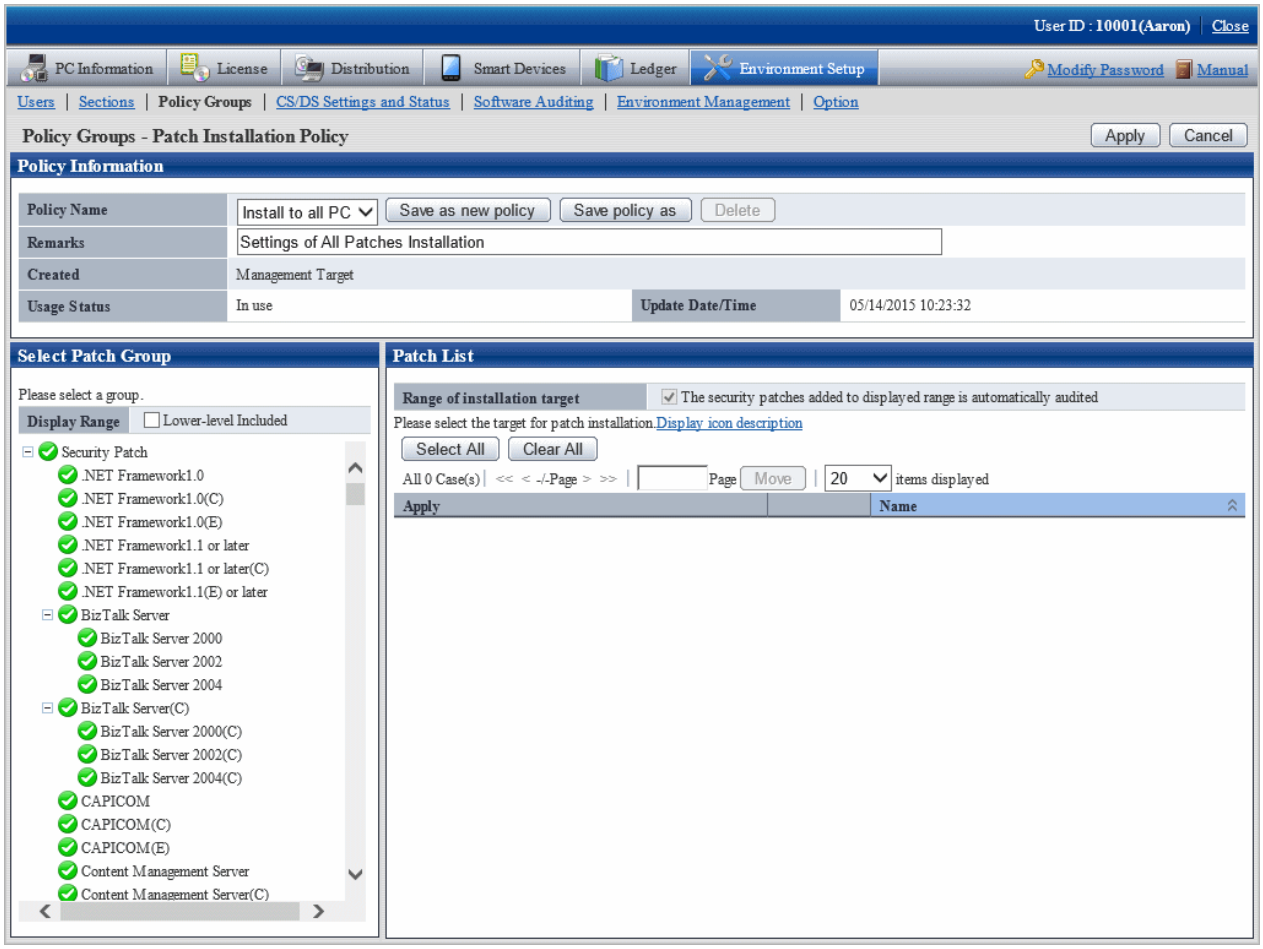
2.3.2.2 Customize Patch Installation

The security patch installed to particular PC is selected, set the patch to be installed.

The procedure is as follows.

1. In the **Customize various policies** window, click the **Patch Installation policy** tab.

   Click the link of policy name, the following window is displayed.



2. Enter the setting information.

Item	Description
Policy Name	The policy name of various policies can be selected from the list.
Save as new policy button	Register the content of various policies with new policy names. Up to 30 multi-byte characters or 60 single-byte characters can be entered in policy name. Characters can be specified are alphanumeric characters and the following single-byte symbols. ("-""@"".""("")""["]""{""}""<"">"":";")
Save Policy as button	Modify the selected policy name. Characters can be specified are the same as **Save As**.
Delete button	Delete the policy selected from the list. After policy name has been deleted, the group that uses policy previously will be in the status of not using policy. In addition, if no policy name exists in the various policies, the **Delete** button will be disabled.
Remarks	Enter the remarks. Up to 128 multi-byte characters and 256 single-byte characters can be entered.

3. Set the security patch to be installed.

   For details on the setting method, refer to "6.2.3 Select security Patches to be Installed to Special PC".

4. Click the **Apply** button, and save the settings.

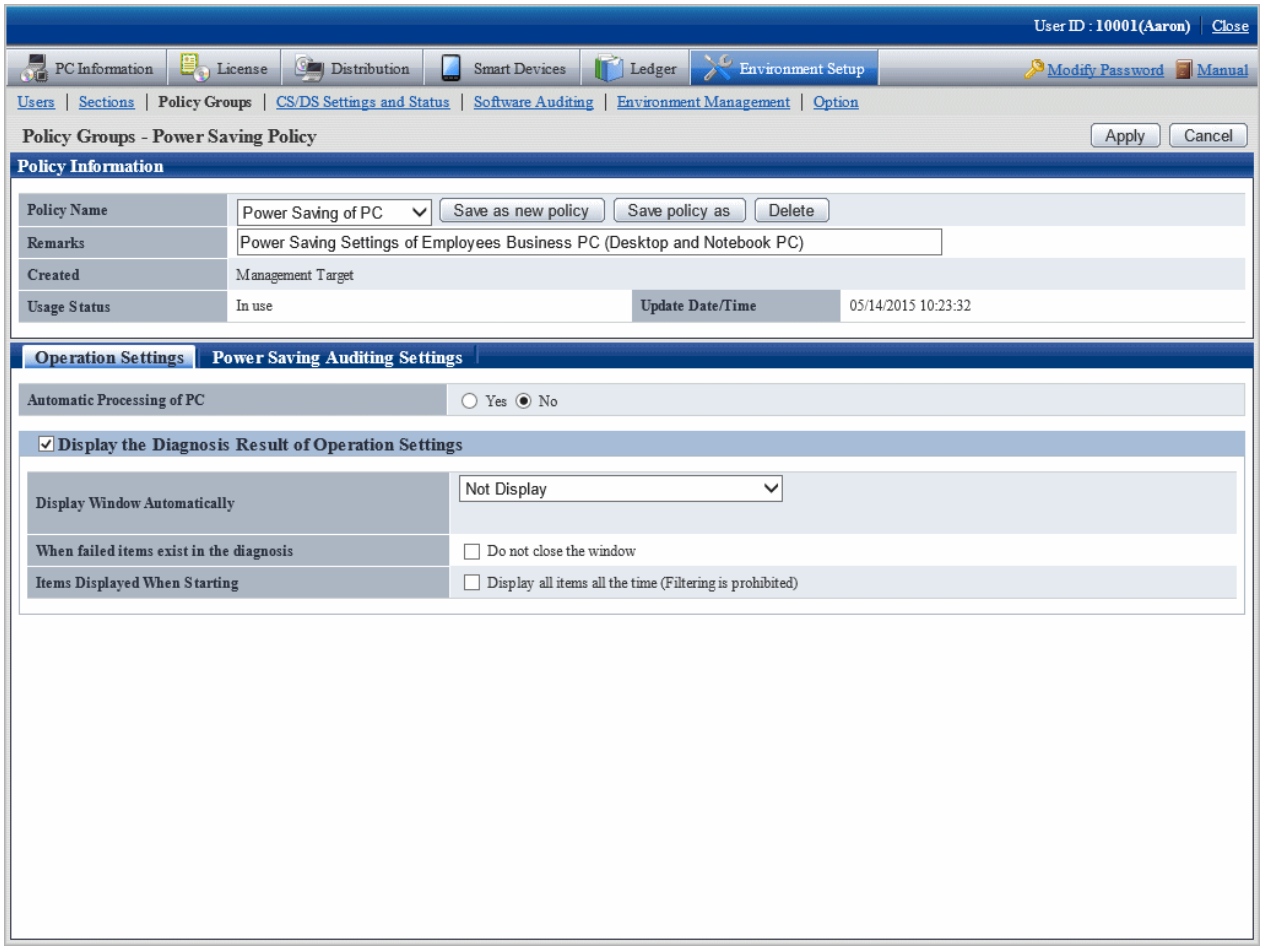
2.3.2.3 Customize Power Saving Policy

Customize the power saving settings.

The procedure is as follows.

1. In the **Customize various policies** window, click the **Power Saving Policy** tab.

   Click the link of policy name, the following window is displayed.



2. Enter the setting information.

Item	Description
Policy Name	The policy name of various policies can be selected from the list.
Save as new policy button	Register the content of various policies with new policy names. Up to 30 multi-byte characters or 60 single-byte characters can be entered in policy name. Characters can be specified are alphanumeric characters and the following single-byte symbols. ("-""@"".""(")""["]""{"}""<"">"":";")

Item	Description
Save policy as button	Modify the selected policy name. Characters can be specified are the same as **Save As**.
Delete button	Delete the policy selected from the list. After policy name has been deleted, the group that uses policy previously will be in the status of not using policy. In addition, if no policy name exists in the various policies, the **Delete** button will be disabled.
Remarks	Enter the remarks. Up to 128 multi-byte characters and 256 single-byte characters can be entered.

3. Set monitoring items.

   For details on the setting method, refer to "Chapter 4 Audit/Control PC Operational Configuration".

4. Click the **Apply** button, and save the settings.

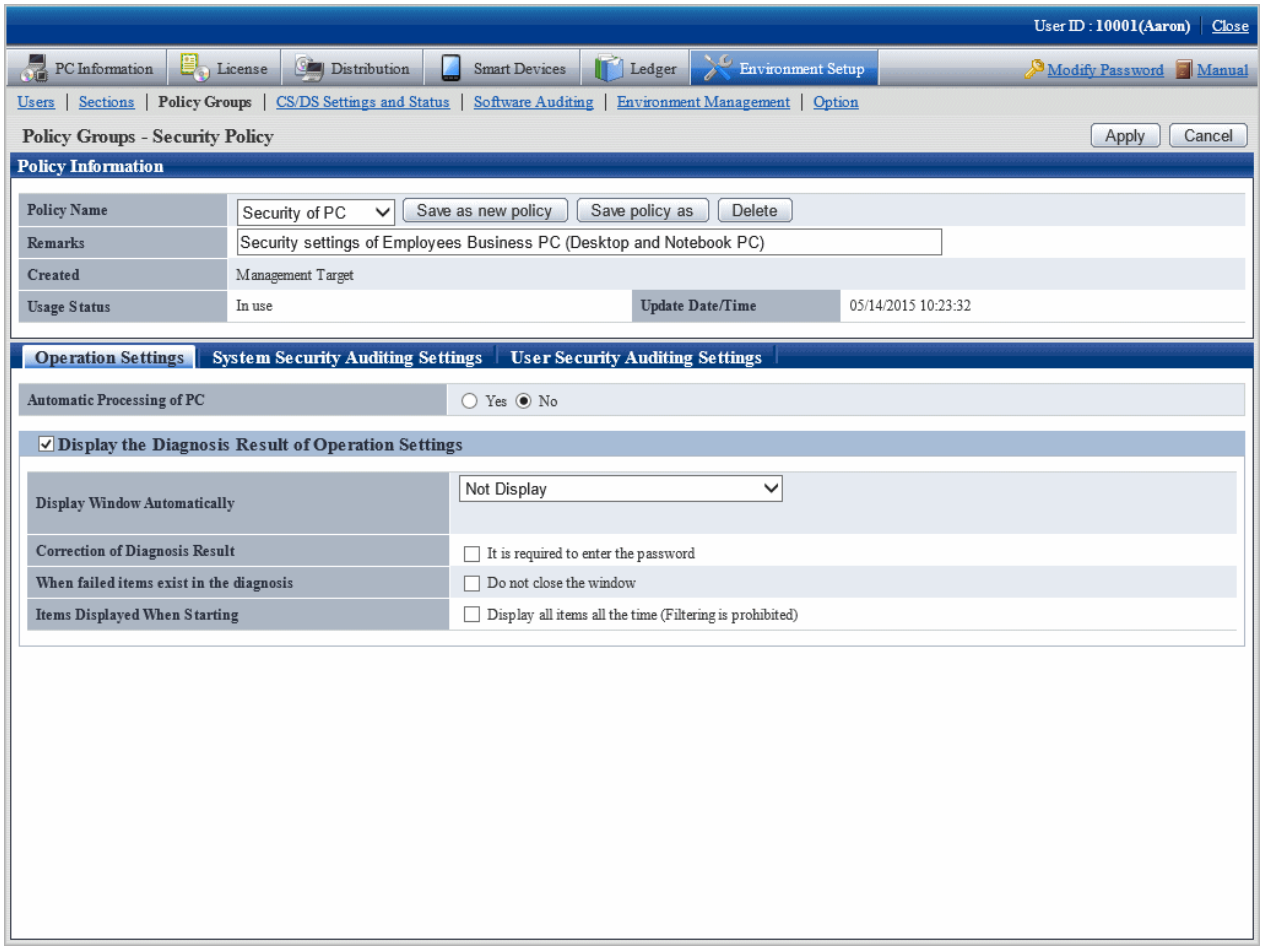
2.3.2.4 Customize Security Policy

Customize security policy.

The procedure is as follows.

1. In the **Customize various policies** window, click the **Security Policy** tab.

   Click the link of policy name, the following window is displayed.



2. Enter the setting information.

Item	Description
Policy Name	The policy name of various policies can be selected from the list.
Save as new policy button	Register the content of various policies with new policy names. Up to 30 multi-byte characters or 60 single-byte characters can be entered in policy name. Characters can be specified are alphanumeric characters and the following single-byte symbols. ("-""@"".""(")"["]"{"}"<">":";")
Save policy as button	Modify the selected policy name. Characters can be specified are the same as **Save As**.
Delete button	Delete the policy selected from the list. After policy name has been deleted, the group that uses policy previously will be in the status of not using policy. In addition, if no policy name exists in the various policies, the **Delete** button will be disabled.
Remarks	Enter the remarks. Up to 128 multi-byte characters and 256 single-byte characters can be entered.

3. Set monitoring items.

   For details on the setting method, refer to "Chapter 4 Audit/Control PC Operational Configuration".

4. Click the **Apply** button, and save the settings.

2.4 Import/Export Structure Information

If the operation environment does not link with Active Directory, Systemwalker Desktop Patrol and Systemwalker Desktop Keeper can link with structure information during initial installation. Structure information can be used to build an environment easily when a system is installed, eliminating the time and effort by system administrators.

This feature cannot be used if the operation environment links with Active Directory. In this case, **Environment Setup** > **Environment Management** is not displayed in the main menu.

Structure information can be used in the cases below. If structure information already exists in the import destination, it cannot be imported.

- When installing Systemwalker Desktop Patrol in an environment where Systemwalker Desktop Keeper is installed

  Import the structure information output by Systemwalker Desktop Keeper, and create structure information for Systemwalker Desktop Patrol.

- When installing Systemwalker Desktop Keeper in an environment where Systemwalker Desktop Patrol is installed

  Export Systemwalker Desktop Patrol structure information, and create structure information for Systemwalker Desktop Keeper.

Points to note

- Structure information can be linked with only during initial installation. Therefore, perform the following operations to link with structure information again.

  1. Download section management information
     Refer to the "Modify a registration" procedure in "2.1.4.3 Register through Uploading".

2. Delete the section using the CSV format file downloaded in step 1.
   Refer to the "New registration" procedure in "2.1.4.3 Register through Uploading", and select **Delete** in **Sections - Upload** > **Processing Option(s)** to upload.

3. Use **Import structure information** to import structure information for Systemwalker Desktop Keeper.

4. Update the section code of the user management information to the imported section code.
   Refer to "2.1.5 Create User Management Information" and update the section code.

- Structure information for Systemwalker Desktop Keeper and Systemwalker Desktop Patrol cannot be used cyclically.
  For example, structure information for Systemwalker Desktop Patrol cannot be reimported into Systemwalker Desktop Patrol after it was imported into and output from Systemwalker Desktop Keeper.

- When a single owner manages multiple PCs in Systemwalker Desktop Patrol (the same user ID is specified for CTs), CTs can be placed only in a single section based on the section code specified in Systemwalker Desktop Patrol even if the owner tries to have CT belong to multiple groups in Systemwalker Desktop Keeper.
  Systemwalker Desktop Keeper allows a single owner to have multiple CTs belong to multiple groups. However, if this structure information is imported into Systemwalker Desktop Patrol, all CTs will be placed in the section to which the owner belongs.

- When structure information output using Systemwalker Desktop Patrol is imported into Systemwalker Desktop Keeper, the section built in Systemwalker Desktop Patrol will be created in the Systemwalker Desktop Keeper Management Server. CTs are placed in the section imported from Systemwalker Desktop Patrol. A section that does not contain any CTs cannot be imported into Systemwalker Desktop Keeper.

Procedure

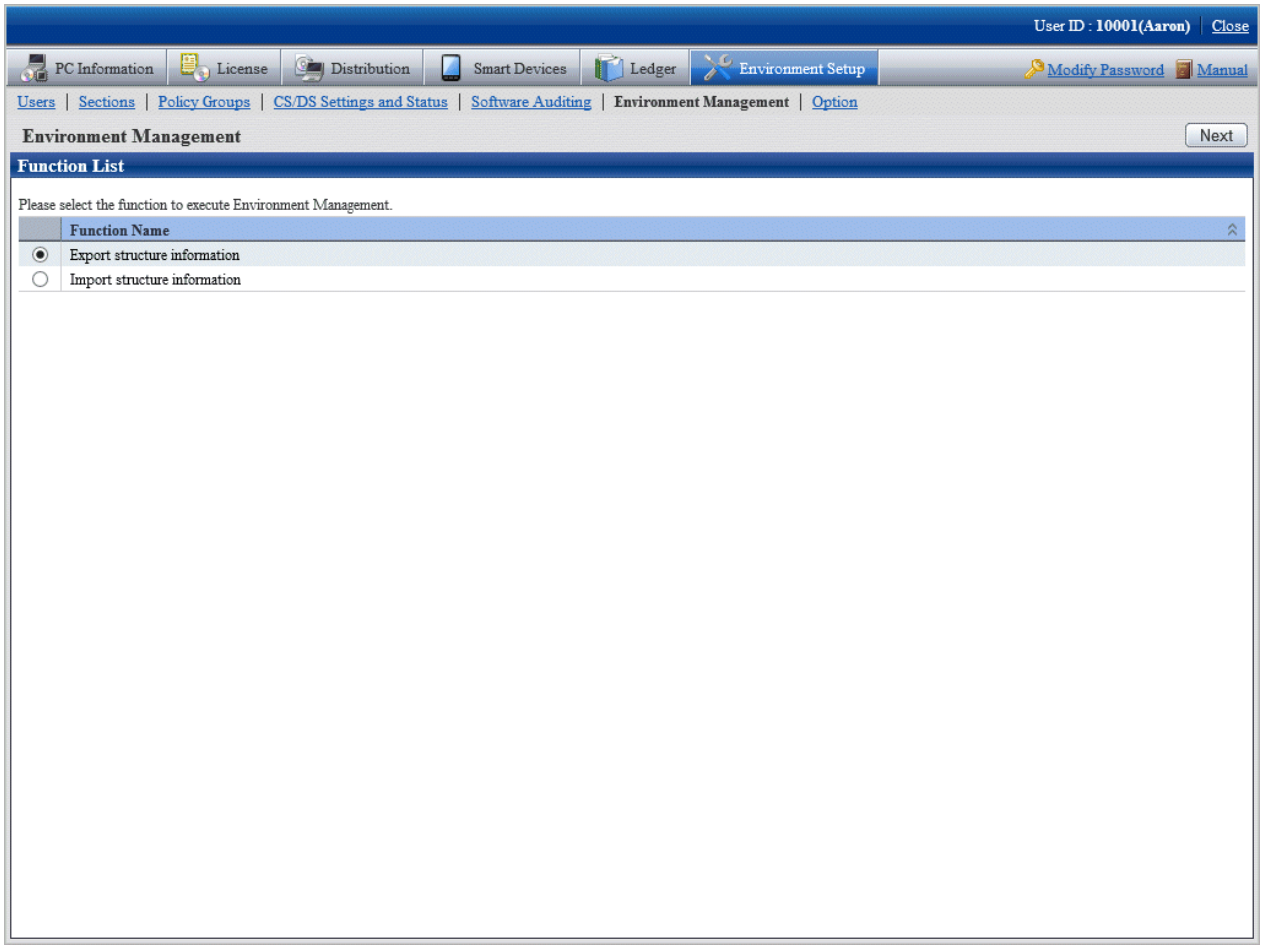
The procedure to import and export structure information is as follows.

1. Log in to the main menu and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Environment Management**.

   The following window will be displayed.



3. Select one of the option buttons and click **Next**.

   - Import structure information
   - Export structure information

4. The relevant window will be displayed.
   Refer to the following descriptions for details on the displayed window.

2.4.1 Import Structure Information

Import the structure information output by Systemwalker Desktop Keeper, and create structure information for Systemwalker Desktop Patrol.

The procedure is as follows.

Point

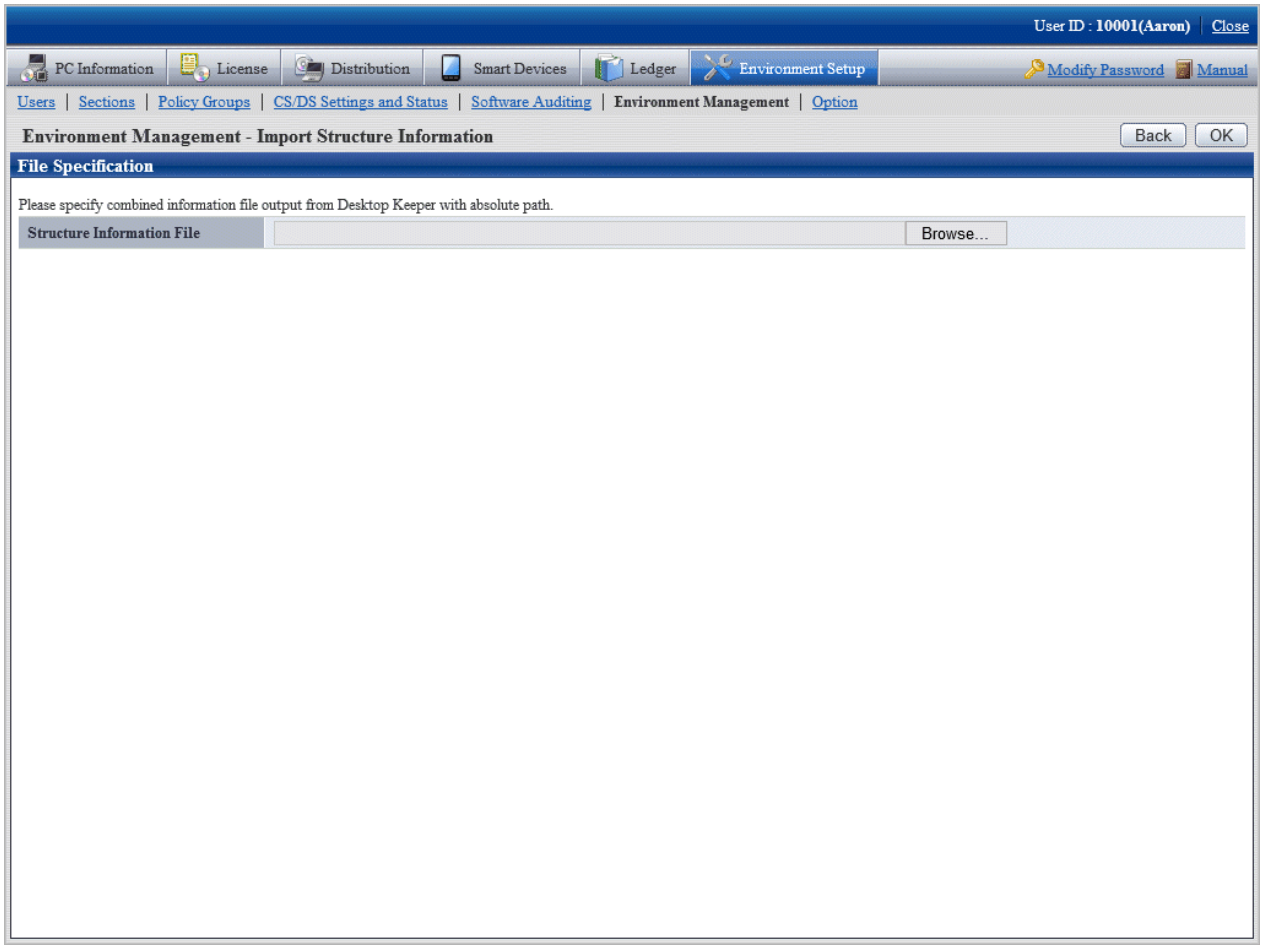
Section codes in Systemwalker Desktop Keeper structure information files can be clearly and easily edited as Systemwalker Desktop Patrol section codes.

Structure information files use the same format as Section Management Information CSV files. Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Take note of **Section Code** and **Higher Section Code** when editing so that the hierarchy structure matches Systemwalker Desktop Keeper.

1. Select **Import structure information** and click **Next**.

   The following window will be displayed.



2. Click **Browse**, specify the structure information file for Systemwalker Desktop Keeper, and then click **OK**.

   The import result will be displayed.

   Upon completion, the import completion message will be displayed.

   The imported structure information can be used as Systemwalker Desktop Patrol section management information.

   Create and register user management information and building management information by specifying the same "section code" used in the imported section management information.

Structure information import example

The example below illustrates importing Systemwalker Desktop Keeper structure information into Systemwalker Desktop Patrol.

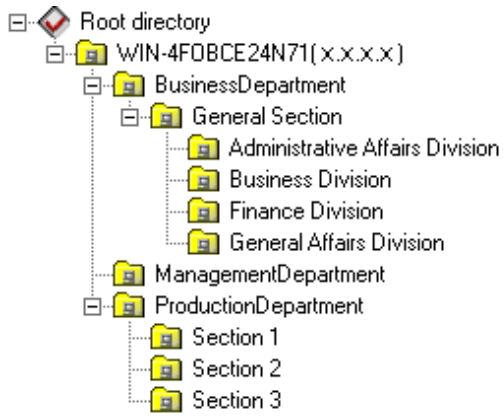
If Systemwalker Desktop Keeper is structured as shown below, the structure information imported into Systemwalker Desktop Patrol will be as follows:

Systemwalker Desktop Keeper structure information

```
Root
+ Management Server (DTK-MASTER)
+ Section A10 ..... PCA010, PCA011
+ Management department ..... PC0001
+ Management Server (DTK-1)
+ Section B10 ..... PCB010
+ Section B20 ..... PCB020, PCB021
```

+ Section B30 ..... PCB030, PCB031, PCB032
+ Section C10 ..... PCC010

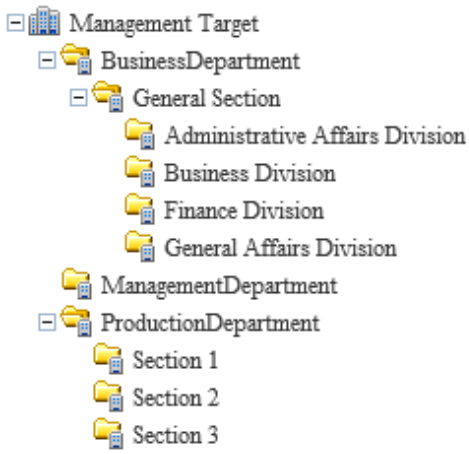
The following example shows a Systemwalker Desktop Keeper window.



Structure information imported into Systemwalker Desktop Patrol

Management target
+ Section A10 ..... PCA010, PCA011
+ Management department PC0001
+ Section B10 ..... PCB010
+ Section B20 ..... PCB020, PCB021
+ Section B30 ..... PCB030, PCB031, PCB032
+ Section C10 ..... PCC010

The following example shows a Systemwalker Desktop Patrol window.



2.4.2 Export Structure Information

Export Systemwalker Desktop Patrol structure information to be imported into Systemwalker Desktop Keeper.

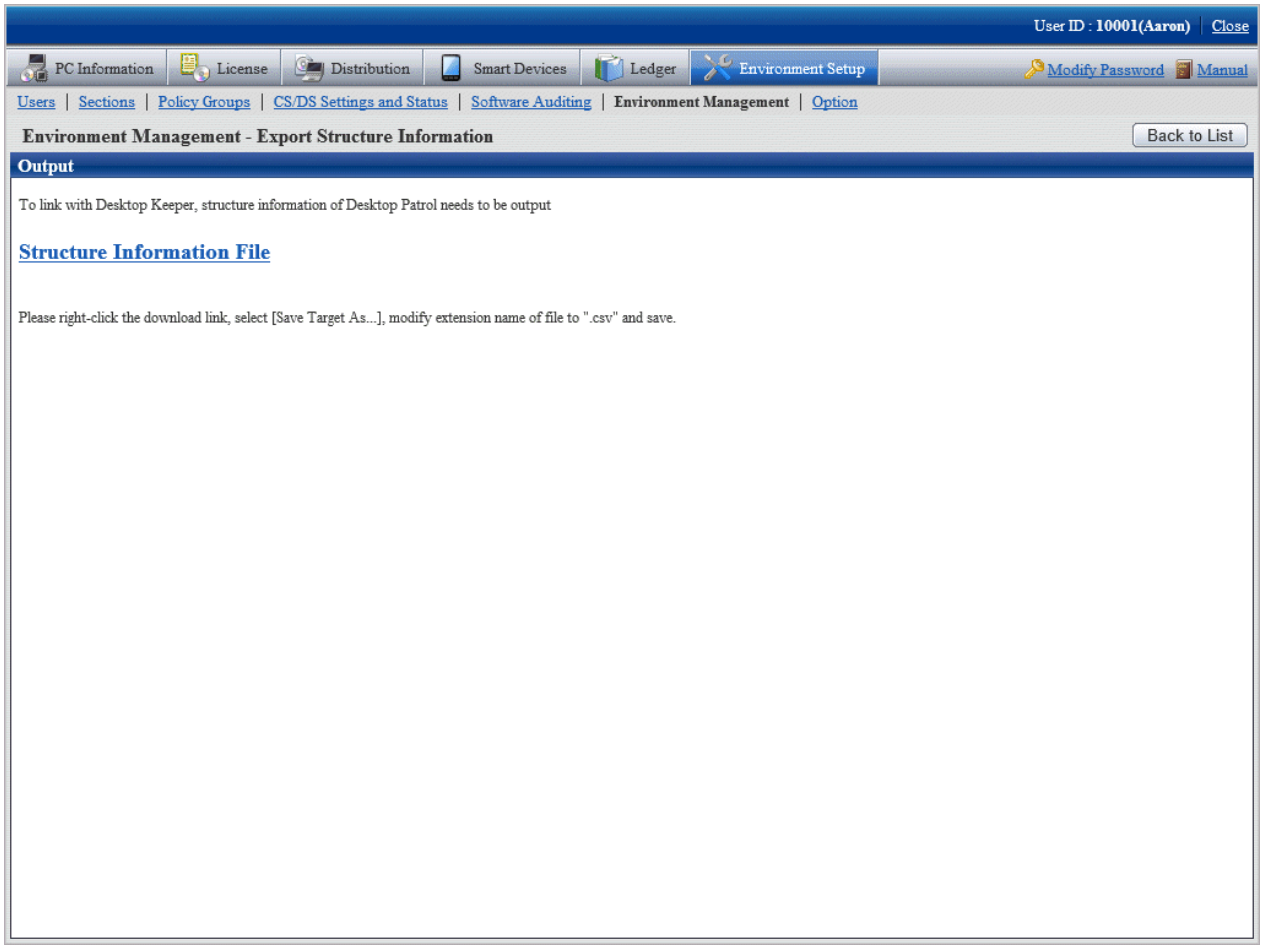
The procedure is as follows.

Point

The procedure below is not required when Systemwalker Desktop Patrol structure information import is automated in the Systemwalker Desktop Keeper settings.

1. Select **Export structure information** and click **Next**.

   The following window will be displayed.



2. Right-click the relevant structure information file that has a download anchor, and select **Save to a file** to save it to a file with the .csv extension.
   Refer to the Systemwalker Desktop Keeper manuals for details on how to import output structure information into Systemwalker Desktop Keeper.

Output in command

Systemwalker Desktop Patrol structure information can also be output using dtpinfcoope.exe (export structure information command).

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Structure information export example

The example below illustrates importing Systemwalker Desktop Patrol structure information into Systemwalker Desktop Keeper.

If Systemwalker Desktop Patrol is structured as shown below and no PC is found in "Section C10" (inventory not reflected), only the section the PC belongs to can be used for structure information, and "Section C10" will not be imported into Systemwalker Desktop Keeper.

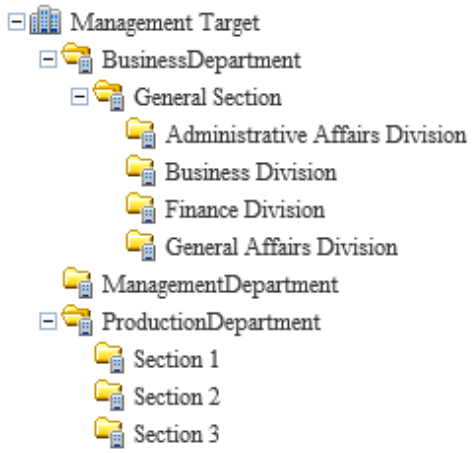
When structure information is imported into Systemwalker Desktop Keeper, the structure will be as follows:

Systemwalker Desktop Patrol structure information

```
Management target
+ Section A10 ..... PCA010, PCA011
+ Management department ..... PC0001
+ Section B10 ..... PCB010
+ Section B20 ..... PCB020, PCB021
```

+ Section B30 ..... PCB030, PCB031, PCB032
+ Section C10 ..... No PC

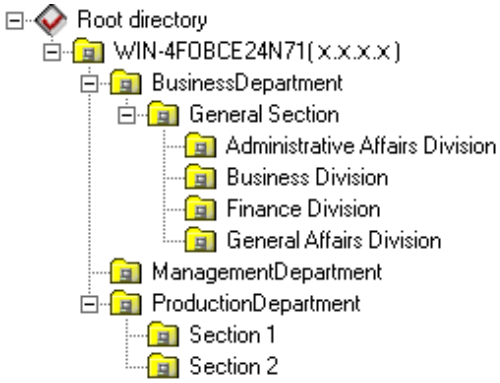
The following example shows a Systemwalker Desktop Patrol window.



Structure information imported using Systemwalker Desktop Keeper

Root
+ Management Server (DTK-MASTER)
+ Section A10 ..... PCA010, PCA011
+ Management department PC0001
+ Section B10 ..... PCB010
+ Section B20 ..... PCB020, PCB021
+ Section B30 ..... PCB030, PCB031, PCB032

The following example shows a Systemwalker Desktop Keeper window.



2.5 Set Alarm Notification

It is very difficult to manage the PC with CT installed one by one. In order to reduce the burden of administrator, information can be notified through E-mail.

In addition, during notification through E-mail, the file in CSV format with the following information can be added as attachment to the E-mail. For the format of CSV file, refer to *Systemwalker Desktop Patrol Reference Manual*.

- License violation information
- Information of user ID change
- Information of memory change
- Information of IP address change

- Information of network card change
- Information of disk change
- Information of drive capacity excess
- Monitoring of installed software
- Information registry change
- Information of Windows logon information change
- Information of product information addition and deletion

Note

- An alarm is not sent to unconfigured PCs.
  To send an alarm to these PCs, register the user of the unconfigured PC in the section, or move the user to the section.
- Due to differences in interpretation of the MIME protocol, CSV file attachments may be attached to the body of emails sent to the administrator and may not be displayed properly.

  You can remedy this phenomenon by changing the following settings:

  - File: *dtpInstallDir*\BNServ\data\dtp_config
  - Section: "MAILOPTION"
  - Key: "boundaryLineFeed"

  Setting example

  Example content of the *dtpInstallDir*\BNServ\data\dtp_config file

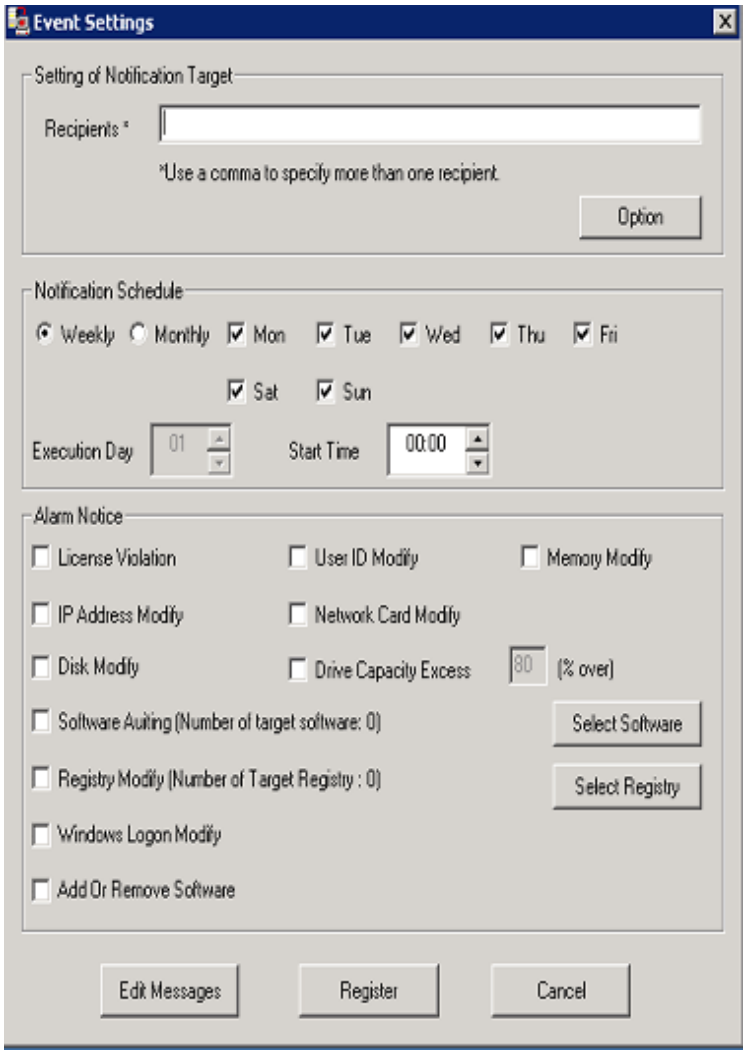
```
:
:
[MAILOPTION]
boundaryLineFeed=1
```

In the setting of alarm notification, authority of the Administrators group is required.

The procedure is as follows.

1. Select **Start** > **Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Event Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Event Settings** of CS.

   The **Event Settings** window is displayed.



2. Enter the following information, and click the **Register** button.

   In addition, when adding the file attachment with CSV format to the E-mail, select the check box of the item of **Alarm Notification**.

   [Input of Items]

Group	Item	Description
Setting of Notification Target	**Recipient** (required)	Specify the E-mail address of the receiving side of alarm notification. The number of characters can be specified is 2047 characters. When you need to enter multiple recipient addresses, separate them with comma.
Notification Schedule	**Weekly**	When **Weekly** is selected, put a check on the check box of the day of a week for E-mail sending and specify **Start Time**. After the check of the check box of all days of a week has been canceled, the alarm notification function will be stopped.

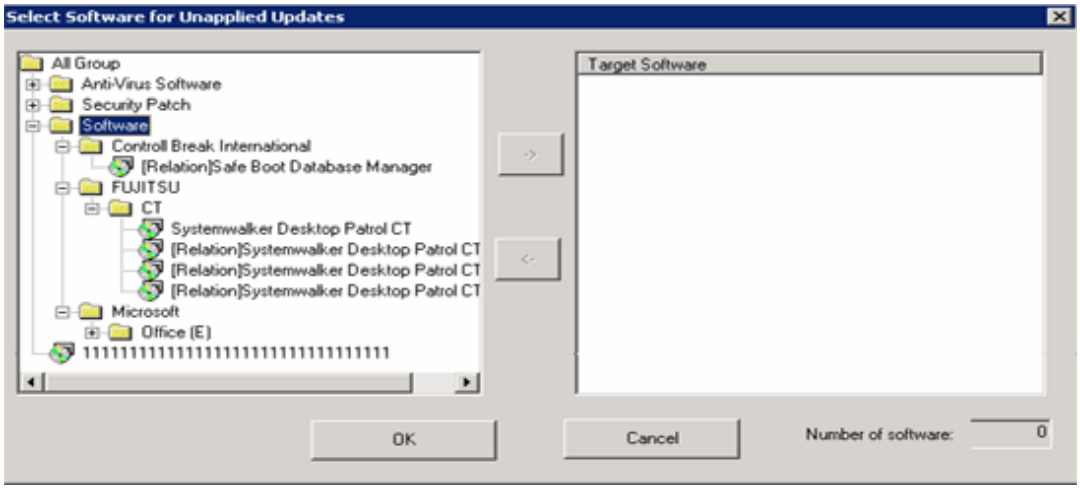
Group	Item	Description
	Monthly	When **Monthly** is selected, select the **Execution Date** of E-mail sending and specify **Start Time**.
Alarm Notice	**License Violation**	Notify the information of user that does not use licensed software.
	User ID Modify	When the user ID of PC is modified, the modification information will be notified.
	Memory Modify	When the memory of PC is changed, the change information will be notified.
	IP Address Modify	When the IP address of PC is modified, the modification information will be notified.
	Network Card Modify	When changing the network card of PC, the change information will be notified.
	Disk Modify	When changing the disk drive of PC, the change information will be notified.
	Drive Capacity Excess	Information will be notified when the usage of local disk drive of PC is beyond the specified value.
	Software Auditing	When the newly installed software is detected in the PC, relevant information will be notified. The definition of software to be monitored is defined in the **List of Target Software** window displayed after clicking the **Select Software** button. For details, refer to the following "Button Click".
	Registry Modify	When the change of value of the specified registry is detected, relevant information will be notified. In addition, click the **Select Registry** button and specify the registry value in the **Select the Registry Requires Modification Notification**. For details, refer to the following "Button Click".
	Windows Logon Modify	When modifying the logon name of PC, relevant information will be notified.
	Add Or Remove Software	When product information has been added or removed, relevant information will be notified.

[Button Click]

- **Option** button

  This button is not used in the alarm notification function.

- **Select Software** button



In the tree view on the left of window, the software set in **Environment Setup** > **Settings of Auditing Software** of the main menu will be displayed. Select the software that will use the alarm notification function.

- Alarm notification for PC in which security patch is not installed

  Select the information of security patch not installed to perform alarm notification.

- Alarm notification for PC in which the version of virus pattern file has expired

  Select the virus pattern file of alarm notification.

- Alarm notification for PC in which the prohibited software is installed

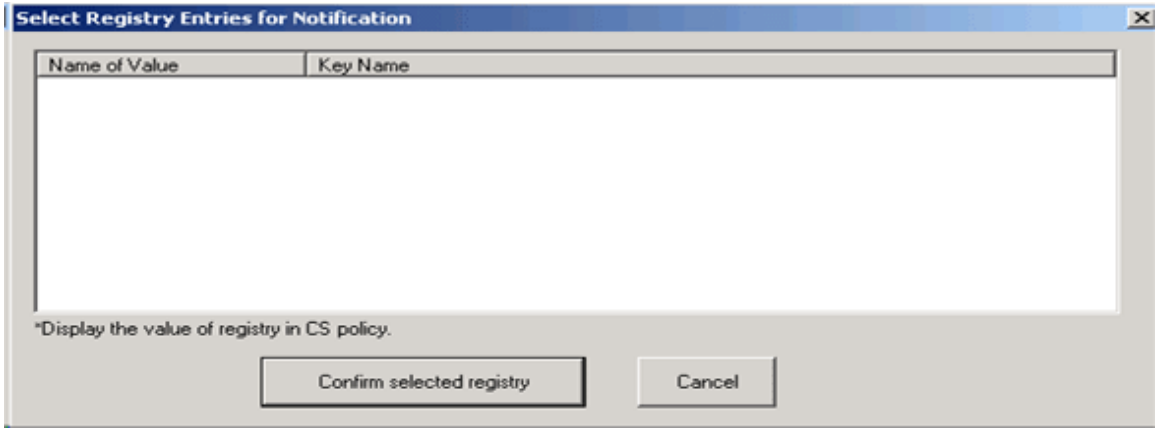
  Select the software prohibited being installed to perform alarm notification.

In addition, every time when the software dictionary is updated, software will be added. If the alarm notification function is to be used for the added software, it is required to select from each category after the software dictionary has been updated. For settings of software dictionary, refer to "2.2 Set Auditing Software".

Select the software specified in **SoftwareAuditing**, click the -> button in the center of window.

After all registration has completed, click the **OK** button.

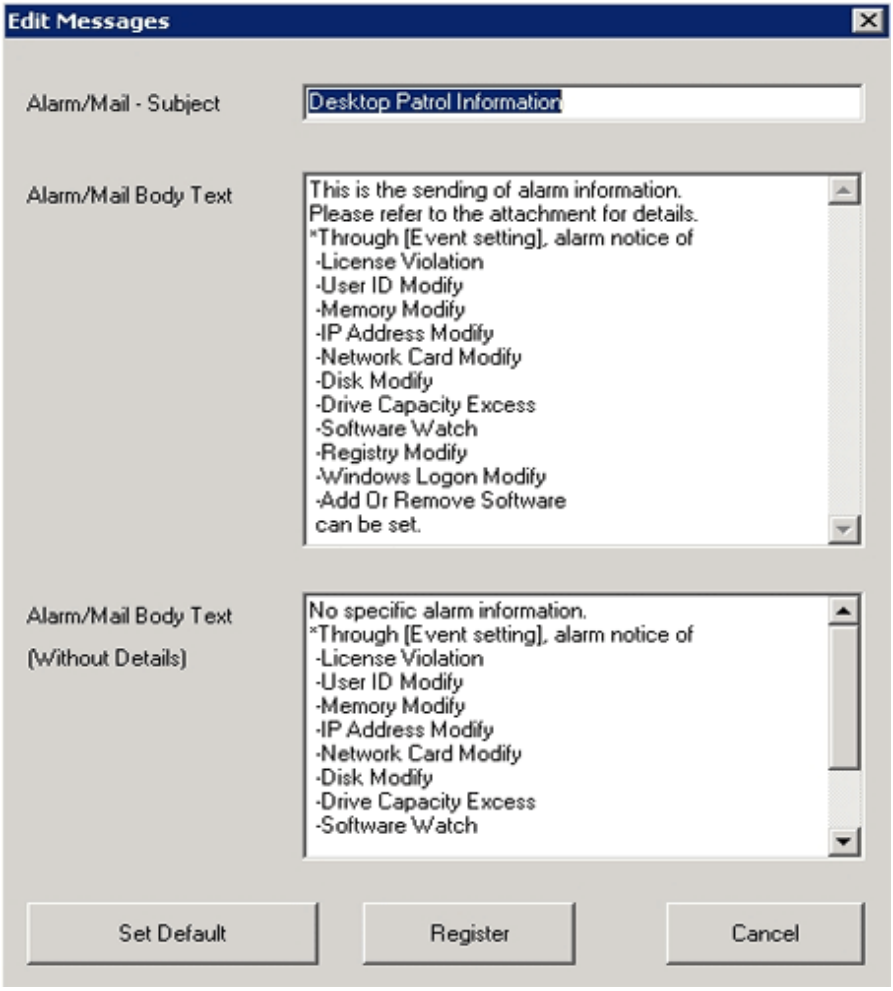
- **Select Registry** button



In the window, the registry value registered in **Policy Groups** is displayed. For settings of registry value, refer to "3.1.1 Perform Operation Settings of Client".

Put a check on the check box, and the item will become the alarm notification target.

- **Edit Messages** button



Item	Description
Alarm/Mail - Subject	Enter the email subject. Use up to 5,120 characters.
Alarm/Mail Body Text	Enter the email body to be sent when alarm information is generated. Use up to 5,120 characters.
Alarm/Mail Body Text (Without Details)	Enter the email body to be sent when no alarm information is generated. Use up to 5,120 characters.

3. When sending E-mail, set through **Environment Setup** > **Options** > **E-mail Environment Settings** of the main menu.

   This setting can only be performed by system administrator.

Item		Description
Settings of SMTP Server	**Server Name**	Set the E-mail server name used by alarm notification function. Specify up to 127 halfwidth characters.
	Port number	Set the port number to be used within 0~65535. If the port number is not entered, Port No. 25 will be set automatically. In addition, if the specified value exceeds the above range, or an incorrect port number is specified, error will occur.
	Authentication method	Select **Do not Authenticate**, **Determine Automatically**, **CRAM-MD5**, **LOGIN**, **PLAIN** as authentication method. The default value is **Do not Authenticate**. If **Determine Automatically** is selected, the authentication method will be determined automatically according to the following sequence. 1. CRAM-MD5 2. PLAIN 3. LOGIN
	User ID	Enter the user ID used in the selected authentication method. Enter no more than 64 single-byte alphanumeric characters and the halfwidth symbol "@". If you omit this item even though you selected the authentication mode, an error will occur.
	Password	Enter the password used in the selected authentication method. Enter no more than 64 single-byte alphanumeric characters.
E-mail Sender		Specify the E-mail address of sender of alarm notification. Use up to 63 fullwidth or 127 halfwidth characters.

2.6 Control Executable file

In order to prohibit illegal use of software, after particular software has been detected, warning and prohibition will be executed. If the software contains window, execution can be prohibited through registering the executable file name to Systemwalker Desktop Patrol in advance.

For example, the operation of warning and prohibition is performed when the software that has nothing to do with business such as game and free software is executed.

In addition, when the following executable file is detected, warning and prohibition cannot be performed for the execution of this file.

- Software without fixed file name
- Program of Windows service

In addition, when Systemwalker Desktop Patrol and Systemwalker Desktop Keeper are coexisting, use the function of Systemwalker Desktop Keeper for execution prohibition of executable file.

When distributing software, pay attention to the following.

- When distributing software to CT, the executable file to be started can be specified. However, if this executable file has been set as prohibited software, this software cannot be distributed.

2.6.1 Settings

After setting the control of executable file, if the specified software is executed at client, the following operations can be performed.

- Notify detection message to client
- Notify warning message to client
- Prohibit execution of software out of business such as games

Set the detection and prohibition of executable file according to the following procedure.

1. Set executable file and message
2. Set software operation status collection
3. Application of client policy
4. Log on CT again

2.6.1.1 Set Executable File and Message

Specify the detection settings of executable file on client PC and the executable file that is warned/prohibited being used in client. In addition, specify the message to be displayed when the executable file is started.

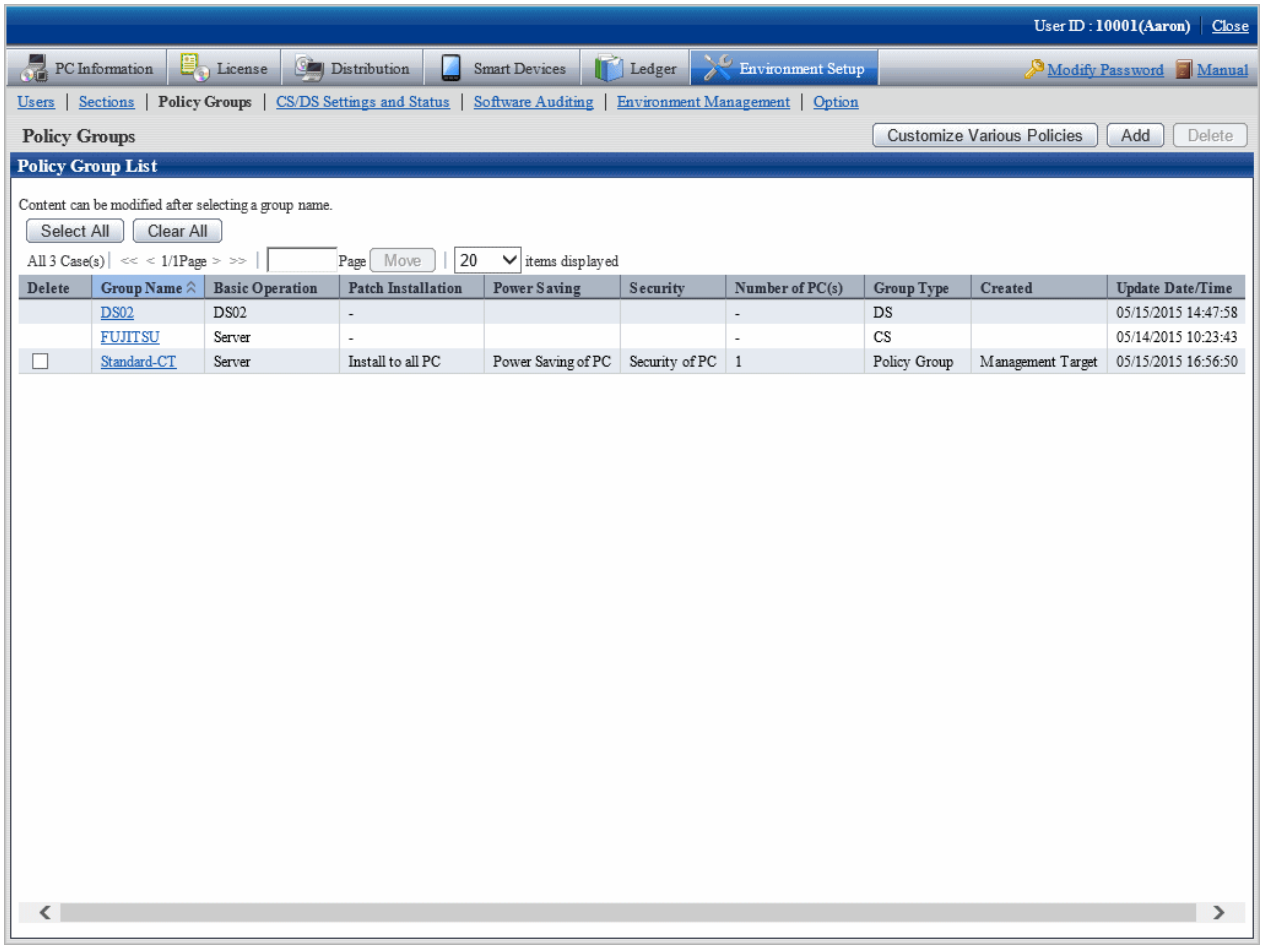
The procedure is as follows.

1. Login to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

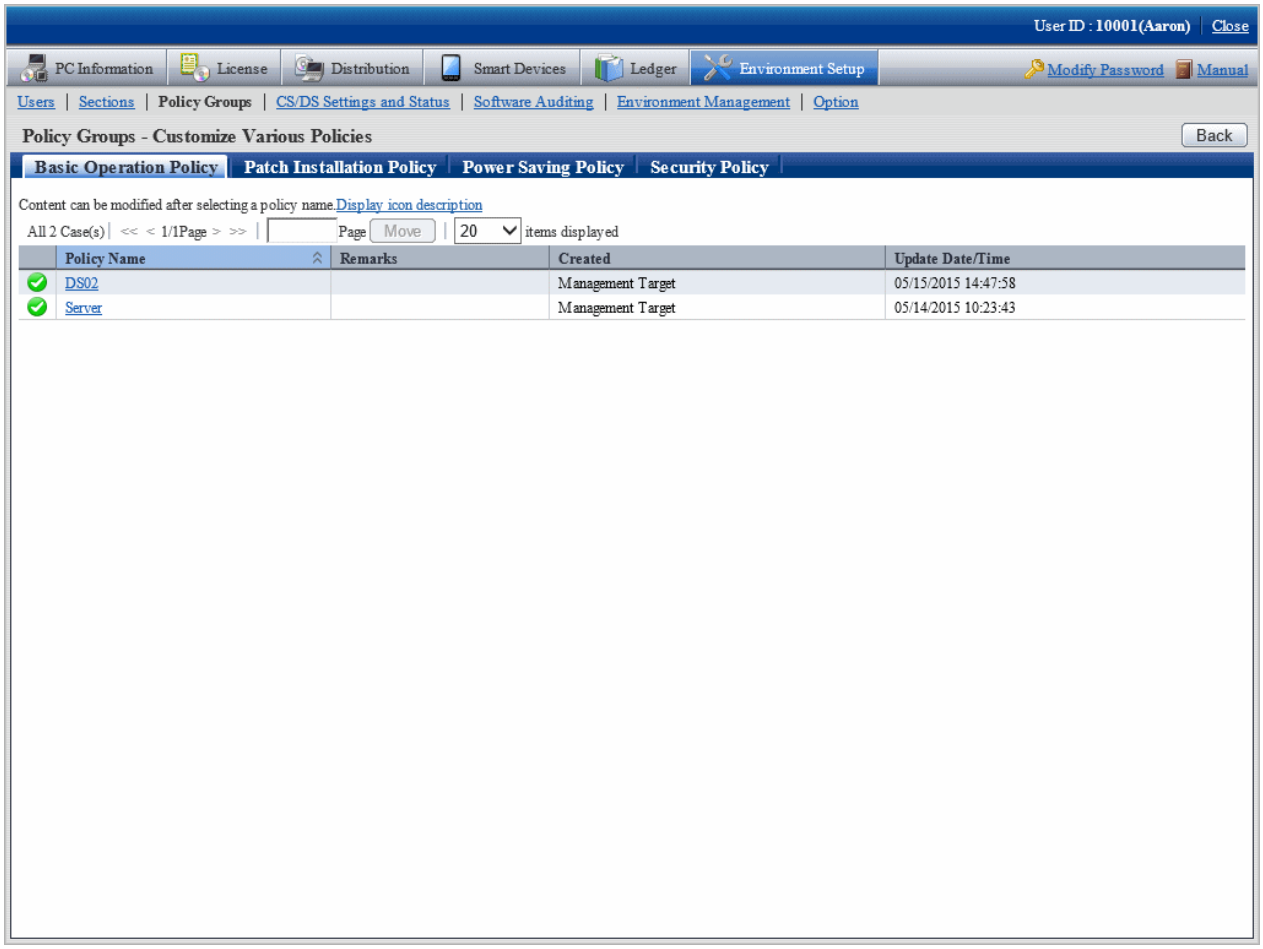
2. Click **Policy Groups**.

   The following window is displayed.



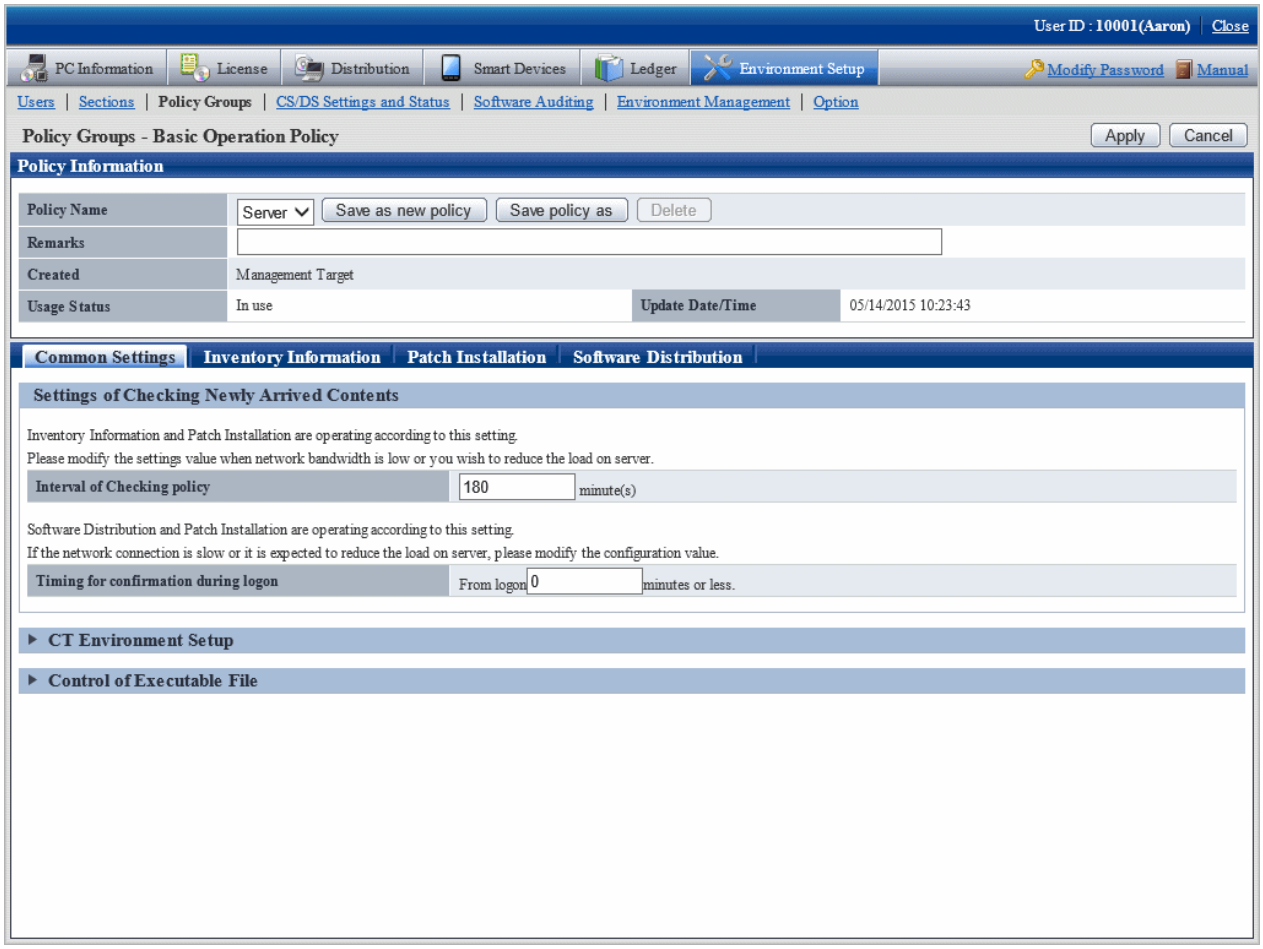
3. Click the **Customize various policies** button.

   The following window is displayed.



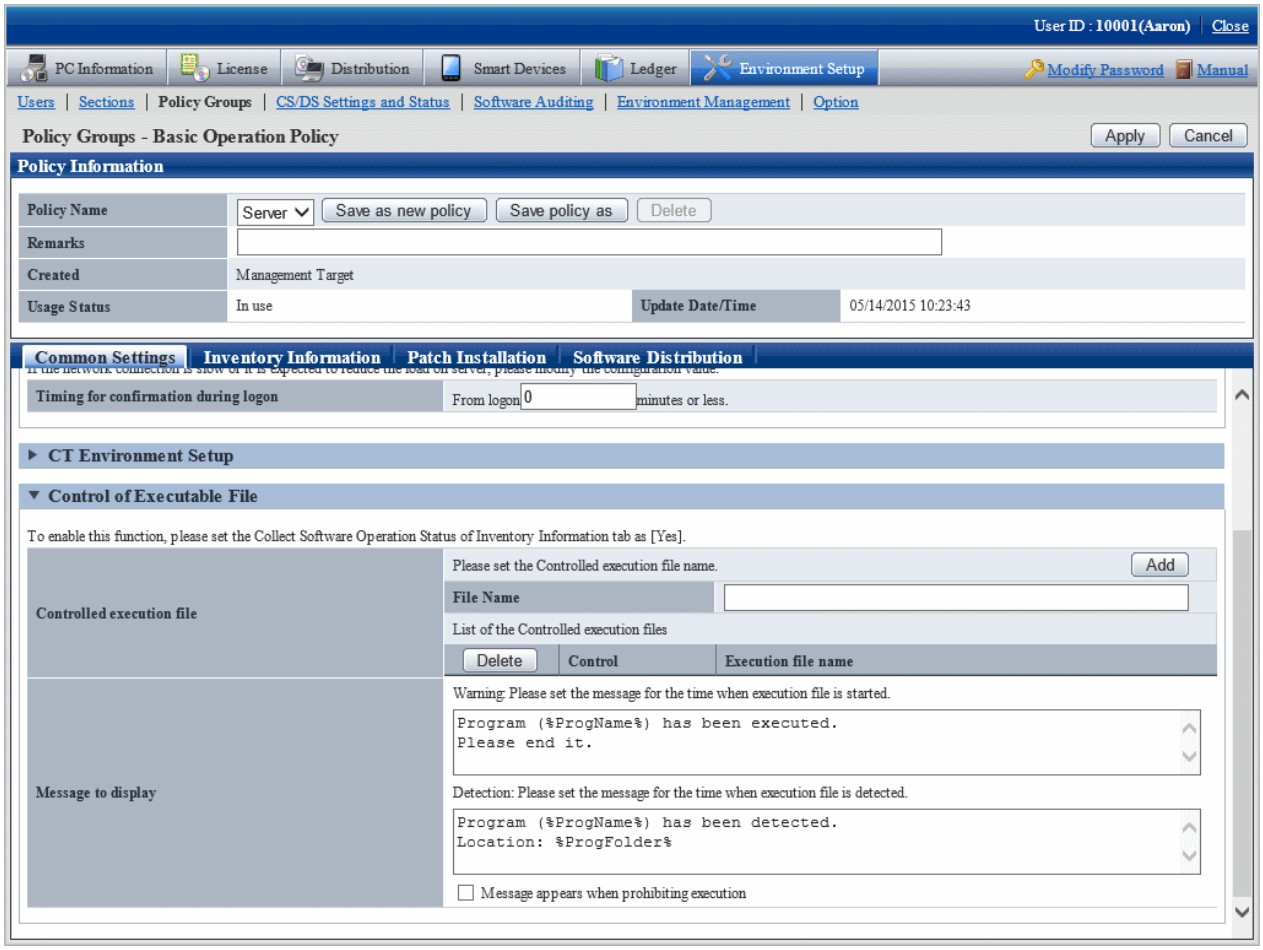
4. Select the **Basic Operation Policy** tab, and click the link of policy name.

   The following window is displayed.



5. Click the **Common settings** tab.

   Click **Control of Executable File**, and the following items will be displayed.



Item	Description
File Name	Specify the name of the file for execution control using up to 129 fullwidth characters or 259 halfwidth characters. The last four characters must be ".exe".
Add button	One line of the field for which the control of executable file can be specified will be added.
Delete button	Delete the control of executable file specified at the line of deletion button.
Control (Note 1)	Select the control. - **Warning** Display the message when the executable file is started. The message content is specified in **Warning**. - **Execution Prohibition** When the executable file is started, exit it by force. When displaying message at the time when execution is prohibited, select **Display message when execution is prohibited** and specify the message content. - **Detection and Warning** Display message when the executable file is detected and when the executable file is started. Specify the message content in **Detection** and **Warning**.

Item	Description
	- **Detection and Execution Prohibition** Display a message when the executable file is detected, and exit the executable file by force when it is started. Specify the message displayed at detection in **Detection**. When message needs to be displayed at execution prohibition, select **Display message when execution is prohibited** and specify the message content.
Message to display (Note 2)	Specify the message to be displayed when the executable file is started using up to 512 fullwidth characters or 1024 halfwidth characters. It cannot be omitted. After (%ProgName%) is recorded in the text of message, when the software specified in the executable file name is started, the executable file name will be displayed.
	Specify the message to be displayed when the executable file is detected using up to 512 fullwidth characters or 1024 halfwidth characters. It cannot be omitted. After (%ProgName%) is recorded in the text of message, when the software specified in the executable file name is started, the executable file name will be displayed. In addition, after (%ProgName%) is recorded, the folder name where the detected file is located will be displayed in message text.
	When displaying message at the time when the start of executable file is prohibited, select "Display message when execution is prohibited" and specify message content using up to 512 fullwidth characters or 1024 halfwidth characters. It cannot be omitted. After (%ProgName%) is recorded in the text of message, when the software specified in the executable file name is started, the executable file name will be displayed.

Note 1)

Same executable file name cannot be specified in **Warning** and **Execution Prohibition**.

In inventory collection, when the executable file on client PC is detected, the detection message will be displayed.

The detection message will be displayed in the information at every time of inventory collection until uninstallation.

Note 2)

The following variables can be used in messages.

- %ProgName%

  Display the detected file name in the text of message. This variable can be used in the following messages.

  - Warning message
  - Detection message
  - Execution prohibition message

- %ProgFolder%

  The folder name where the detected file is located will be displayed in the text of message. This variable can be used in the following messages.

  - Detection message

6. Confirm settings and click the **Apply** button.

   The settings are saved.

Note

For detection of executable fie, only the following fixed drives will be detected.

- Built-in hard disk

- Network connection hard disk using the "NDAS" technology
- Part of USB connected hard disk (Note)

However, the executable file in the **Recycle Bin** of Windows cannot be detected. However, the executable files exist in the folder within the **Recycle Bin** of Windows can be detected.

Note) The conditions of USB connection hard disk that can be detected are as follows.
Select this drive in Windows Explorer, select **Type** of the **General** tab in the hard disk properties window displayed in **File** > **Properties**, and the hard disk displayed as **Local Disk** here can be detected.

2.6.1.2 Set the Collection of Software Operation Status

In order to perform warning and execution prohibition of the start of executable file, it is required to specify the software operation status collection to **Yes** in the collection conditions of client policy. In addition, when the executable file can be detected only, this setting is not required.

Check in the main menu about whether the software operation status collection has been set.

Settings of Collected Items of **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** tab > **Inventory Information** tab of the main menu.

2.6.1.3 Apply Client Policy

When information in "2.6.1.1 Set Executable File and Message" and "2.6.1.2 Set the Collection of Software Operation Status " mentioned above is set to CT when the client policy is applied.

The client policy is applied according to the schedule set in the main menu. For schedule, confirm in the main menu.

Settings of Collection Schedule of **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** tab > **Inventory Information** tab of the main menu

2.6.1.4 Log on CT Again

The setting of "2.6.1.1 Set Executable File and Message" and "2.6.1.2 Set the Collection of Software Operation Status " mentioned above will be effective when log on to the PC again after the client policy has been applied to CT.

Log on to each PC again at the timing when operation starts.

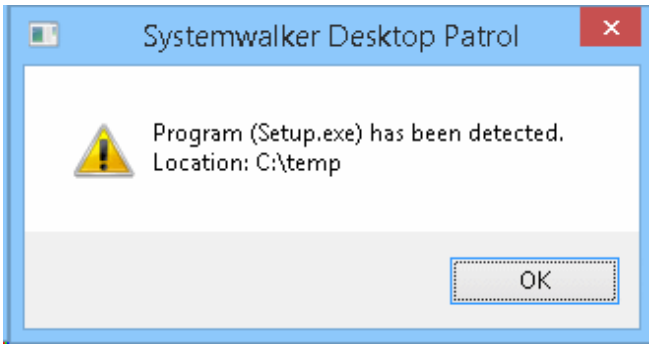
2.6.2 Operation

After the setting of control of executable file has completed, operation can be started.

After the specified executable file has been detected on CT, a message window will be displayed at CT side.

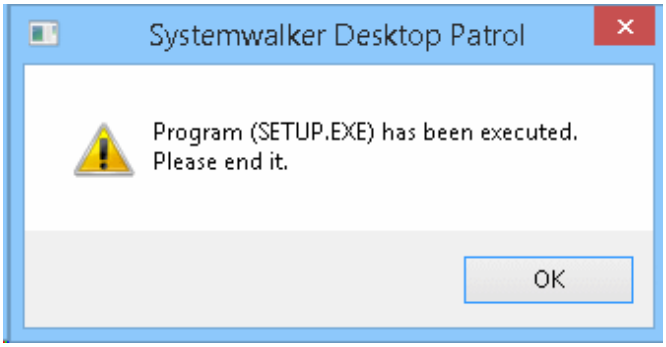
Following are the example of detection message, warning message and execution prohibition message.

[Detection message]



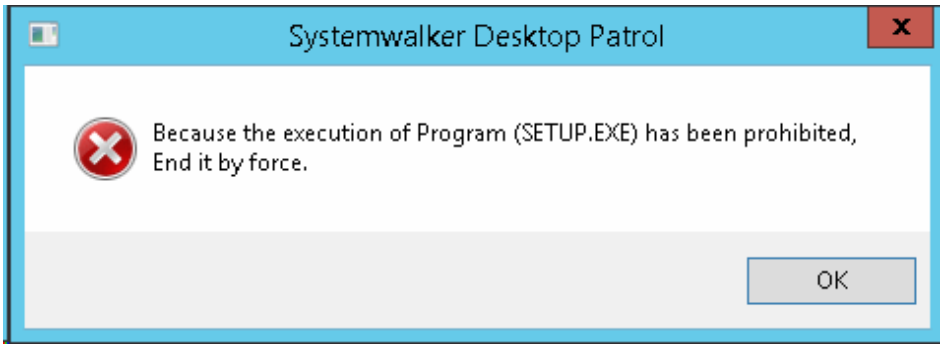
*The displayed message varies according to settings.

[Warning message]



*The displayed message varies according to settings.

[Execution prohibition message]



*The displayed message varies according to settings.

Chapter 3 View PC Information

This chapter describes how to view PC information collected from CT.

3.1 Settings Performed as Needed

Right after installing CS and DS, collection of PC information will be set to be performed according to the policy set in CS or DS.

The content to be set and setting method are described as follows.

Operation settings of client

For collection condition of PC information, the setting method on each PC is as follows.

Setting Content	Setting Method
Settings of Inventory Collection Condition	**Environment Setup** > **Policy Groups**
Settings of File Collection	**Environment Setup** > **Policy Groups**
Settings of Registry Collection Condition	**Environment Setup** > **Policy Groups**
Settings of Collection Condition of Software Operation Status	**Environment Setup** > **Policy Groups**

Operation settings of entire system

For the collection condition of PC information, the method of setting as the operation of the entire system is as follows.

Setting Content	Setting Method
Settings of User Information	**Environment Setup** > **Option**
Settings of Software Dictionary	**Environment Setup** > **Settings of Auditing Software**

In addition, the following settings are required.

Settings of inventory collection using command mode CT

In mobile PC disconnected from network or the network with low speed, perform the setting of inventory collection by command mode CT.

Settings of PC operation management

For PC as operation management target, to perform power operation and immediate collection of inventory information (hardware information], perform the setting of PC operation management.

Settings related to display of operation status

To modify the display content related to the display of operation status, perform the following settings.

Setting Content	Setting Method
Modify the settings of display content related to the display of operation status	**Environment Setup** > **Option** > **Status Related Settings**

Settings related to operation processing

To modify the settings related to operation processing, perform the following settings.

Setting Content	Setting Method
Modify the settings related to operation processing	**Environment Setup** > **Option** > **Settings Related to Processing**

3.1.1 Perform Operation Settings of Client

This section describes the settings of collection condition of PC information.

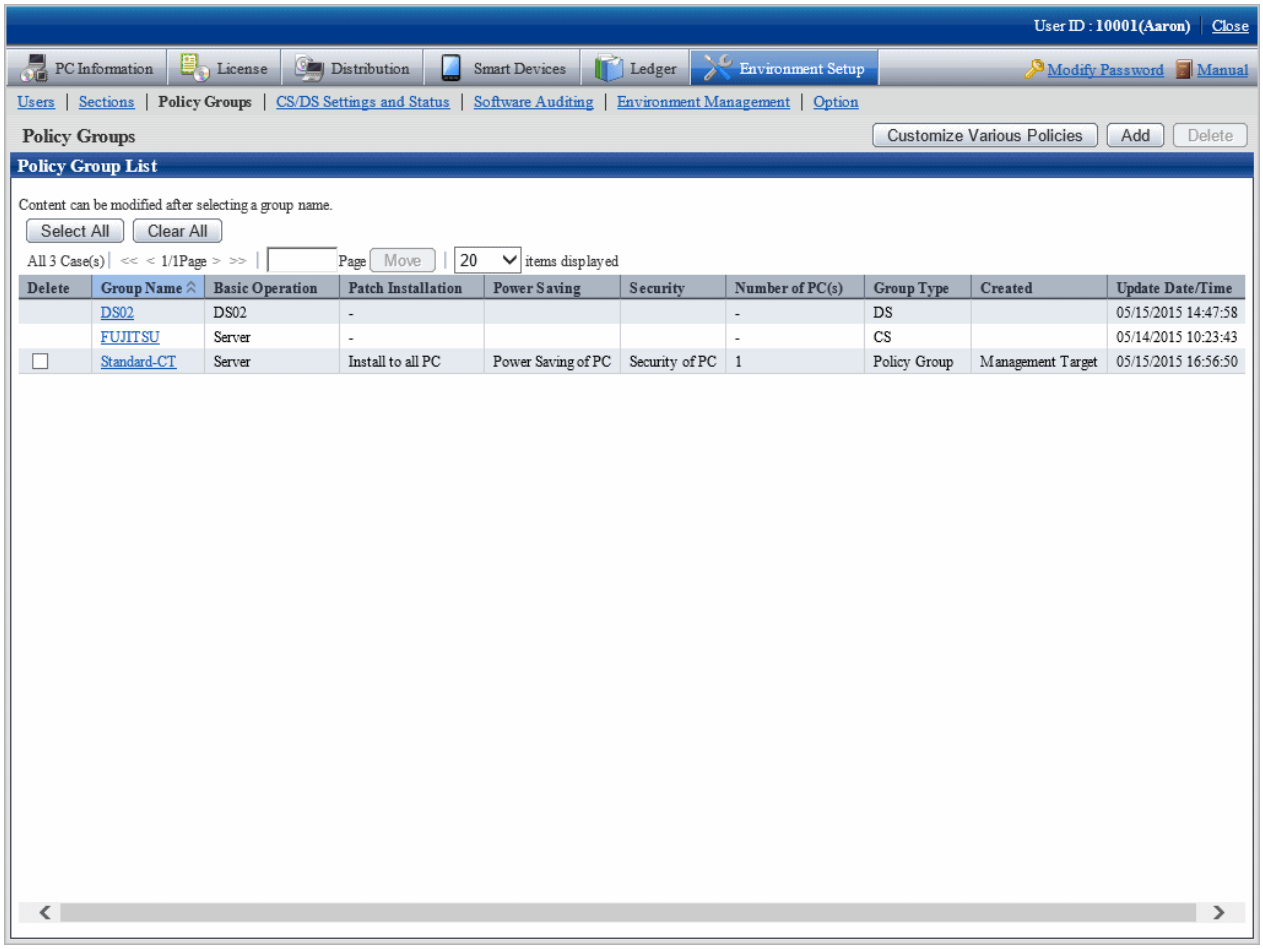
The operation procedure is as follows.

1. Log in to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

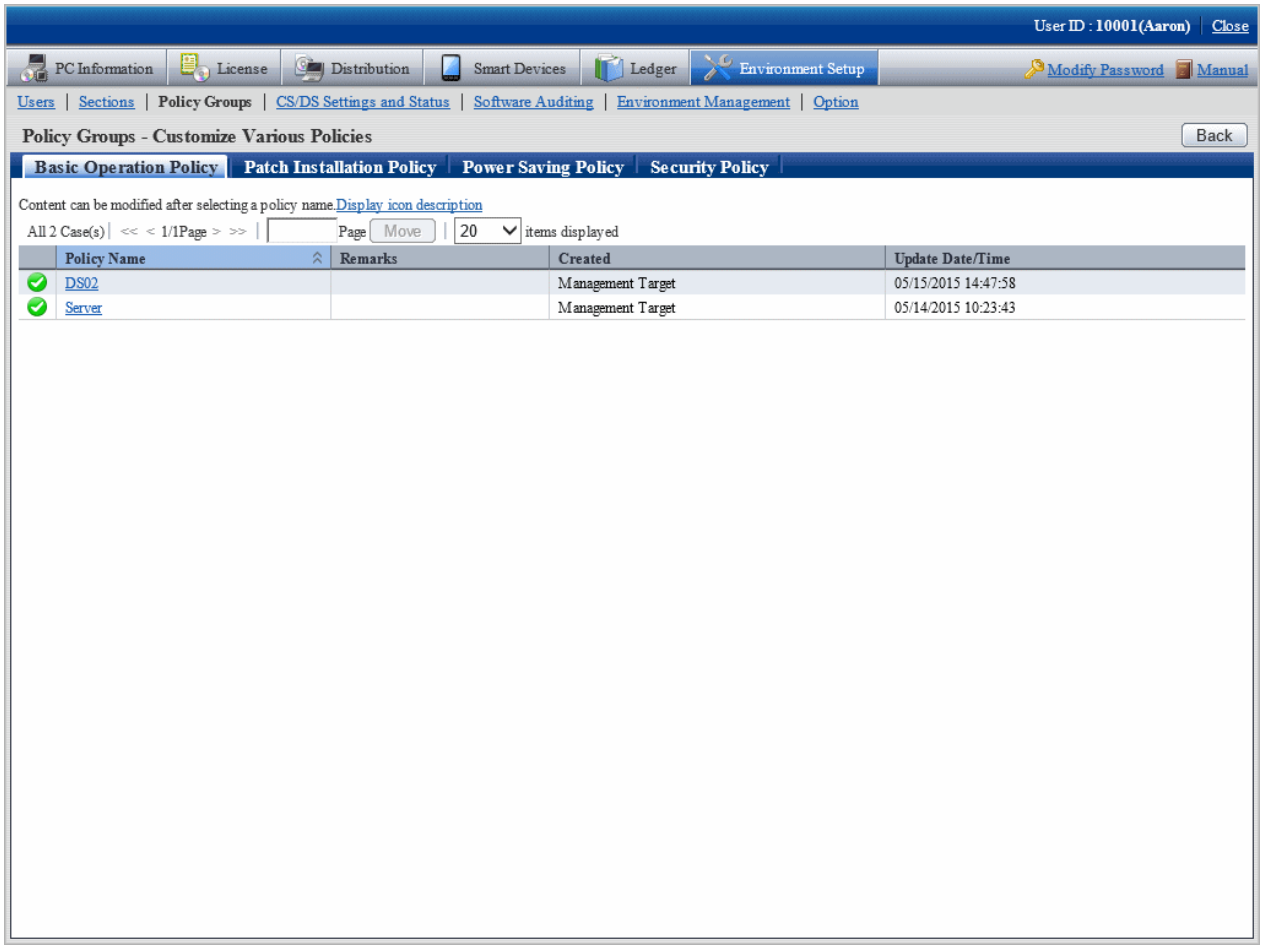
2. Click **Policy Groups**.

   The following window will be displayed.



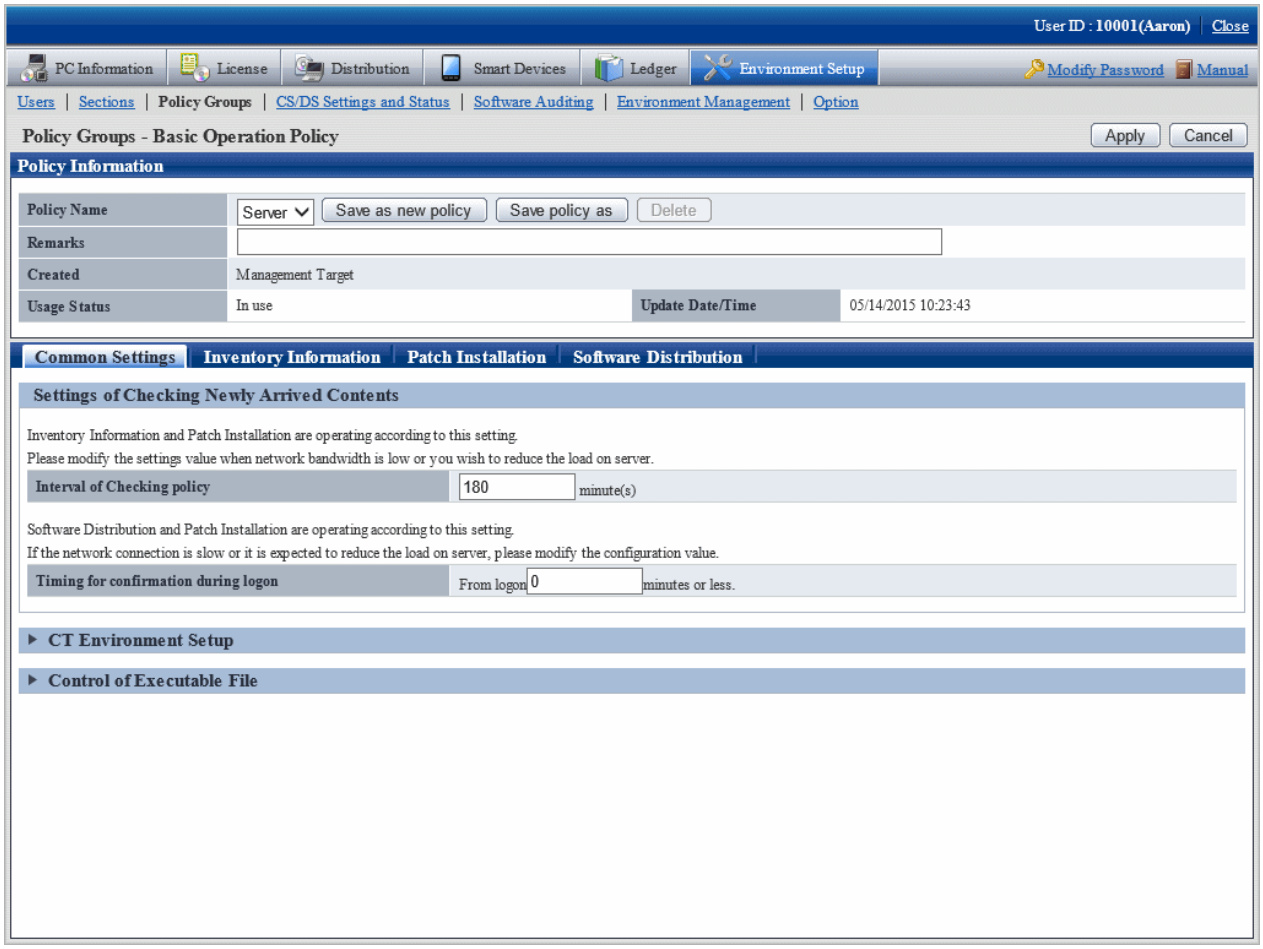
3. Click the **Customize Various Policies** button.

   The following window will be displayed.



4. Click the **Basic Operation Policy** tab.

   After clicking the link of policy name, the following window will be displayed.



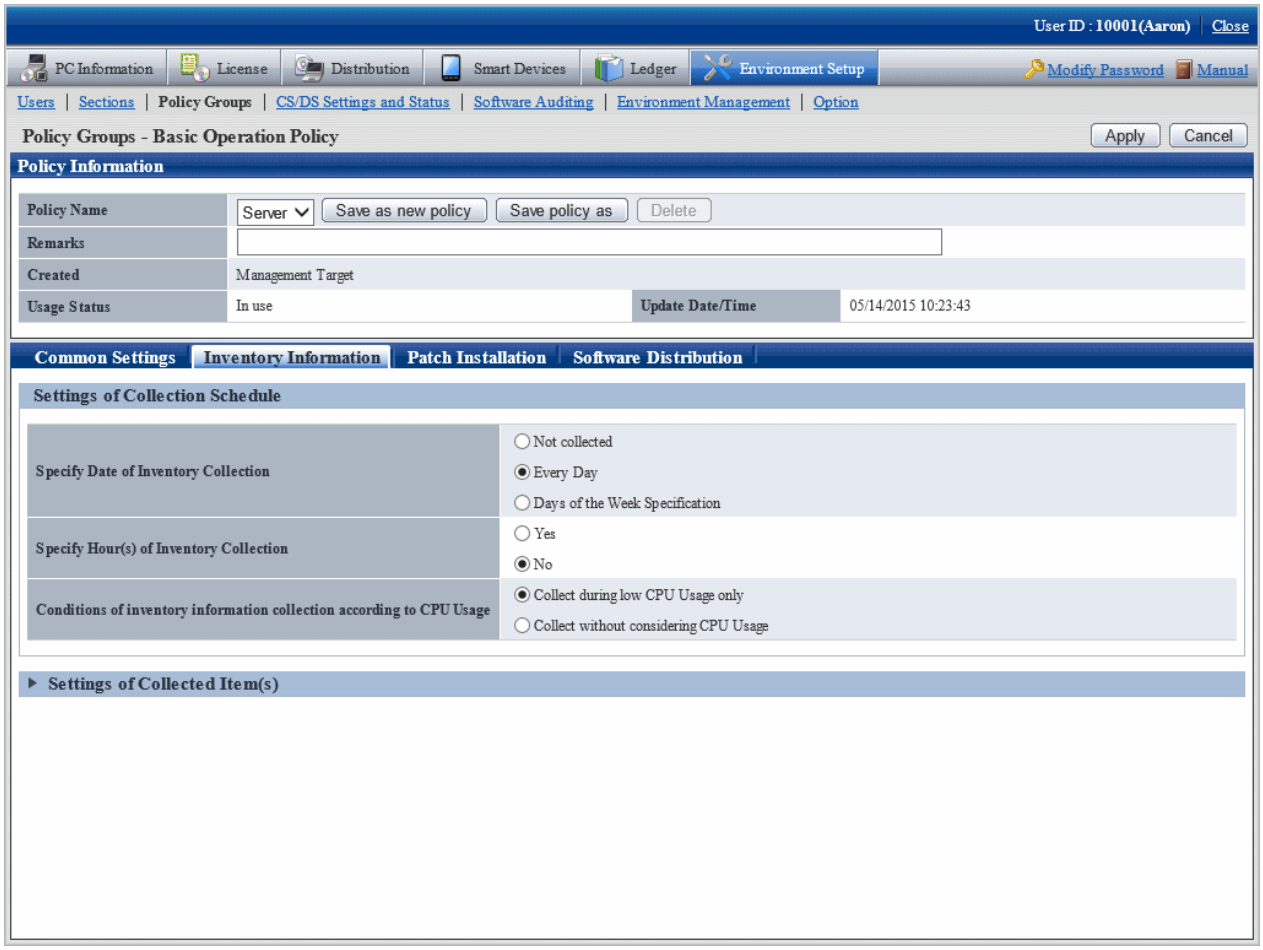
5. Click the **Common Settings** tab, set the following items.

Item	Description
Interval of Checking policy	Set the time interval for confirming the newly arrived information after the client PC is connected to the higher server in minutes. Specify a value within 30~1440. The inventory collection function and automatic patch installation function run according to this setting. When the network bandwidth is narrow or to reduce the server load, modify the set value. The initial value is 180 minutes. The initial timing of new arrival confirmation takes this value as the maximum for decentralization.
Timing for confirmation during logon	Specify the maximum time from logon to Windows till the new arrival confirmation. Specify a value within 0~180. When specifying a value except 0, the actual time from logon to Windows to the confirmation of newly arrived information will be decentralized according to a random number between 0 to the maximum time. The initial value is 0 minute. - The maximum is *n* minutes later from logon To decentralize the following confirmation timing, select the check box. - Decentralize the timing of confirming software from client

Item	Description
	- Decentralize the timing of confirming security patches from client

6. Click the **Inventory Information** tab.

   The following window will be displayed.



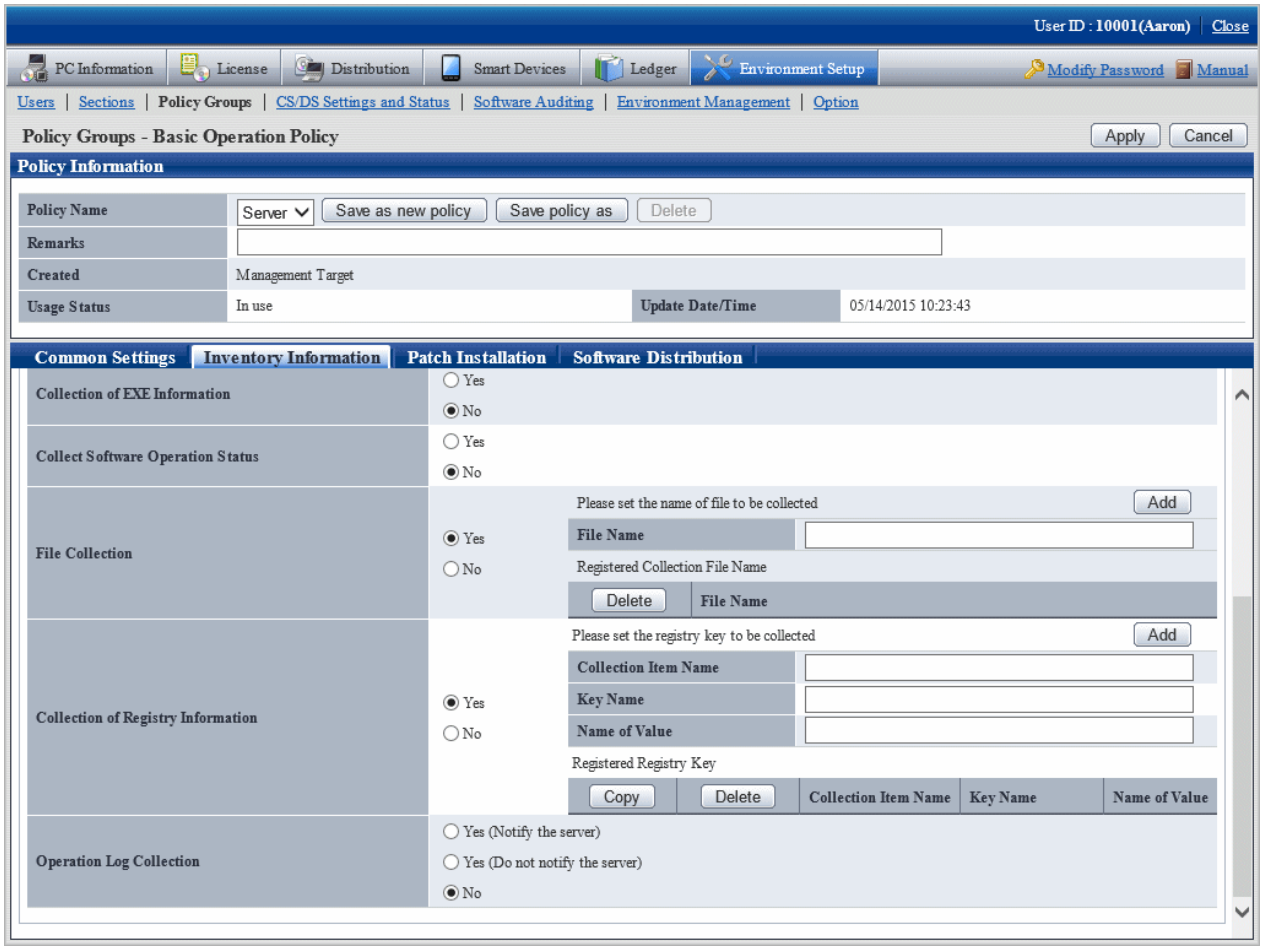
7. Set the following items.

Item	Description
Specify Date of Inventory Collection	Specify the day of a week and time frame to perform inventory collection. - If **Everyday** is selected, then inventory information will be collected every day. - If **Specify a day of a week** is selected, collection of inventory information will be performed in the day selected from Monday to Friday. The initial value is **Everyday**.
Specify Hour(s) of Inventory Collection	Specify the existence of time frame to perform inventory collection and the time frame. - If **Yes** is selected, then inventory collection will be performed when new client policy is confirmed during the specified period. - If **No** is selected, then inventory collection will be performed whenever new client policy is confirmed, regardless of the period. The initial value is **No**. For the timing of collecting inventory information, refer to "3.2.10 Timing of Collecting PC Information of Collecting PC Information".

Item	Description
Conditions of inventory information collection according to CPU Usage	- If **Collect during low CPU Usage only** is selected, inventory information will be collected only when the CPU utilization of PC is low. - If **Collect without considering CPU Usage**, inventory information will be collected regardless of CPU utilization of PC. The initial value is **Collect without Limit of CPU Utilization**. Under the status of high load work such as business, starting inventory information collection can be prevented.

8. After setting the collection condition of software operation status, the connection of software operation status will be started after logging in to Windows again on CT. Other information will be collected according to the set schedule.

   Click **Settings of Collected Item(s)**, the following items will be displayed.



Set the following items.

Item	Description
Collection of EXE Information	- If **Yes** is selected, then the information of all executable files (file with .exe extension) in the build-in hard disk of each PC will be collected. - If **No** is selected, then the information of executable file will not be collected. The initial value is **No**. The executable files contained in hard disk or flash memory connected through USB, CD-ROM drive, DVD-ROM drive and network drive will be not collected as EXE information.

Item	Description
	The initial value for the EXE information collection is "difference collection". This can be changed by using the CustomPolicy.exe command with the -cl.diff.collectExe option.
Collect Software Operation Status	- If **Yes** is selected, then the software operation status will be collected. - If **No** is selected, then software operation status will not be collected. - The initial value is **No**.
File Collection	Specify whether to collect random file from the hard disk of each PC and accumulate on server. - If **Yes** is selected, then the specified file will be collected. - If **No** is selected, then the specified file will not be collected. The initial value is **No**. - Set the file name to be collected Specify up to 129 fullwidth or 259 halfwidth characters.Specify the file name with the absolute path that contains drive name. In addition, the files with same name cannot be specified even if they are saved in different folders. Note When collection is performed after specifying the file under the System32 folder in the Windows system directory for **Collection File Name**, the following files will be collected according to OS. Example of setting: C:\Windows\System32\test.txt - When file collection is performed on 32-bit OS, the files under the following folder will be collected according to specification. C:\Windows\System32\test.txt - When file collection is performed on 64-bit OS, redirection will be performed automatically according to the function of OS and the files under the following folder will be collected. C:\Windows\SystemWOW64\test.txt
Collection of Registry Information	Specify whether to collect the registry content of each PC. - If **Yes** is selected, then the specified registry information will be collected. - If **No** is selected, then registry information will not be collected. The initial value is **No**. - **Collection Item Name** Specify any name that is easy to manage using up to 127 fullwidth or 255 halfwidth characters. - **Key Name** Specify the registry key name to be collected using up 127 fullwidth or 255 halfwidth characters. Specify the registry key under the key shown as follows. \HKEY_LOCAL_MACHINE \HKEY_CLASSES_ROOT

Item	Description
	\HKEY_USERS \HKEY_LOCAL_MACHINE64 - **Name of Value** Specify the registry value name to be collected using up 127 fullwidth or 255 halfwidth characters. The types of registry key value can be collected are as follows. - REG_BINARY - REG_DWORD - REG_MULTI_SZ - REG_SZ Note - When collecting the registry value of CT, if the **Value Name** of collection condition is omitted (**(Standard)** or **(Regulated)** is specified), the collection result will vary depending on OS according to the following conditions. [Condition] When the **Key Name** and **Value Name** of registry collection condition exist but the data of value does not exist. [Collection Result] When **Registry Information** is viewed from **Inventory Information** of the main menu, **Collection Item Name** will not be displayed. - The key named "\HKEY_LOCAL_MACHINE64" does not exist. When CT runs on the Windows of 64-bit OS, to collect the key value under the "\HKEY_LOCAL_MACHINE\Software" registry key, redirection of Windows will be performed and it will be the value of key specified under "\HKEY_LOCAL_MACHINE\Software\WOW6432node" that is actually collected. For the key not to be redirected through this registry redirection, but to collect the key value under the specified key, specify "\HKEY_LOCAL_MACHINE64".
Operation Log Collection	Specify whether to collect the simple operation logs of each PC. - If **Yes (Notify the server)** is selected, then the simple operation log on CT will be recorded in the simple operation log file and this information will be notified to server during the collection of inventory information. Through notifying the server, the simple operation log file on CS will be collected and the required disk capacity will be increased, but collective management of logs can be performed on CS. - If **Yes (Do not notify the server)** is selected, the simple operation log information on CT will be recorded in the simple operation log file, but will not be notified to server as inventory information. To confirm the recorded log information, it is required to confirm through the simple operation log on CT. - If **No** is selected, then simple operation log will not be collected. Even if this item is in selected status, the past simple operation logs saved on CS or CT will not be deleted.

Item	Description
	The initial value is **No**. Note - Since it will increase the required disk capacity of CT and CS, this function is disabled in factory settings. To enable this function, it is required to perform policy settings. - If **Yes (Notify server)** is selected, the required disk capacity will be increased.

9. Confirm the settings, and click the **Apply** button.

   The set content will be saved.
   On CT, the function will be enabled after the modified policy is received.

3.1.2 Perform Operation Settings of the Entire System

This section describes how to set the operation conditions of the entire system for collecting PC information.

There are following types of operation condition of the entire system.

- Settings of software dictionary
- Settings of user information item label

3.1.2.1 Set Software Dictionary

To collect software information in Systemwalker Desktop Patrol, it is required to define the search condition for judging the software. In Systemwalker Desktop Patrol, this definition is called "Software Dictionary".

For settings of software dictionary, refer to "2.2 Set Auditing Software"

3.1.2.2 Set the Item Label of User Information

In Systemwalker Desktop Patrol, any information input by user on CT can be managed as PC information. This information is called information.

Item name of user information can only be set/modified on CS.

Maximum 10 items can be set for user information, which can be used as information management required during inventory making, such as property number, manufacture number, operation remarks .etc.

The following describes how to set user information items.

Procedure

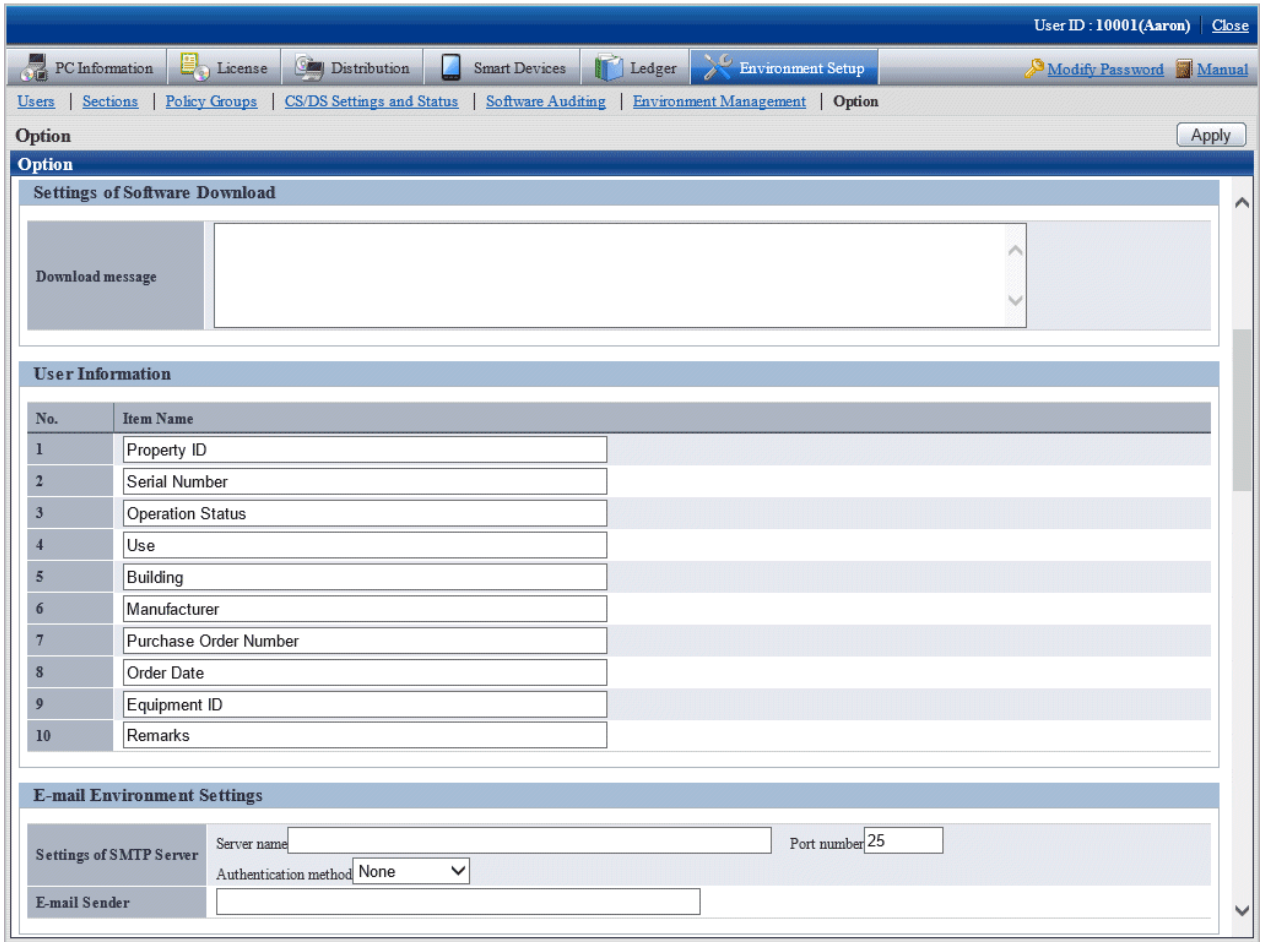
The operation procedure is as follows.

1. Log in to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Option**.

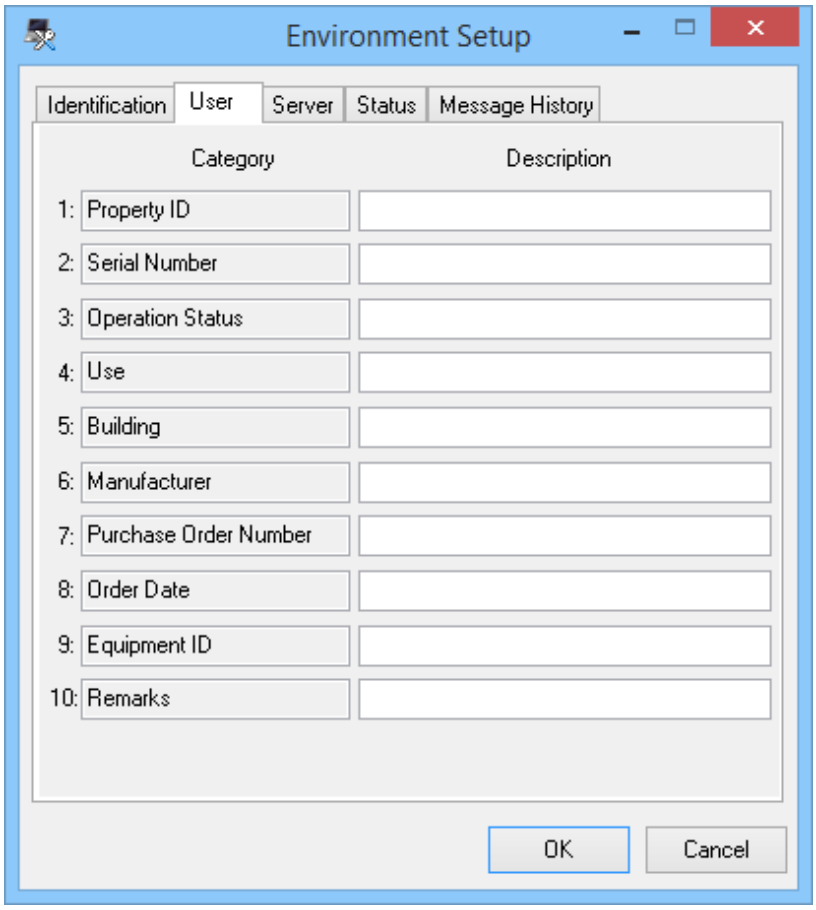
   The following window will be displayed.



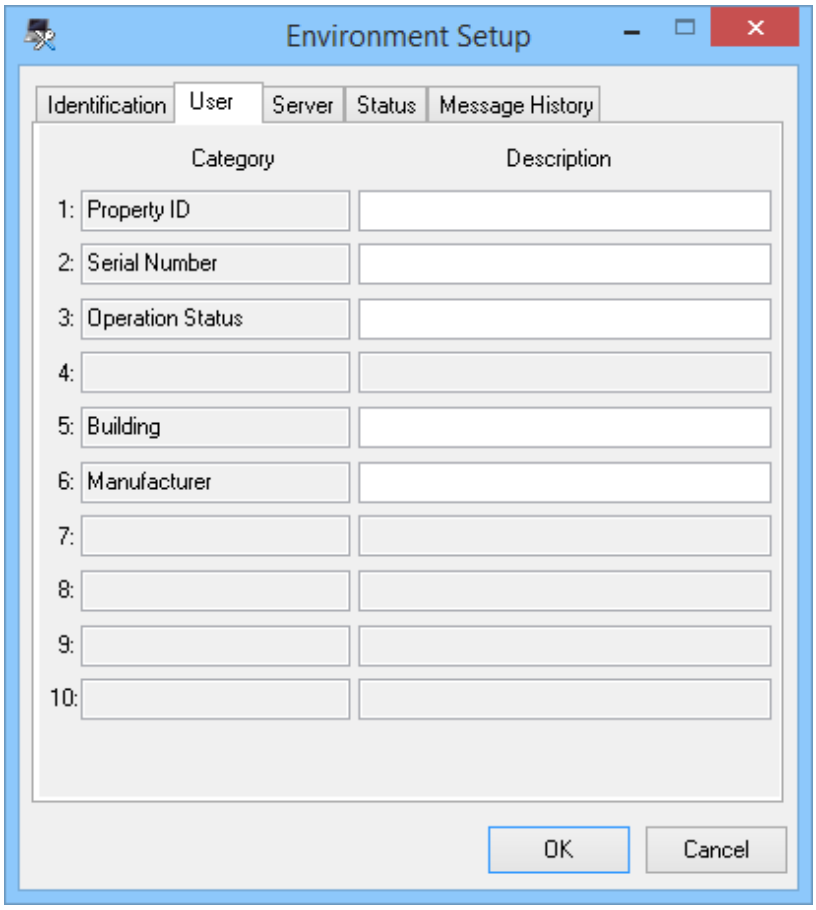
3. Enter **Item Name** of **User Information**.

Item	Description
Item Name	Specify the item name of user information with Japanese or alphanumeric characters. Specify up to 32 fullwidth or 64 halfwidth characters. The following symbols can be specified. "-""@"."("")""["]""{"}""<"">"":";" It is unable to specify with only the space. In addition, the duplicated item name cannot be specified. The following 10 item names are specified by default. Item name can be modified freely. **Property ID**, **Serial Number**, **Operation Status**, **Use**, **Building**, **Manufacturer**, **Purchase Order Number**, **Order Date**, **Equipment ID**, **Remarks**

The item of user information that has been set is displayed in CT as follows.



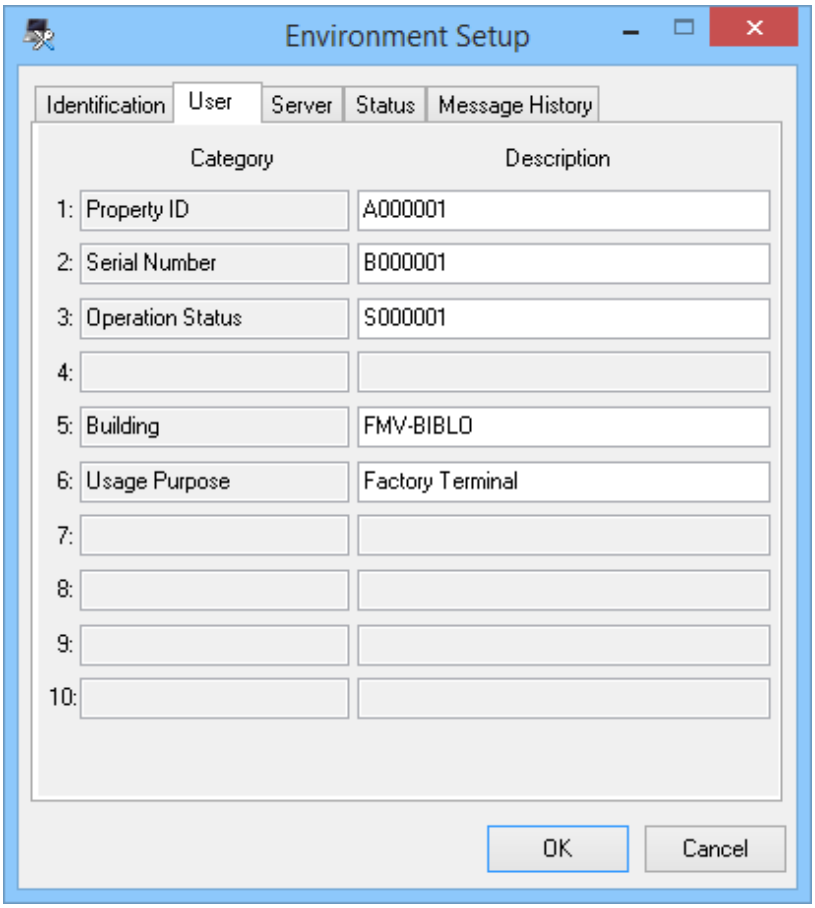
The line without entered item will not be allowed to enter content in CT.



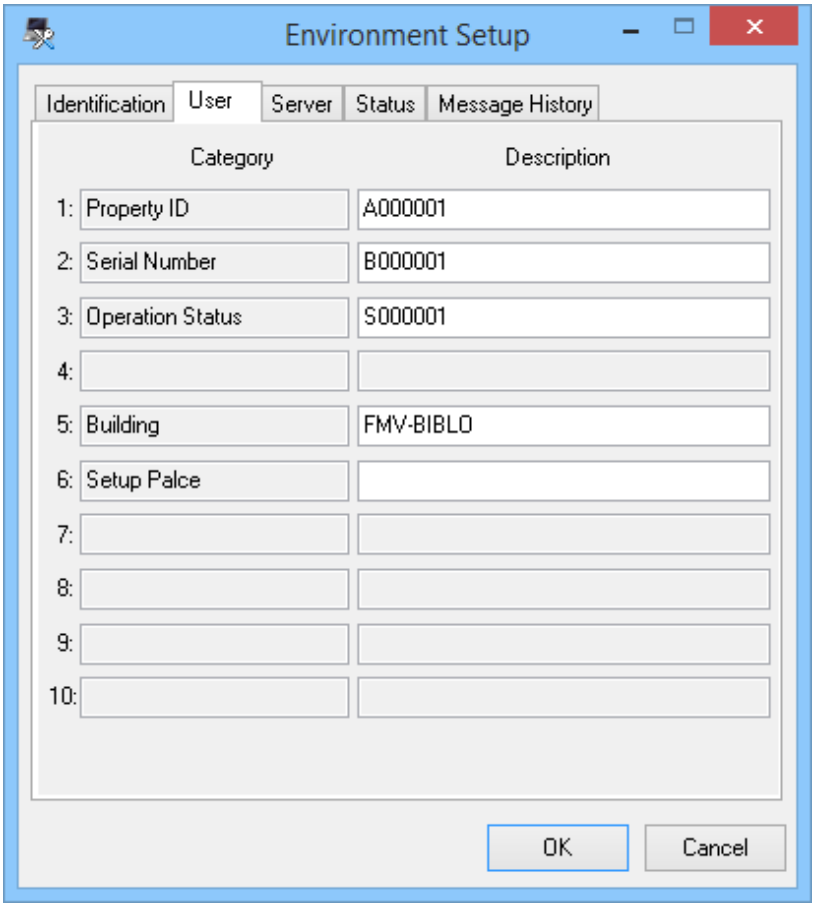
Consideration

- When modifying the item label under the status that PC information has been collected from CT, the value that has been set in the user information of CT environment setup window will be deleted.

  Therefore, set the item of user information during system construction.



In this example, since the item label has been modified from **Usage Purpose** to **Setting Location**, **Factory Terminal** with content being set will be deleted.



3.1.3 Perform Settings of Inventory Collection by Command Mode CT

In the mobile PC that is disconnected from network or due to the reason of low network speed, CT function of command mode will be used for collection of inventory information.

On command mode CT, the inventory information that can be collected is as follows.

Collection Information		Collection in Command Mode CT
Inventory Information	Basic Information (OS information, hardware information)	Y
	Software information	Y
	Anti-Virus software	Y
	Product information	Y
	User Information	Y
	EXE Information	Y
	Registry Information	Y
	Unapplied Patch Information	Y

Collection Information		Collection in Command Mode CT
	Security Information: System Security Information User Security Information	Y
	Security Information: Desktop Keeper Information	N
Software Operation Status		N
Operation log		N
File Collection		N
Report Information	Power Saving Auditing Information: Power Saving setting value	Y
	Power Saving Auditing Information: Power Saving operation status	N

Y: can be collected

N: cannot be collected

In command mode CT, the following functions are prepared. It is not required to install CT to PC.

- "CTOffline.exe": Function of collecting inventory information
- "CTMail.exe": Function of collecting inventory information and sending inventory information through E-mail

The command mode CT downloads from the download menu.

In addition, "CTOffline.exe" and "CTMail.exe" are created in the following timing.

- When software dictionary is updated
- When auditing software is changed
- When the operation settings of command mode CT is modified

At the above timing, and when modifying the CS/DS for registering inventory information, use "CTOffline.exe" and "CTMail.exe" that are newly created.

There are following method to register the collected inventory information to CS or DS.

- When E-mail is not used
- When E-mail is used

When e-mail is not used

In the PC environment in which E-mail cannot be used, collect inventory information by "CTOffline.exe" and register the created file to CS or DS.

The operation procedure from collection of inventory information to registration is shown as follows.

1. Select the software to audit.

   For this procedure, refer to "2.2 Set Auditing Software".

2. Perform operation settings of command mode CT.

   For this procedure, refer to "2.3.1.2 Add Command Mode CT".

3. Execute "CTOffline.exe" on the PC to collect inventory information.

   The inventory information file of "Use ID + PC Name" will be created.

4. Save the inventory information file to CS or DS.

5. Perform the following settings before registering the file of collected inventory information.

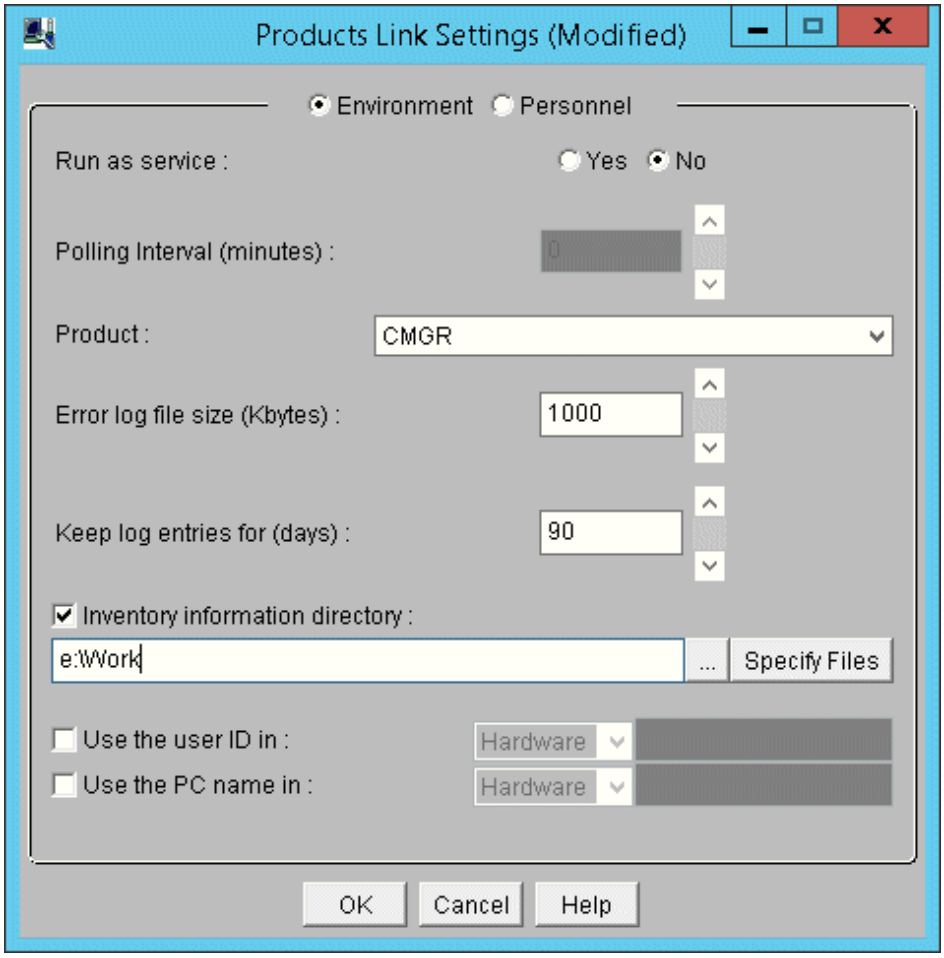
   - When registering to CS

     Select **Start** > **Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Link with Other Product - Environment Setup**, or **Apps** > **Systemwalker Desktop Patrol** > **Products Link Settings**.

   - When registering to DS

     Double-lick the "iissetup.exe" file in <DTP Installation Directory>\FJSVsbiis\bin

   The **Products Link Settings (Modified)** window will be displayed.



6. Enter the following information, and click the **OK** button.

   In addition, for other information, refer to "14.2 Collection of Inventory Information".

   - Select **Yes** or **No** in the radio button of **Run as service**

     When **Yes** is selected

     According to polling interval, collection of inventory information will be performed automatically.

     When **No** is selected

Execute the following command in command prompt and inventory information file will be imported. In the parameter, enter "CT".

```
DTP installation directory\FJSVsbiis\bin\InvSend.exe CT
```

- Select **CT** from the pull-down menu of **Product**
- In the **Inventory information directory** text box, enter the folder path for saving inventory information file in the step "3." Mentioned above.

  After the inventory information has been sent by E-mail, the file itself will be deleted from the path for saving inventory information. When it is not sent successfully, the inventory information file will still be saved in the path for saving inventory information.

When e-mail is used

In the PC environment in which E-mail can be used, use "CTMail.exe" to collect inventory information, the create file will be registered to CS or DS using E-mail.

The operation procedure from collection of inventory information to registration is shown as follows.

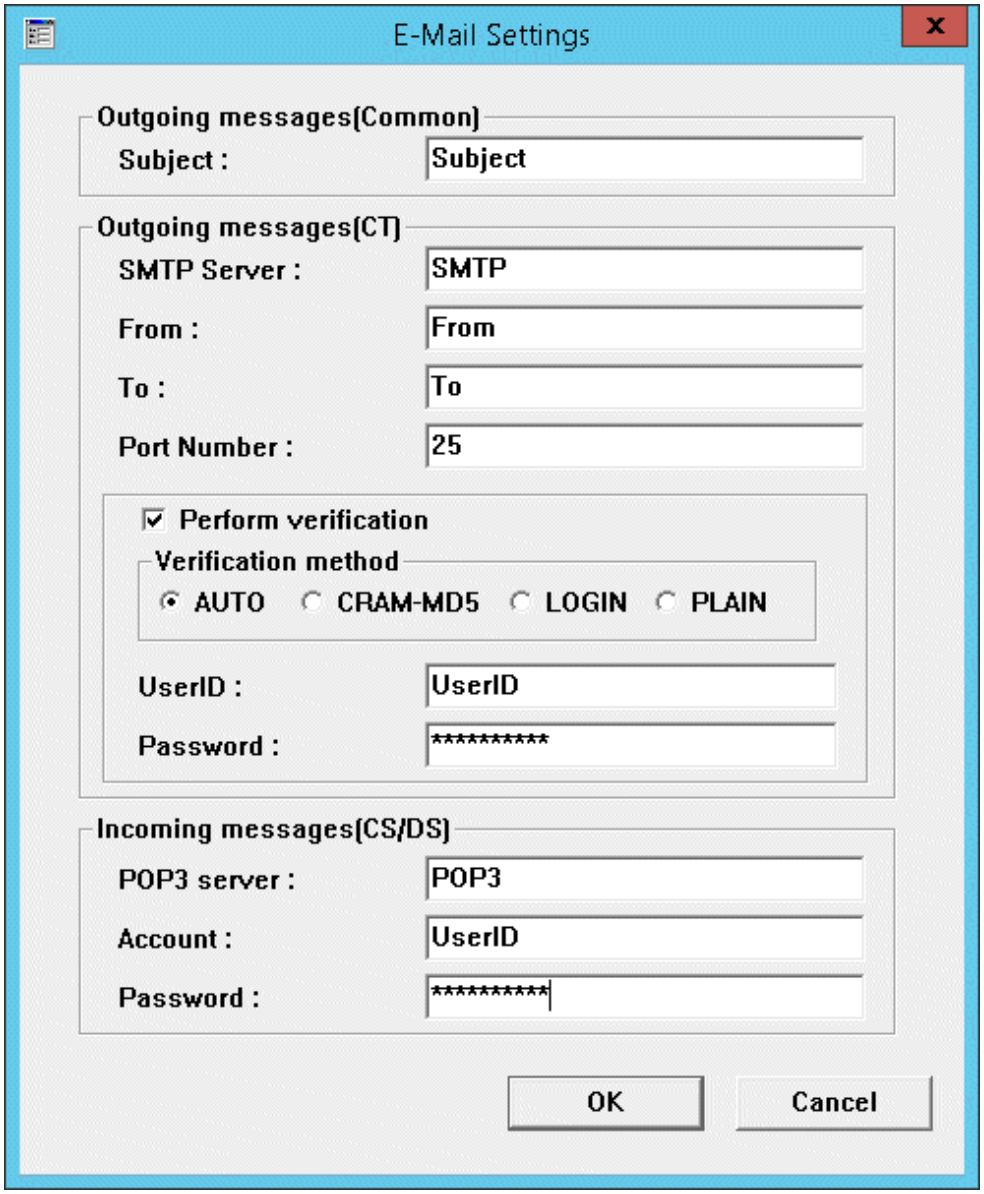
1. Prepare the account and E-mail address for receiving E-mails in the E-mail server.
2. Set the E-mail environment.
   - In case of CS

     Select **Start** > **Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **E-mail Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **E-Mail Settings**.

   - In case of DS

     Double-click the "mailenv.exe" file in <DTP Installation Directory>\FJSVsbiis\bin.

The **E-mail Settings** window will be displayed.



3. Enter the following information and click the **OK** button.

	Item	Description
Outgoing messages (Common)	**Subject**	Set the E-mail subject when inventory information is sent by E-mail. Specify up to 1023 halfwidth alphanumeric characters.
Outgoing messages (CT) (Note)	**SMTP Server**	Set the SMTP server address when inventory information is sent by E-mail. Specify up to 1023 halfwidth alphanumeric characters.
	From	Set the sender name when inventory information is sent by E-mail. Specify up to 1023 halfwidth alphanumeric characters, and the following symbol: @
	To	Set the recipient address when inventory information is sent by E-mail.

	Item	Description
		Specify up to 1023 halfwidth alphanumeric characters, and the following symbol: @
	Port Number	Set a value within 0~65535 as the port number used by SMTP Server. When this item is omitted, the system will set the port to No. 25 automatically. In addition, if the specified value exceeds the above range or an incorrect port number has been specified, error will occur.
	Perform verification	Select it when performing SMTP authentication. The following items will be activated.
	Verification method	In authentication method, **AUTO**, **CRAM-MD5**, **LOGIN**, **PLAIN**. The default value is **AUTO**. When **AUTO** is selected, the authentication method will be determined automatically according to the following sequence. 1) **CRAM-MD5** 2) **PLAIN** 3) **LOGIN**
	User ID	Enter the user ID used in the selected authentication method. Specify up to 64 halfwidth alphanumeric characters, and the following symbol: @ No matter if the authentication method is selected, if this item is omitted, an error will occur.
	Password	Enter the password used in the selected authentication method with no more than 64 single-byte alphanumeric characters.
Incoming messages (CS/DS)	**POP3 server**	Set the POP server address used when inventory information is received by E-mail. Enter with single-byte alphanumeric characters within 1023 characters.
	Account	Enter the user ID for authentication when inventory information is received by E-mail. Specify up to 64 halfwidth alphanumeric characters, and the following symbol: @
	Password	Enter the password for authentication when inventory information is received by E-mail. Enter no more than 64 single-byte alphanumeric characters.

Note) In case of DS, **Outgoing messages (CT side)** cannot be set.

4. Perform the following settings before registering the inventory information file.

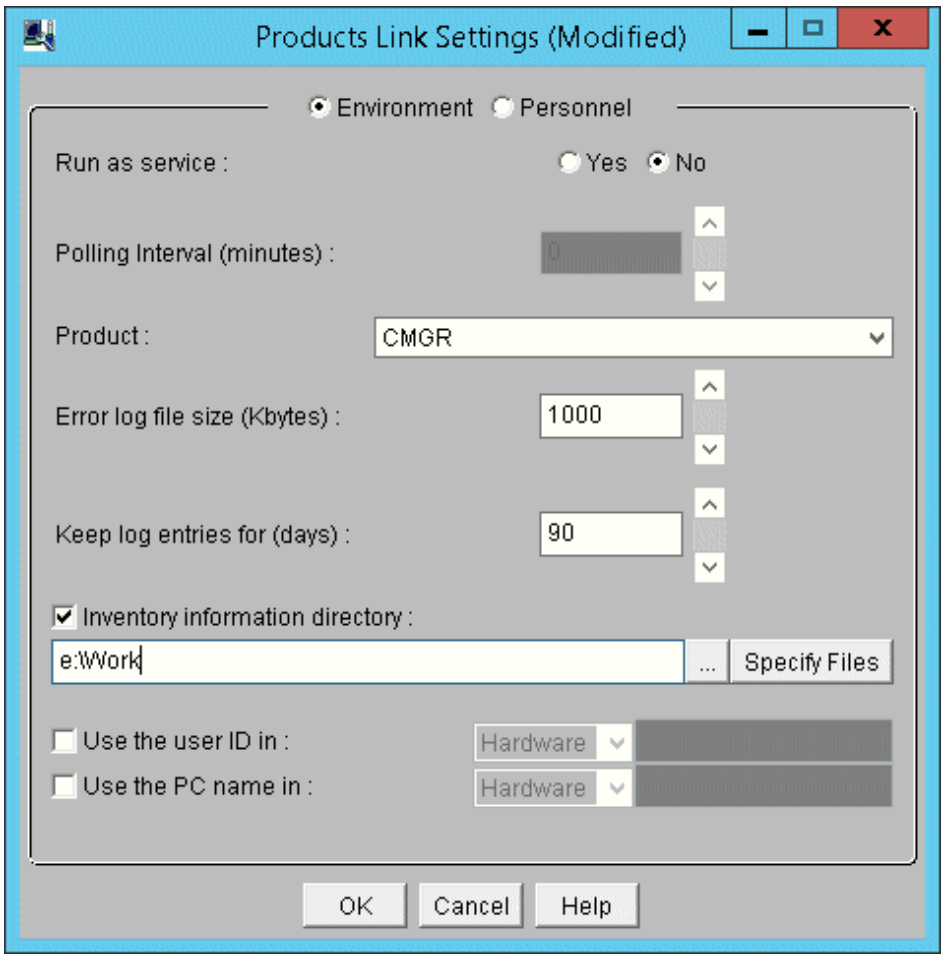
   - When registering to CS

     Select **Start** > **Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Products Links Settings - Environment Setup**, or **Apps** > **Systemwalker Desktop Patrol** > **Products Link Settings**.

   - When registering to DS

     Double-click the "iissetup.exe" file in <DTP Installation Directory>\FJSVsbiis\bin.

The **Products Link Settings (Modified)** window will be displayed.



5. Enter the following information, and click the **OK** button.

   In addition, for other information, refer to "14.2 Collection of Inventory Information".

   - Select **Yes** or **No** in the radio button of **Run as service**

     When **Yes** is selected

     According to polling interval, collection of inventory information will be performed automatically.

     When **No** is selected

     Execute the following command in command prompt and inventory information file will be imported. In the parameter, enter "CT".

     ```
     DTP installation directory\FJSVsbiis\bin\InvSend.exe CT
     ```

   - Select **CT** from the pull-down menu of **Product**
   - In the **Inventory information directory** text box, enter the inventory information file path sent through E-mail (no need to specify file name)
   - After the inventory information has been sent by E-mail, the file itself will be deleted from the path for saving inventory information. When it is not sent successfully, the inventory information file will still be saved in the path for saving inventory information.

6. Select Software to Audit

   For detailed procedure, refer to "2.2 Set Auditing Software".

7. Perform operation settings of command mode CT.

   For detailed procedure, refer to "2.3.1.2 Add Command Mode CT".

8. On the PC to collect inventory information, execute "CTMail.exe".

   Send the inventory information file of "User ID + PC Name" using E-mail.

3.1.4 Perform Settings of PC Operation Management

When using the PC operation management function, it is required to perform the following settings on CS and the PC to perform operation management.

- Settings of CS

  The system administrator will register the PC to perform operation management to CS.

- Settings of the PC to perform operation management

  The system administrator or the PC user that has knowledge in BIOS settings will perform the settings required by AMT on the BIOS settings window of the PC to perform operation management.

3.1.4.1 Settings of CS

Perform the following settings on CS.

- Define the PC information of operation management target

  The information of PC to perform operation management is defined in CSV file.

  For details of CSV file, refer to *Systemwalker Desktop Patrol Reference Manual*.

- Register the PC to perform operation management

  Execute the dtpamtent.exe (register information of PC as operation management target) command on CS to register information of PC as operation management target.

  For details of the dtpamtent.exe (register information of PC as operation management target) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

3.1.4.2 Settings of Operation Management Target PC

Perform the following setting on the BIOS settings window of the PC to perform operation management. For information on how to display the BIOS settings window, refer to the manual of PC itself.

1. Startup of ME BIOS (Start the window such as AMT settings .etc)
2. Settings of Intel(R) ME Configuration
3. Settings of Intel(R) AMT Configuration

For method of setting, refer to the manual of PC to perform operation management.

Example of setting in case of FMV-D5330

The method of setting on FMV-D5330 is as follows.

Start ME BIOS

Start according to the following procedure.

1. Turn on the power of PC and start the PC.

2. After the "FUJITSU" logo is displayed, "Press <Ctrl-P> to enter Intel(R) ME Setup" will be displayed on the window. At this time, press [Ctrl] and [P] at the same time.
3. The setting window of "Intel (R) ME Configuration", "Intel (R) AMT Configuration" will be displayed. After "Intel(R) ME Password" is displayed, enter the following password.

Settings of Intel(R) ME Configuration

After ME BIOS is started, perform password authentication, select "Intel (R) ME Configuration", and perform the following settings. do not modify other settings.

Setting Items		Setting Value
Intel(R) ME Power Control	Intel(R) ME State upon Initial Power-On	ON
	Intel(R) ME ON in Host Sleep States	ALWAYS

Setting Procedure

1. Select **Intel(R) ME Configuration**.
2. Select **Intel(R) ME Power Control**. In setting items, select the following two items separately and perform settings.
   - **Intel(R) ME State upon Initial Power-On**
   - **Intel(R) ME ON in Host Sleep States**

- Select **Return to Previous Menu**.
- Select **Return to Previous Menu**.

Settings of Intel(R) AMT Configuration

After starting ME BIOS, execute password authentication and select **Intel (R) AMT Configuration** to perform the following settings. Perform settings according to the sequence of **Provision Model**, **TCP/IP**. Do not modify other settings.

Setting Items		Setting Value	Required/ Optional
Provision Model	-	Intel AMT 2.0 Mode (Note)	R
	-	Small Business (Note)	R
TCP/IP	**Network Interface**	Enable (Note)	R
	DHCP	Disable (Note)	R
	IP address	IP address	R
	Subnet mask	Subnet mask	R
	Default Gateway address	Default gateway	O
	Preferred DNS address	Preferred DNS	O
	Alternate DNS address	DNS	O
	Domain Name	Domain name	O

R: Required item

O: Optional item (Set a value that is same as the network settings of OS.)

Note) Whether to modify the current setting value, select yes (Y) or no (N).

Setting Procedure

1. Select **Intel(R) AMT Configuration**.
2. In setting items, select **Provision Model**, the following items will be displayed in sequence. Perform settings in sequence. (After settings have been completed, **Provision Model** will disappear from the list of setting items.)
   - **Intel(R) AMT 2.0 Mode**
   - **Small Business**
3. In setting items, select **TCP/IP**. The following setting items will be displayed in sequence, perform settings separately.
   - **Network Interface**
   - **DHCP**
   - **IP address**
   - **Subnet mask**
   - **Default Gateway address** (If not to set, click [Enter] directly)
   - **Preferred DNS address** (If not to set, click [Enter] directly)
   - **Alternate DNS address** (If not to set, click [Enter] directly)
   - **Domain Name** (If not to set, click [Enter] directly)
4. Select **Return to Previous Menu**
5. Select **Exit**

In the OS and AMT to perform operation management of PC, fixed IP address should be assigned separately. Do not perform DHCP settings in OS and AMT.

3.1.5 Perform Settings Related to Operation Status

This section describes how to set for modifying the displayed content related to the operation status in the status window.

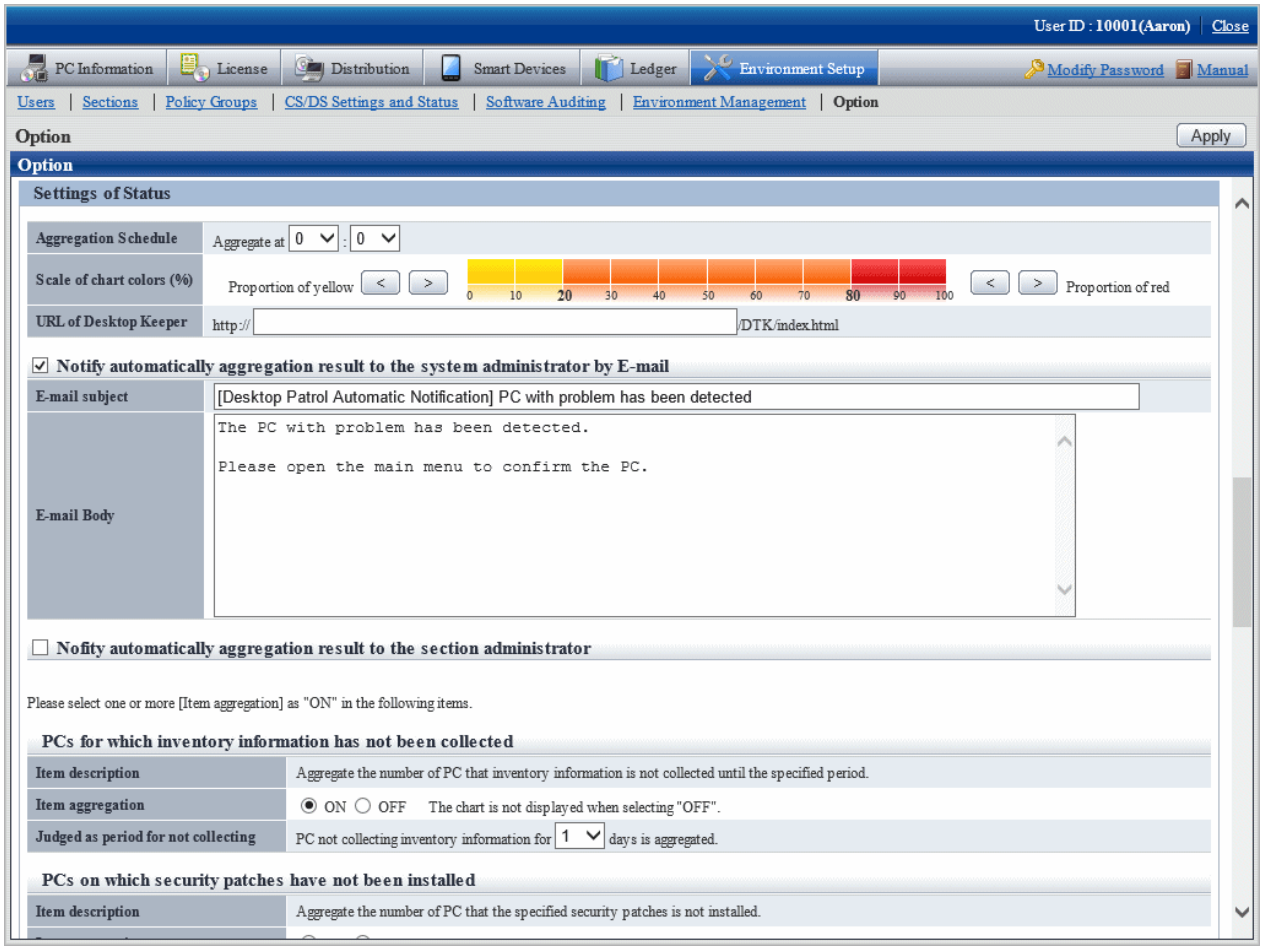
Procedure

The procedure is as follows.

1. Log in to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Option**, and view **Settings of Status**.



First of all, set the following items.

Item	Content
Aggregation Schedule	Specify the time to start aggregation. Hour: Selection can be made in hours within the range of 0~23. Minute: Selection can be made in minutes within the range of 0~59. [Initial Value] 00:00 Aggregate the information to be output to status window at specified time.
Scale of chart colors (%)	For the graph color of aggregation, the proportion of yellow and red can be modified by 10%. [Initial Value] - The threshold value of yellow bar graph is within 20% - The threshold value of red bar graph is within 80%
URL of Desktop Keeper	Set when log management information of Systemwalker Desktop Keeper of V14.2.0 or later is displayed. In addition, set when performing log search of the same PC in the log search window of Systemwalker Desktop Keeper V14.2.0. In this setting, specify the FQDN name or host name or IP address of Management Server of Desktop Keeper or Master Management Server of Desktop Keeper using up to 261 halfwidth characters.

Item	Content
	[Initial Value] Not displayed.

Point

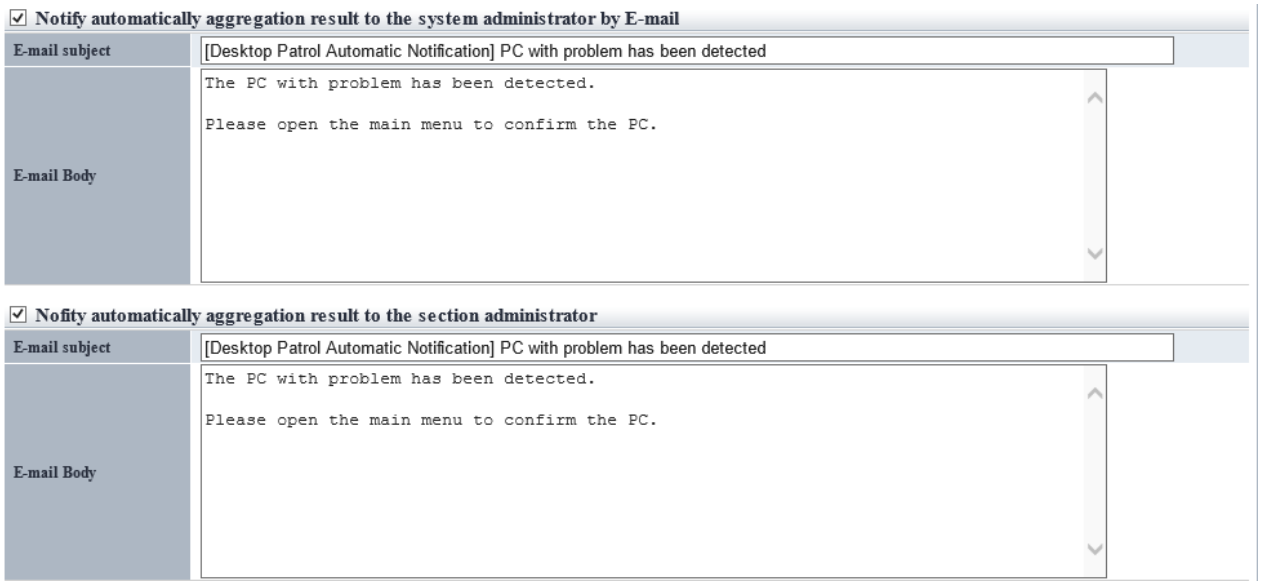
Information of all PCs managed on Systemwalker standard database will be viewed during aggregation.

Therefore, it is likely that the load on the server of CS will be increased, so it is recommended to set the aggregation schedule to the time frame that will not affect business (for example, at 00:00 .etc).

Point

About automatic E-mail notification of aggregation result

The aggregation result of operation status that has been aggregated according to the aggregation schedule can be notified by E-mail automatically. After this function has been enabled, the aggregation result of operation status will be notified automatically by E-mail, which is very convenient.



To notify the aggregation result to all system administrators, select "Notify the aggregation result to system administrator automatically by E-mail".

To notify the PC information in the aggregation item to the section administrator of the section to which the PC belongs, select "Notify the aggregation result to section administrator automatically by E-mail".

The item content is as follows.

Item	Content
E-mail subject	Specify the email subject. Specify up to 64 fullwidth or 128 halfwidth characters. When this item is omitted, the E-mail will be sent without a subject. The initial value is the following subject. The PC with problems has been detected by [Desktop Patrol Automatic Sending].
E-mail Body	Specify the email body text. Specify up to 1024 fullwidth or 2048 halfwidth characters.

Item	Content
	When this item is omitted, only the information attached by the system will be added to the body text. The initial value is the following content. A PC with problem has been detected. Open the main menu and confirm this PC.

The system will attach the following information apart from the E-mail body text.

```
  :
:(E-mail body text set in the options window)   (1)
:

[Summary]   (2)
Aggregation target section : Development Department 1   (3)

[Aggregation Information]   (4)
PCs for which inventory information has not been collected: 38 pcs   (5)
PCs on which security patches have not been installed: 10 pcs   (6)
PCs violating security policy: 26 pcs   (7)
PCs violating power saving policy: 14 pcs   (8)
PCs on which unlicensed software is installed: 2 pcs   (9)
Expired contracts: 2 contracts   (10)
Contracts about to expire: 1 contract   (11)
Devices for which stocktaking is not yet complete: 16 devices   (12)
Devices detected as unregistered devices: 33 devices   (13)
--
http://server information (FQDN name or Host name or IP address of CS)/DTP/index.html   (14)
```

Item	Content
E-mail subject	It is the subject that has been set.
(1)	Display the content of E-mail body text set in the option window.
(2) ~ (14)	It is the information attached by the system. [Summary] Display the aggregation target section. [Aggregation Information] Display the following information that has been aggregated. - 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 URL of Systemwalker Desktop Patrol Adopt the host name specified at CS installation.

Confirm the status after logging in to the main menu for details.

Note

- The aggregation item whose aggregation result is 0 will not be output. In addition, when all the aggregation items are 0, automatic notification will not be performed.
- When E-mail cannot be used due to the reasons such as unable to communicate with the SMTP server set by administrator, error information will be output to event log and the latest information will be sent by E-mail at next aggregation.

Point

When performing automatic E-mail notification

E-mail environment settings and settings of E-mail address are required for system administrator or section administrator to perform automatic E-mail notification.

- Settings of E-mail environment

  Set E-mail environment in **Environment Setup** > **Option** > **E-mail Environment Settings**. Only the system administrator can perform the setting.

- E-mail address settings

  Set the E-mail address of recipient. For details on how to set, refer to "2.1 Construct Master Data".

Note

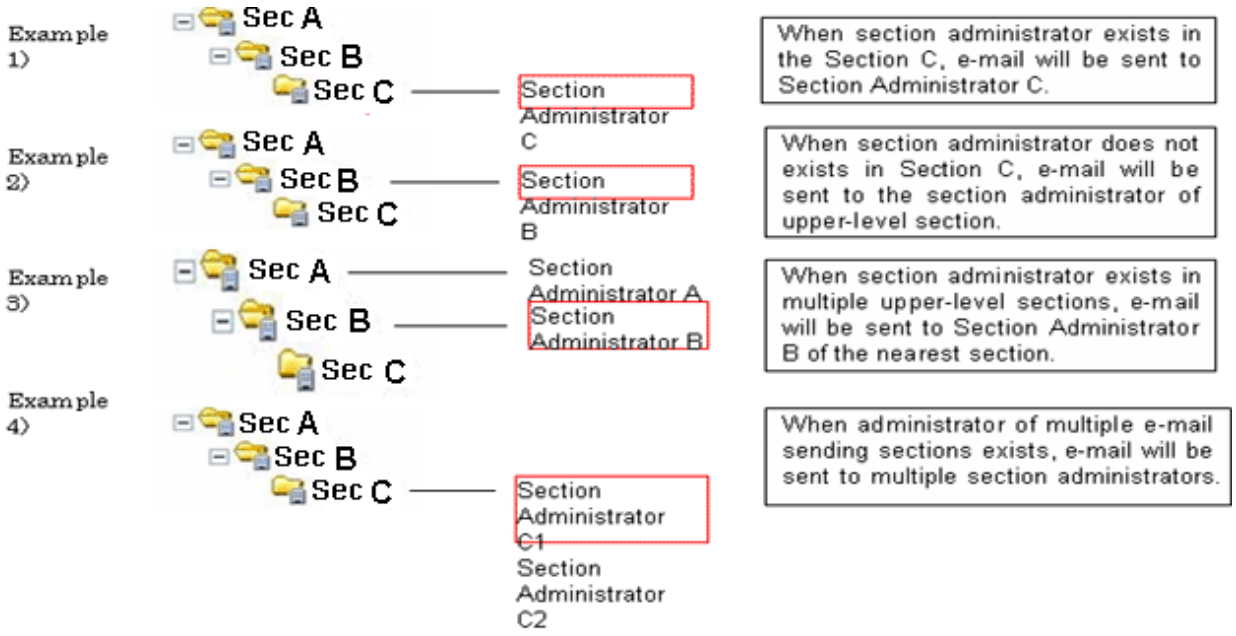
When E-mail address is not set in recipient address, automatic E-mail notification will not be performed.

Point

Recipient of automatic E-mail notification to section administrator

Even if notification to the section administrator of the section to which the PC belongs is performed, if there is no section administrator for the section it belongs, notification will be sent to the nearest higher section.

The following is the example when problem occurred in the PC that belongs to the section C and automatic notification is sent to the section administrator.



Next, set each aggregation item according to operation.

In each item, set one **Yes** for **Aggregation of Item** at least.

PCs for which inventory information has not been collected

Set the following items.

Item	Content
Item description	It is the description of the **PCs for which inventory information has not been collected** item.
Item aggregation	Set whether to aggregate the number of PC corresponding to the **PCs for which inventory information has not been collected** item. **Yes**: In the timing of aggregation schedule, aggregate the number of PC corresponding to this item and display the aggregation result of this item in the **Status** window. **No**: Do not aggregate the number of PC corresponding to this item and do not display this item in the **Status** window.
Judged as period for not collecting	It is the setting items displayed when **Yes** is selected in **Aggregation of Item**. Aggregate the inventory information prior to the date set in this period based on the date when aggregation is performed. For example, when **1** is selected in the pull-down menu, the information beginning from the day before yesterday will be aggregated. The content set in this item will be effective at the next time when the aggregation schedule is executed. Specify the day by selecting **1~31** from the pull-down menu.

PCs on which security patches have not been installed

Set the following items.

Item	Content
Item description	It is the description of the **PCs on which security patches have not been installed** item.
Item aggregation	Set whether to aggregate the number of PC corresponding to the **PCs on which security patches have not been installed** item. **Yes**: In the timing of aggregation schedule, aggregate the number of PC corresponding to this item and display the aggregation result of this item in the **Status** window. **No**: Do not aggregate the number of PC corresponding to this item and do not display this item in the **Status** window. When no security patch is published, select **No**. If **Yes** is selected when no security patch is published, **No corresponding PC in xxx pcs** will be displayed on the **Status** window.

PCs violating security policy

Set the following items.

Item	Content
Item description	It is the description of the **PCs violating security policy** item.
Item aggregation	Set whether to aggregate the number of PC corresponding to the **PCs violating security policy** item. **Yes**: In the timing of aggregation schedule, aggregate the number of PC corresponding to this item and display the aggregation result of this item in the **Status** window. **No**: Do not aggregate the number of PC corresponding to this item and do not display this item in the **Status** window.

PCs violating power saving policy

Set the following items.

Item	Content
Item description	It is the description of the **PCs violating power saving policy** item.
Item aggregation	Set whether to aggregate the number of PC corresponding to the **PCs violating power saving policy** item. **Yes**: In the timing of aggregation schedule, aggregate the number of PC corresponding to this item and display the aggregation result of this item in the **Status** window. **No**: Do not aggregate the number of PC corresponding to this item and do not display this item in the **Status** window.

PCs on which unlicensed software is installed

Set the following items:

Item	Content
Item description	Description of the **PCs on which unlicensed software is installed** item.
Item aggregation	Specify whether to aggregate the number of PCs that fall into the **PCs on which unlicensed software is installed** item. **Yes**: The number of PCs that fall into this item will be aggregated as per the aggregation schedule, and the result will be displayed in the **Status** window.

Item	Content
	No: The number of PCs that fall into this item will not be aggregated, and this item will not be displayed in the **Status** window.

Expired contracts

Set the following items:

Item	Content
Item description	Description of the **Expired contracts** item.
Item aggregation	Specify whether to aggregate the number of contracts that fall into the **Expired contracts** item. **Yes**: The number of contracts that fall into this item will be aggregated as per the aggregation schedule, and the result will be displayed in the **Status** window. **No**: The number of contracts that fall into this item will not be aggregated, and this item will not be displayed in the **Status** window.

Contracts about to expire

Set the following items:

Item	Content
Item description	This is the description for **Contracts about to expire**.
Item aggregation	Specify whether to aggregate the number of contracts that fall into the **Contracts about to expire** item. **Yes**: The number of contracts that fall into this item will be aggregated as per the aggregation schedule, and the result will be displayed in the **Status** window. **No**: The number of contracts that fall into this item will not be aggregated, and this item will not be displayed in the **Status** window.

Devices for which stocktaking is not yet complete

Set the following items:

Item	Content
Item description	This is the description for **Devices for which stocktaking is not yet complete**.
Item aggregation	Specify whether to aggregate the number of devices that fall into the **Devices for which stocktaking is not yet complete** item. **Yes**: The number of devices that fall into this item will be aggregated as per the aggregation schedule, and the result will be displayed in the **Status** window. **No**: The number of devices that fall into this item will not be aggregated, and this item will not be displayed in the **Status** window.

Devices detected as unregistered devices

Set the following items:

Item	Content
Item description	This is the description for **Devices detected as unregistered devices**.
Item aggregation	Specify whether to aggregate the number of devices that fall into the **Devices detected as unregistered devices** item.

Item	Content
	Yes: The number of devices that fall into this item will be aggregated as per the aggregation schedule, and the result will be displayed in the **Status** window. **No**: The number of devices that fall into this item will not be aggregated, and this item will not be displayed in the **Status** window.

3. Modify settings according to operation, and click the **Apply** button.

3.1.6 Perform Settings Related to Operation Processing

In the following window, perform operation processing according to the judgment of system administrator/section administrator.

- By clicking the corresponding number of sets in the **Status** window, the list of PC will be displayed (Processing window)
- **Inventory information** window

Note

- For the following PC, processing except inventory deletion cannot be executed.
  - PC in which the version of CT is prior to V13.2.0
  - PC on which the inventory information is collected through command mode CT
  - PC on which the inventory information is collected through other products
- Only the latest 20 items of processing instructions for 1 PC are effective. Therefore, if the instruction content that is not processed exceeds 21 items for one PC, the previous processing instructions will be invalid.
- If the processing result is not notified 7 days after the processing is instructed, it indicates that the processing result was ended abnormally.

The following describes the operation processing that is likely to occur in each window.

Operation Processing	Window that can use the operation Y: can be processed N: cannot be processed	
	Processing window	Inventory information window
Message Sending	Y	Y
Inventory Collection	Y	Y
Inventory Delete	Y	Y
Security Patch Installation	Y (Note 1)	N
Security Settings Modification	Y (Note 2)	N
Power Saving Settings Modification	Y (Note 3)	N

Note 1) Can be processed only in case of **PCs on which security patches have not been installed**
Note 2) Can be processed only in case of **PCs violating security policy**
Note 3) Can be processed only in case of **PCs violating power saving policy**

The following describes the setting method.

Procedure

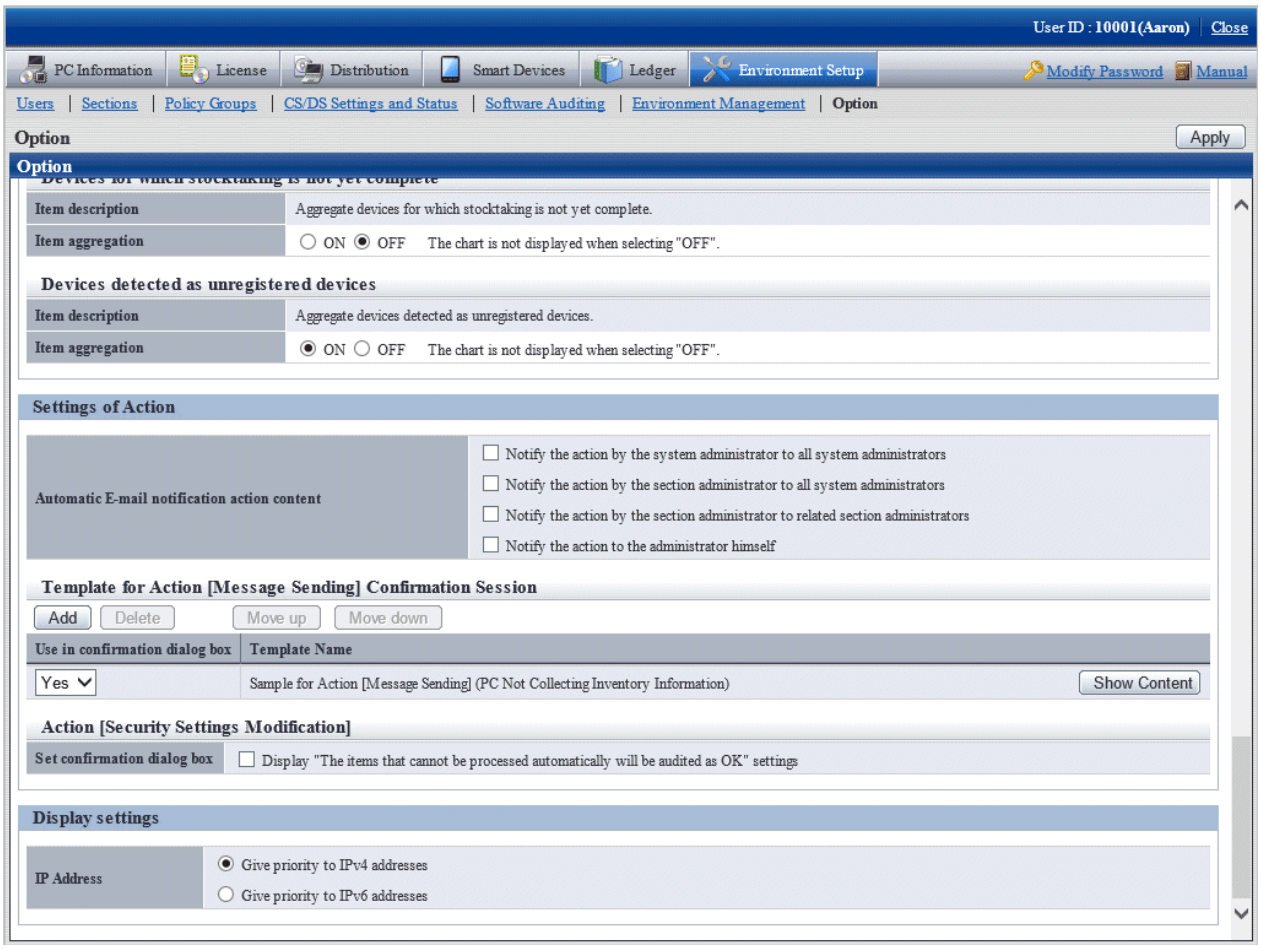
The setting for performing operation processing can only be done by system administrator.

The procedure is as follows.

1. Log in to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

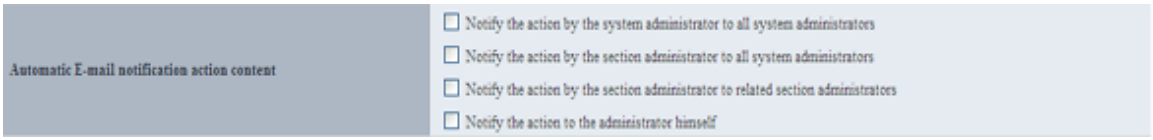
2. Click **Option**, and view **Settings of Action**. Modify the settings according to operation and click the **Apply** button.



The setting items are described in order as follows.

Automatic e-mail notification of action content

It is the settings when the processing content that has been done is notified through E-mail automatically.



Item	Content
Automatic E-mail notification action content	Notify the processing content that has been done through E-mail automatically. Select how to notify the processing content automatically through E-mail and put a check to the checkbox. - Notify the action by the system administrator to all system administrators

Item	Content
	- Notify the action by the section administrator to all system administrators - Notify the action by the section administrator to related section administrators - Notify the action to the administrator himself

The content to be notified by E-mail is the content of performed processing and the list file of PCs that perform the processing.

The format of list file of PC to process is equivalent to the format of **CSV Export** of the processing window.

- E-mail Subject

  [Desktop Patrol Automatic Notification]

- E-mail Text

```
03/16/2011 9:55:55 Processing has been executed.   (1)

[Processing]   (2)
Message Sending

[Text]   (3)
Please perform XXXX.

[Target PC]   (4)
Please refer to the attached file.


--   (5)
Development Department 1 (Section Administrator) Fujitsu Taro   (6)
User ID Smith   (7)
Contact address Elmer.Smith @jp.fujitsu.com 1111-2222   (8)
http://server information (FQDN name or Host name or IP address of CS)/DTP/index.html   (9)
```

Item	Content
E-mail subject	Fixed value.
(1)	MM/DD/ YYYY hh:mm:ss is the time when processing is executed.
(2)	It indicates the processing content selected during processing.
(3)	Output body text only when the processing **Message Sending** is selected.
(4)	Display the list of PCs selected during processing.
(5) ~ (9)	Display the information of user that instructed the processing. Authority is displayed in the () after the section name, the contact address is output when specifying E-mail address and telephone number in user management information. The host name specified during CS installation is adopted as the URL of Systemwalker Desktop Patrol.

Note

Due to differences in interpretation of the MIME protocol, CSV file attachments may be attached to the body of emails sent to the administrator and may not be displayed properly.

You can solve this issue by changing the following settings:

- File: *dtpInstallDir*\BNServ\data\dtp_config
- Section: "MAILOPTION"
- Key: "boundaryLineFeed"

Setting example

Example content of the *dtpInstallDir*\BNServ\data\dtp_config file

```
:
:
[MAILOPTION]
boundaryLineFeed=1
```

Point

When performing automatic E-mail notification

E-mail environment settings and settings of E-mail address are required for system administrator or section administrator to perform automatic E-mail notification.

- Settings of E-mail environment

  Set E-mail environment in **Environment Setup** > **Option** > **E-mail Environment Settings**. Only the system administrator can perform the setting.

- E-mail address settings

  Set the E-mail address of recipient. For details on how to set, refer to "2.1 Construct Master Data".

Note

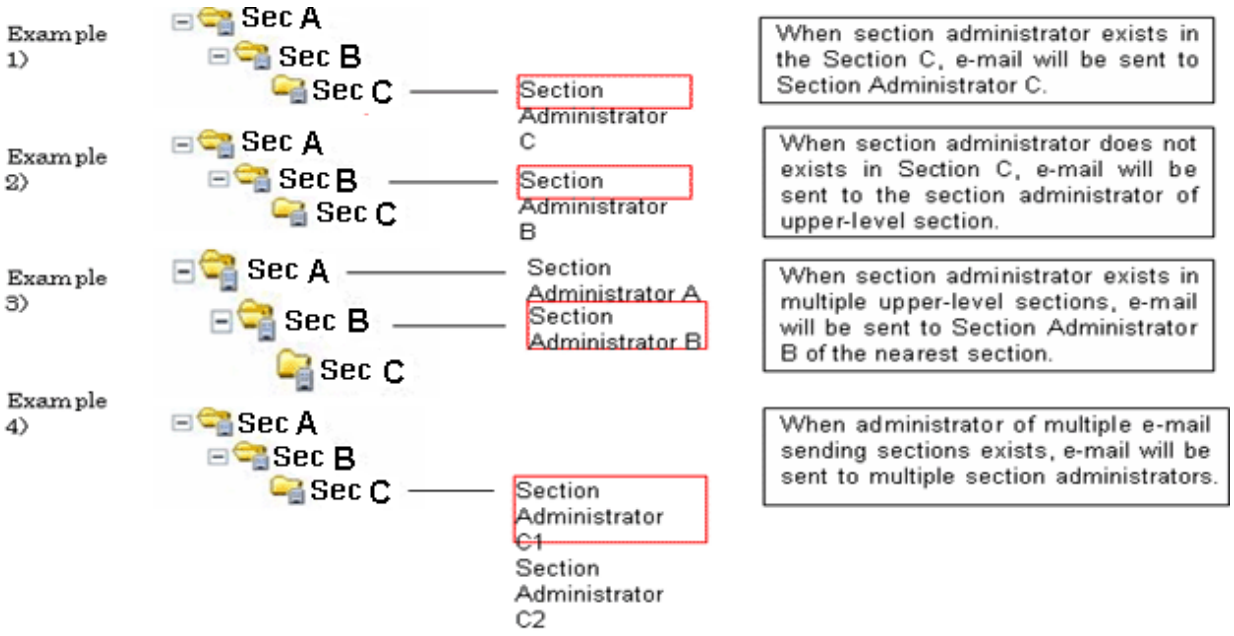
When E-mail address is not set in recipient address, automatic E-mail notification will not be performed.

Point

Recipient of automatic E-mail notification to section administrator

Even if notification to the section administrator of the section to which the PC belongs is performed, if there is no section administrator for the section it belongs, notification will be sent to the nearest higher section.

The following is the example when problem occurred in the PC that belongs to the section C and automatic notification is sent to the section administrator.



When performing the processing message sending

Template using for Action Message Sending Confirmation Session

Manage the template that can be specified in the processing **Message Sending** confirmation dialog.

The list of action **Message Sending** confirmation session is displayed in the following sequence in the row.

Description relating to the template list

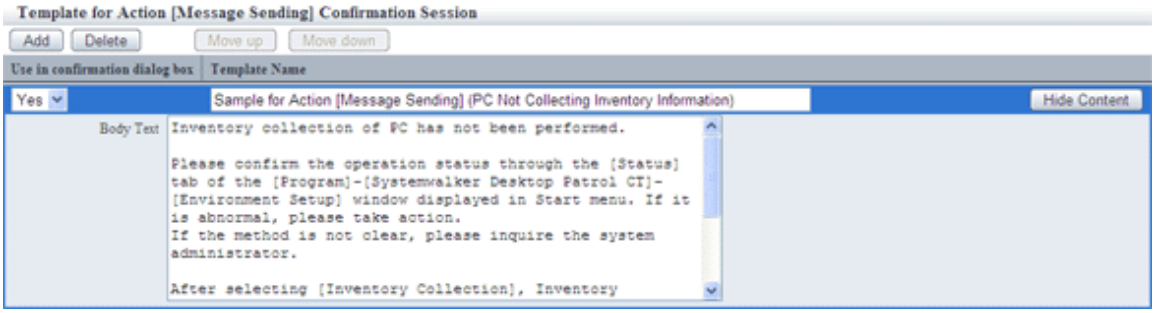
Item	Content
Use in confirmation dialog box	- **Yes** Select the created template when it can be specified in the **Message Sending** confirmation dialog. - **No** Select it when you wish to create a temporary template.
Template name	It is the name of template. Click the display content button, the template name can be edited, and the template content can be confirmed/edited. To close the content, click the hide content button.

Description related to button

Button Name	Content
Add	Create a new template in the template list. Up to 50 templates can be added.
Delete	Delete a template from the template list.

Button Name	Content
Move up/Move down	Select the template to be moved and click the Move button, the sequence of template will be modified and the sequence will be reflected to the list of confirmation dialogs.

Click the Display Content button, and the content of template can be edited.



Item	Content
Template Name	Template name. Specify up to 64 fullwidth or 128 halfwidth characters. This item is required.
Body Text	Body text of action **Message Sending** Specify up to 1024 fullwidth or and 2048 halfwidth characters.

In addition, since the following samples are provided, use it as needed.

- The sample for the action **Message Sending** (**PCs for which inventory information has not been collected**)

The following settings are required based on the content of processing. Perform settings according to requirements.

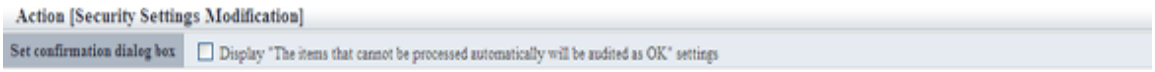
When performing "Security Patch Installation"

Perform settings for the installation of security patches. For details on how to set, refer to "Chapter 6 Distribute/Install Security Patches".

When performing "Security Settings Modification"

Perform the setting for modifying the security settings. For details on how to set, refer to "4.2.2 Settings Related to Auditing Security Settings".

IN addition, settings related to the operation of action **Security Settings Modification** should also be performed.



Item	Content
Security Settings Modification	If **Display the "Set the items that does not allow auto-processing to auditing OK" Settings** is selected, this option will be displayed in the confirmation dialog appeared after the processing **Security Settings Modification** is selected. This option does not perform auto-processing for actual PC.

When performing "Power Saving Settings Modification"

Perform the settings for modifying the power saving settings. For details on how to set, refer to "4.2.1 Settings for Auditing Power Saving Settings".

3.2 Operation

Confirm the collection status of PC information and view PC information.

3.2.1 View Inventory Information

This section describes the operation that views inventory information collected from each PC.

Information can be confirmed from the main menu. In addition, it can also be output to the file in CSV format.

The information that can be confirmed is as follows.

- Basic information (Hardware information)
- Software information
- Anti-Virus software
- Product information
- User information
- EXE information
- Registry information
- Unapplied patch information
- Contract information
- Security information
- Power saving information

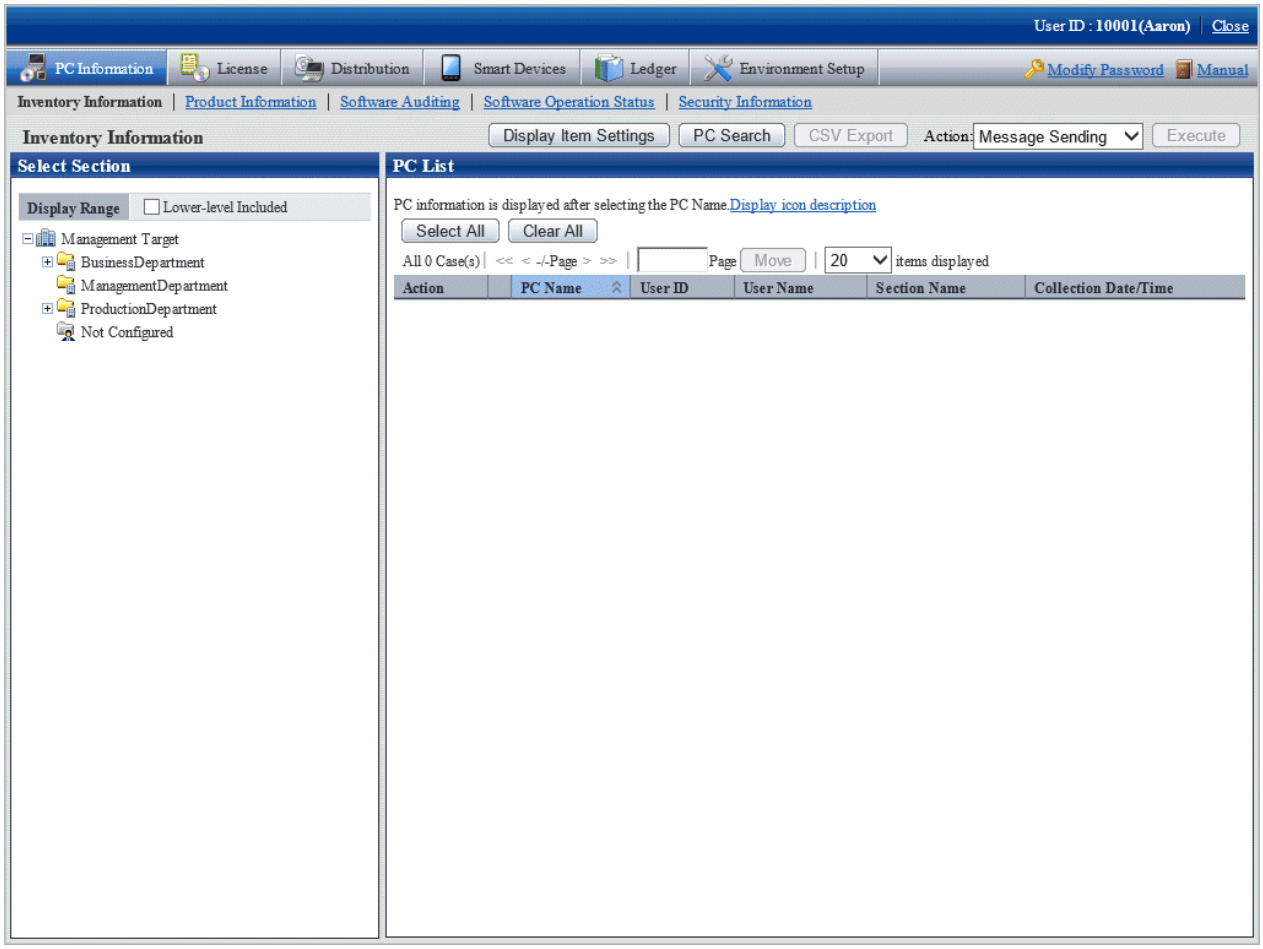
How to view from section tree

Through selecting the PC displayed in the **PC Information** window of the main menu, the inventory information of the PC can be viewed.

The procedure is as follows.

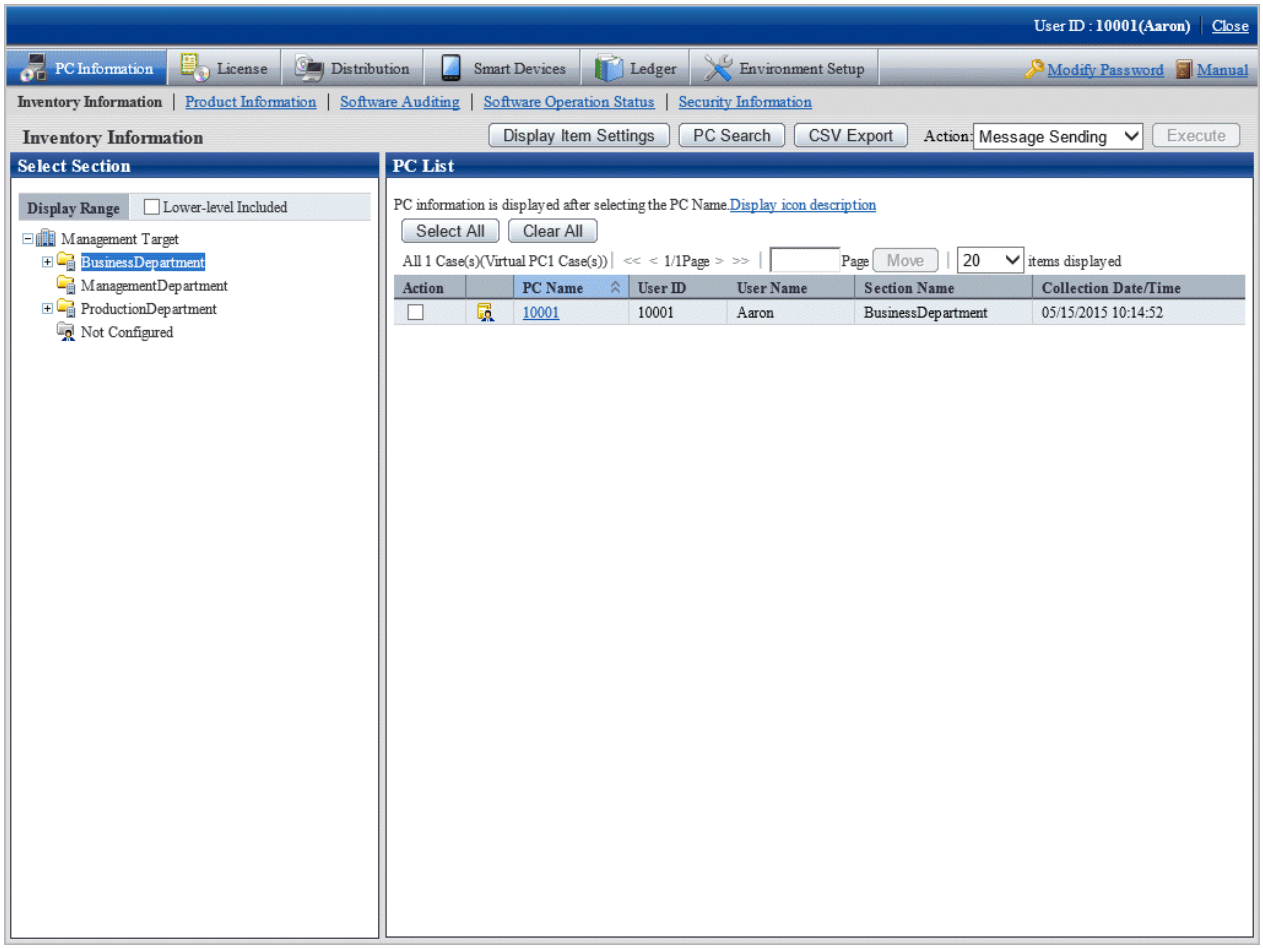
1. Log in to the main menu, and click **PC Information**.

   The following window will be displayed.



2. Select a section from the section tree in the field on the left.

   The PCs under the selected section will be displayed in the field on the right.



   [Confirming with the colours of software dictionary version]

   Version of software dictionary can be recognized by the icon colour of a PC. The relationship between icon colour and version is as follows.

   - (Green):

     Indicates the information is collected with the latest software dictionary.

   - (Yellow):

     Indicates the information is collected with the software dictionary of three generations before.

   - (Red):

     Indicates the information is collected without a software dictionary or with the software dictionary of four generations before.

3. When the hardware information of PC shown in the field on the right is output to the file in CSV format, perform the following procedure. When not to output, proceed to the next step.

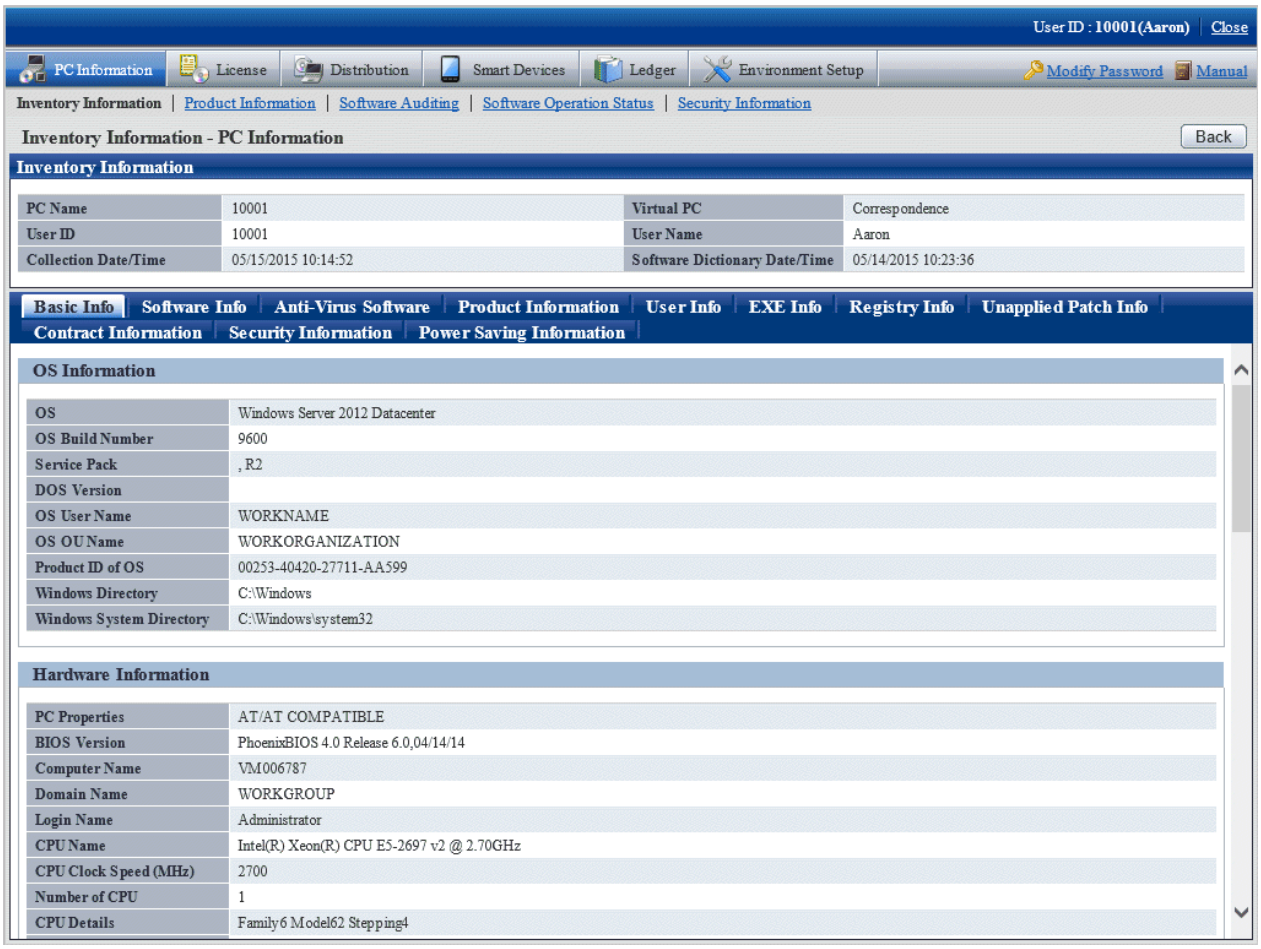
   a. Click the **CSV Export** button.

      The download window will be displayed.

   b. Output the hardware information to a file in CSV format according to the window.

4. Click the PC name in the field on the right.

   The inventory information of the clicked PC will be displayed.



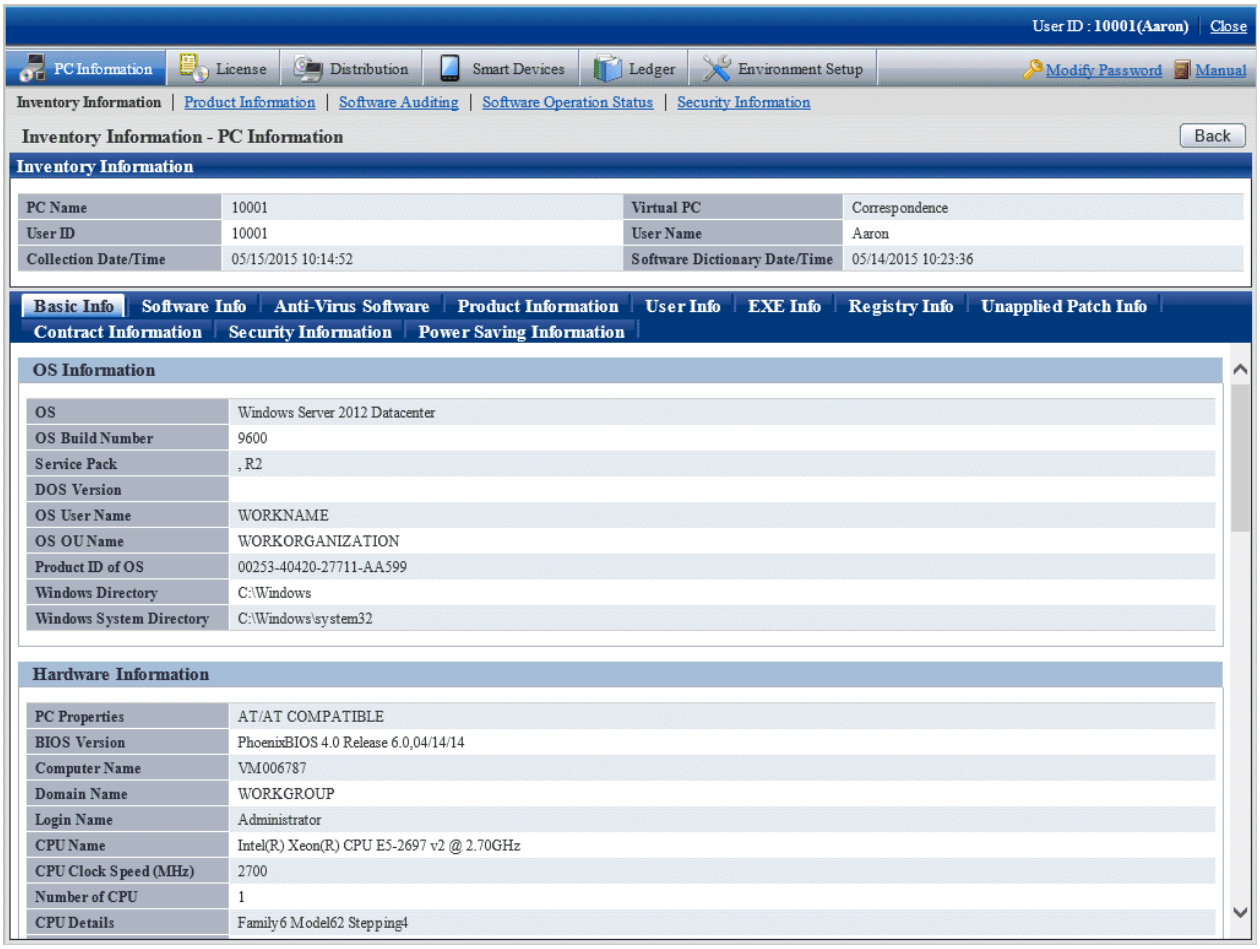
5. Select the following displayed items.

   - **Basic Info** tab
   - **Software Info** tab
   - **Anti-Virus Software** tab
   - **Product Information** tab
   - **User Info** tab
   - **EXE Info** tab
   - **Registry Info** tab
   - **Unapplied Patch Info** tab
   - **Contract Information** tab
   - **Security Information** tab
   - **Power Saving Information** tab

   The selected window will be displayed. For display window, refer to the following description.

When Basic Info **is selected**

The basic information is displayed. The OS information and hardware information of PC can be viewed.



Note

When all the three DNS servers contain registered IP address, part of the information on the third DNS server will not be displayed.

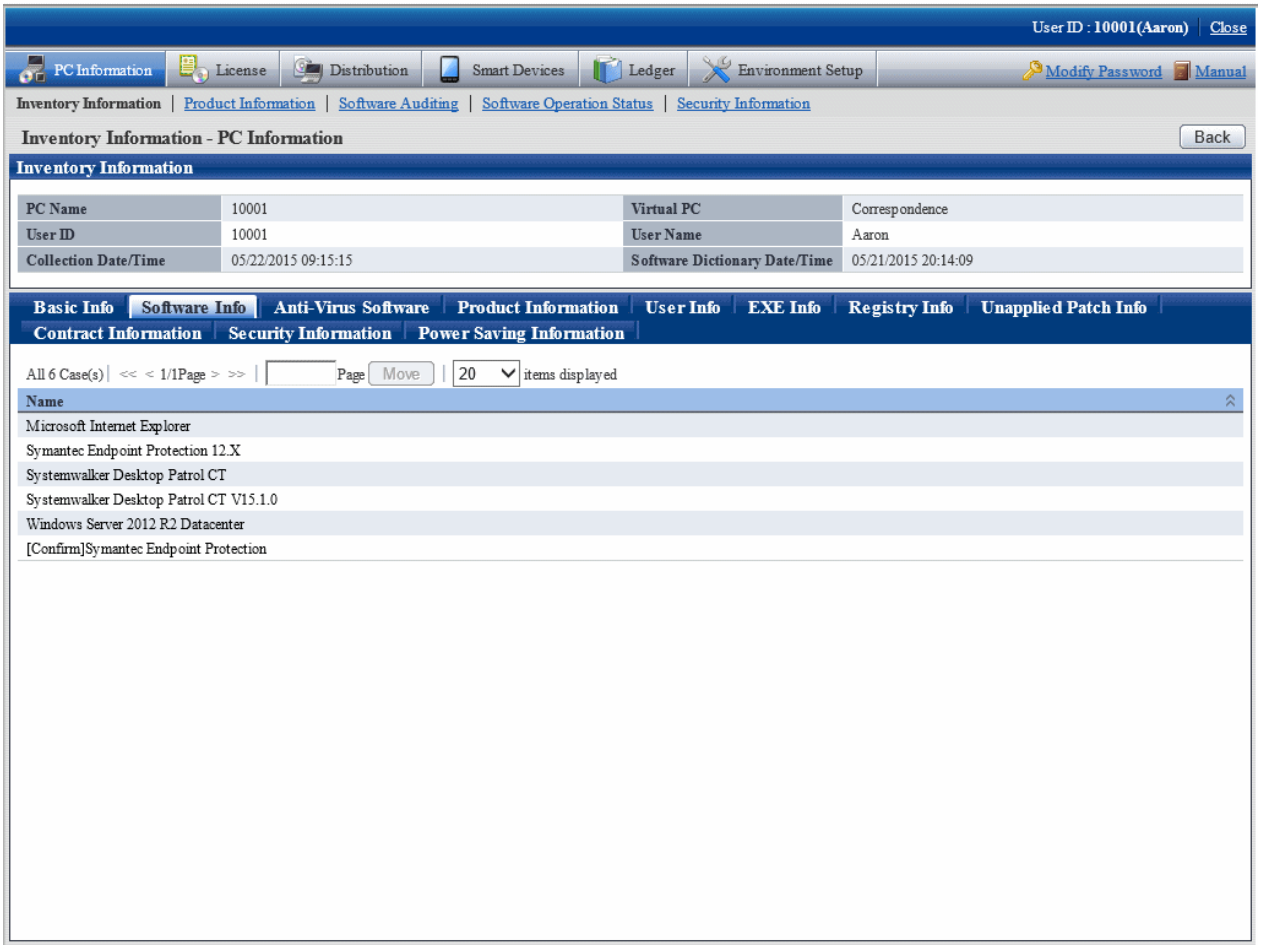
Point

IP addresses in **TCP/IP Information** are expressed as follows:

- To display both IPv4 and IPv6 addresses in dual stack environments, separate them with a forward slash (/).
- IPv6 addresses are separated with a semicolon (;).
- Temporary addresses are prefixed with a number sign (#). However, this applies only to inventory information collected by CT.

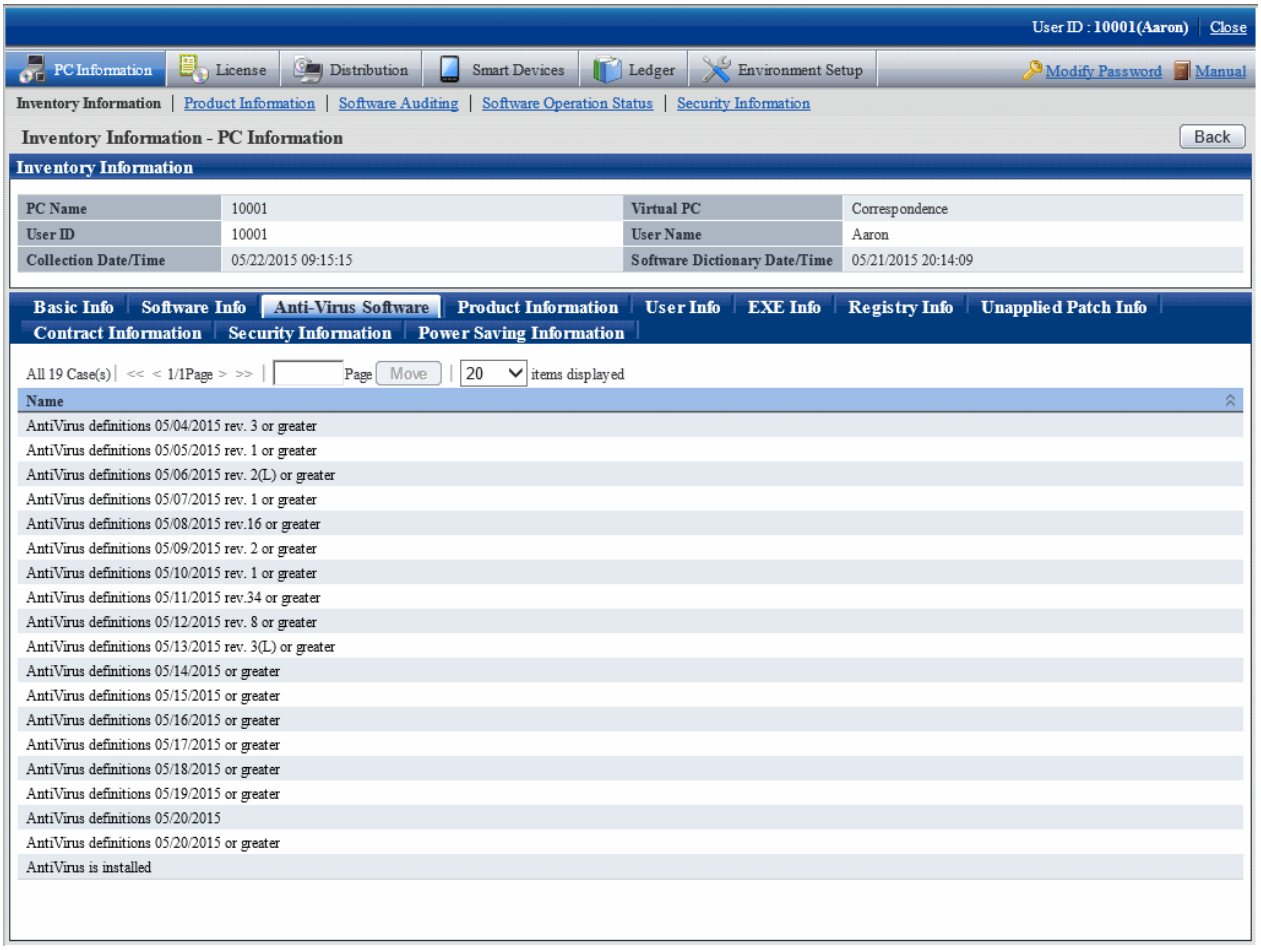
When Software Info **is selected**

The software information will be displayed. The name of software on the selected PC can be viewed.



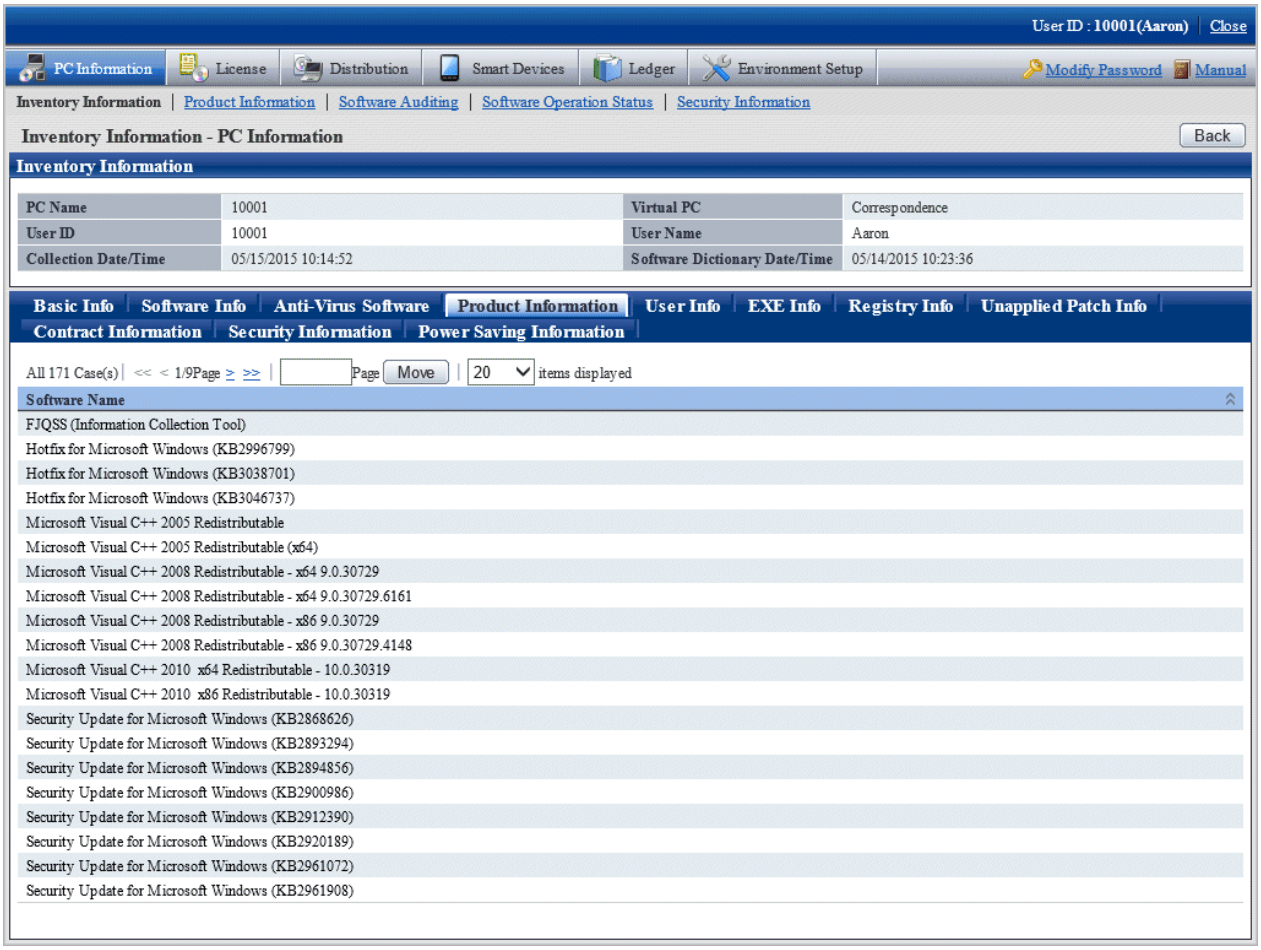
When Anti-Virus Software **is selected**

The information of anti-virus software will be displayed. The anti-virus software installed in the selected PC can be viewed.



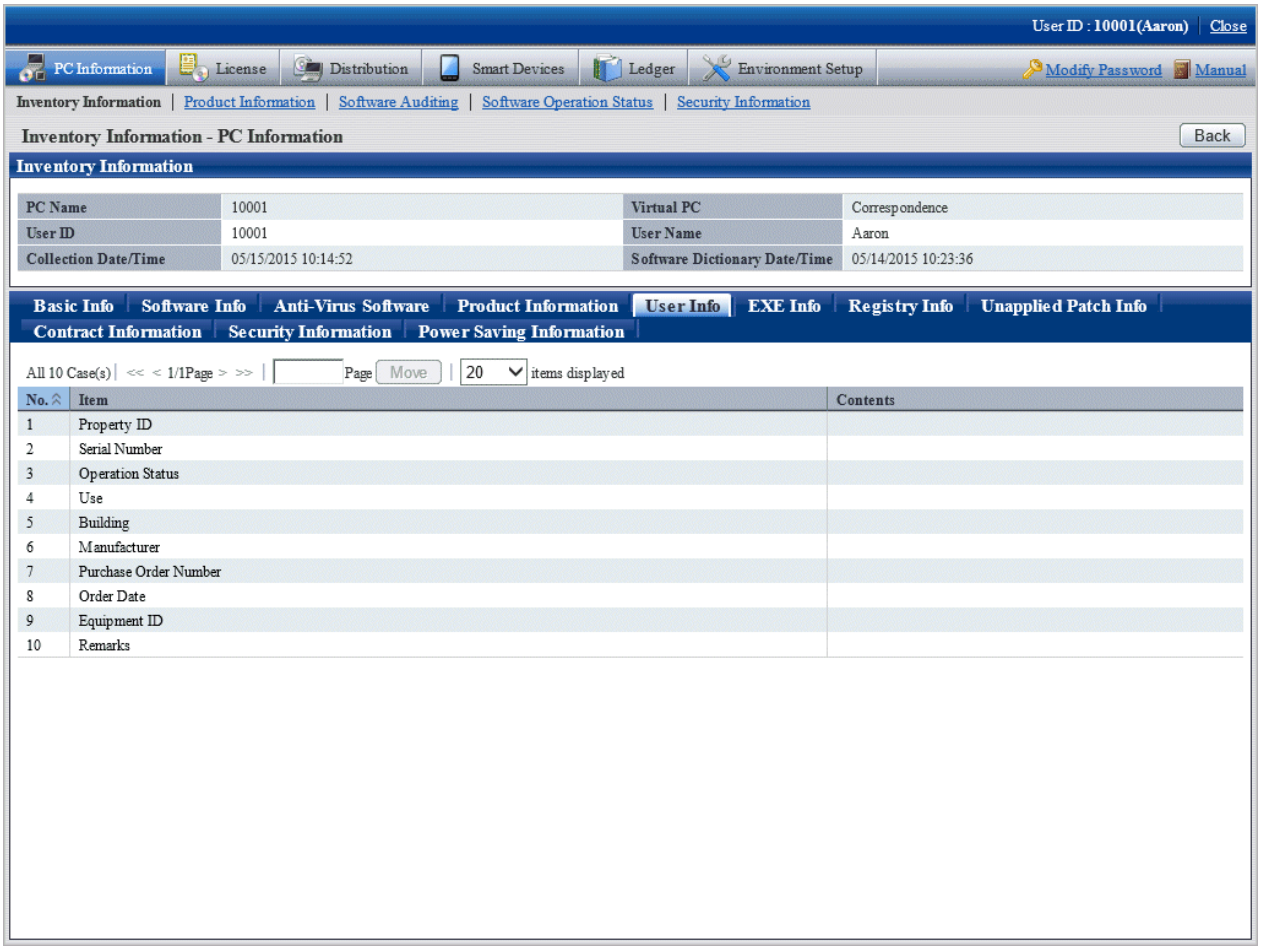
When Product Information **is selected**

Product information will be displayed. The software displayed in a part of **Uninstall a program** and **View installed updates** in **Add or Remove Programs** or **Programs and Features** on the selected PCs can be viewed.



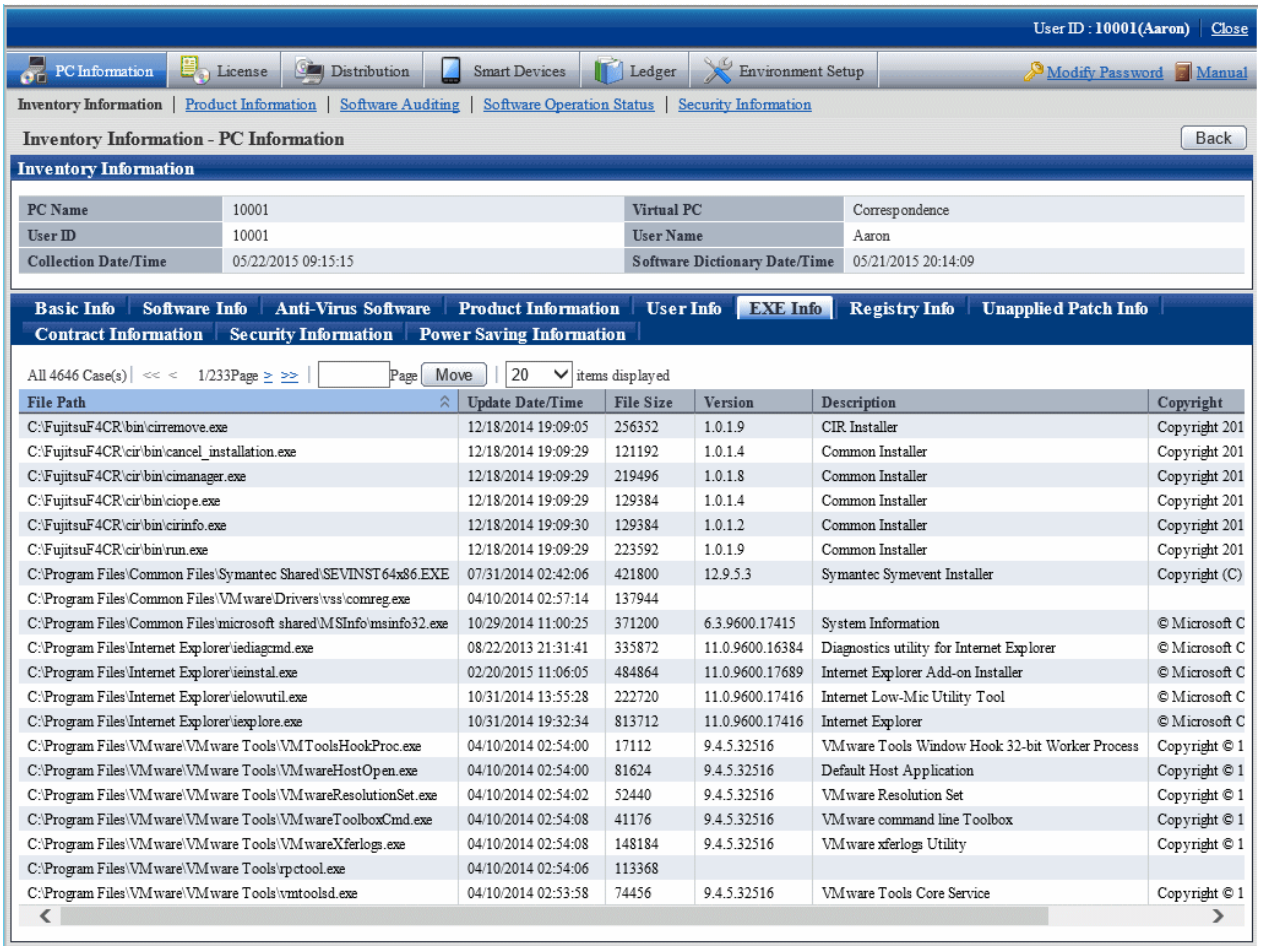
When User Info **is selected**

User information will be displayed. The user information of PC can be viewed.



When EXE Info **is selected**

EXE information will be displayed. The absolute path of the executable file (extension is .exe) on the selected PC can be viewed.



Point

If a collected file path exceeds 127 fullwidth characters or 380 halfwidth characters, the middle portion of the file path will be omitted when the path is collected and displayed, as in the example below.

Example:

```
C:\...(:::)...:1234ABCD1234ABCD1234ABCD
```

C:\... Lead portion of the path

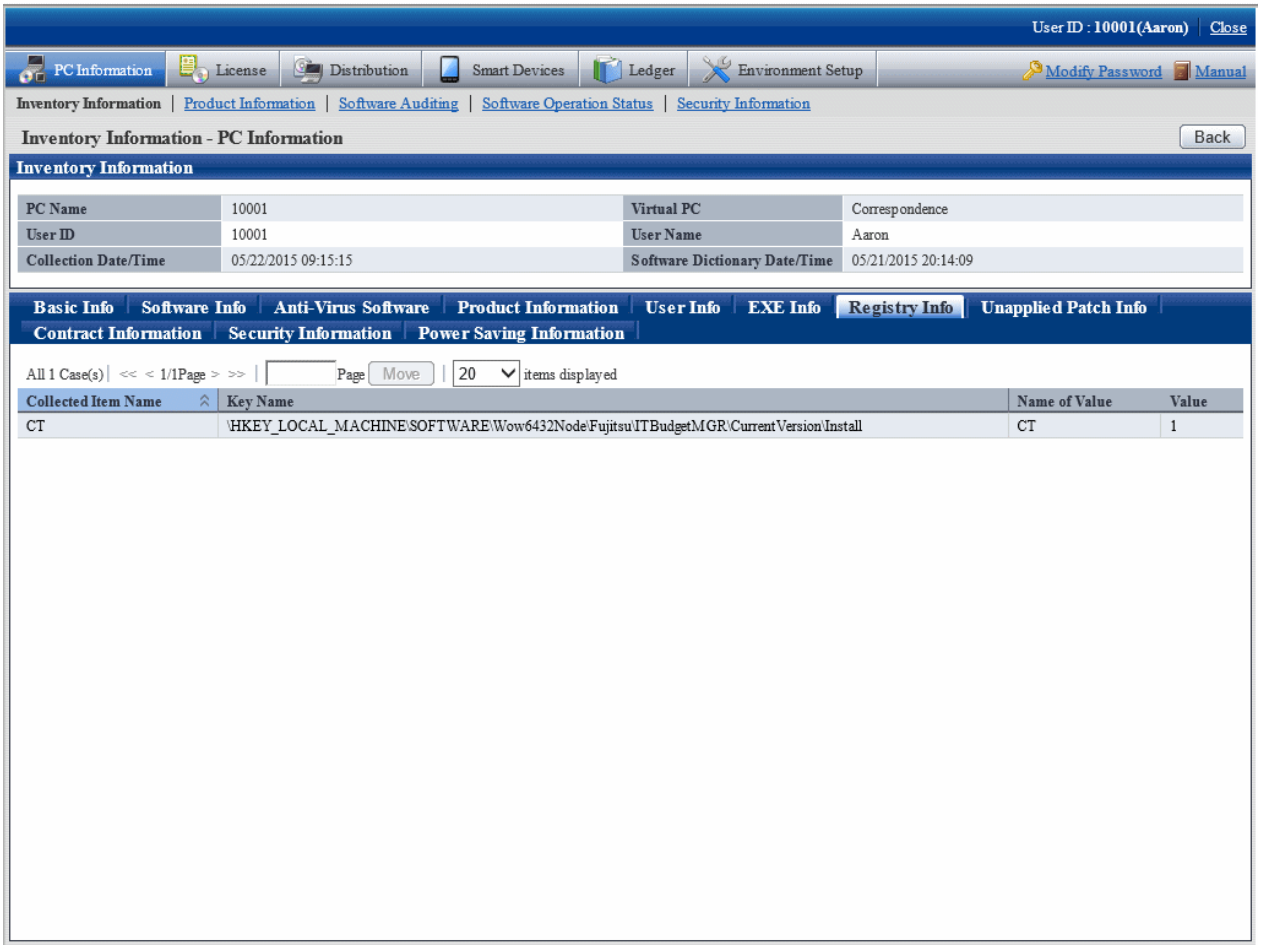
(:::) Symbol indicating omission

... End portion of the path

:1234ABCD1234ABCD1234ABCD Unique string (25 characters) for each file

When Registry Info **is selected**

The registry information will be displayed. The registry information collected from the selected PC can be viewed.

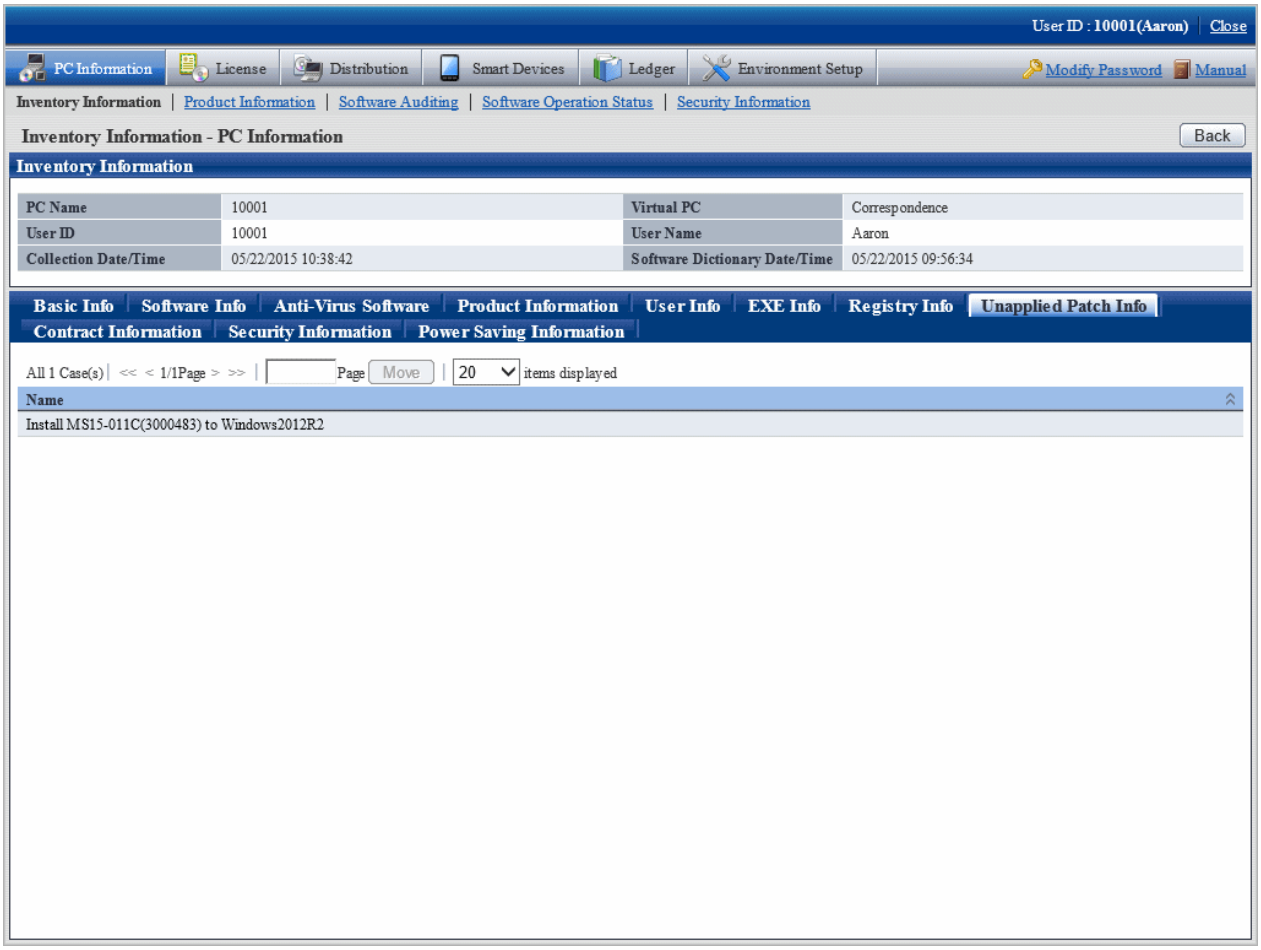


Description of the items in the above window is as follows.

Item	Description
Collection Item Name	Display the **Collection Item Name** defined in the main menu.
Key Name	Display the **Key Name** defined in the main menu.
Name of Value	Display the **Value Name** defined in the main menu.
Value	Display the registry information collected from CT.

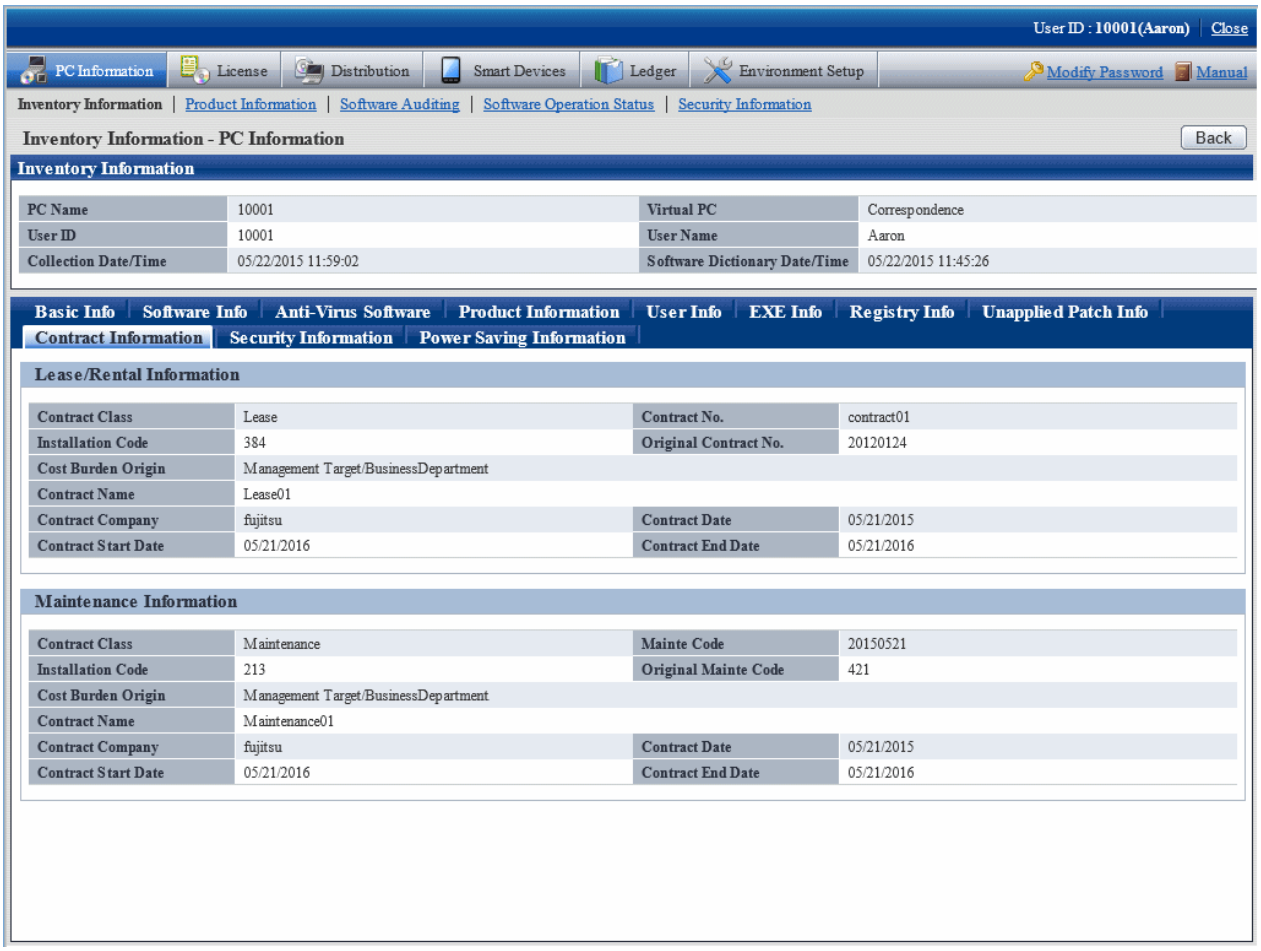
When Unapplied Patch Info **is selected**

The information of patch that is not installed to CT can be viewed in the patch of automatic installation target.



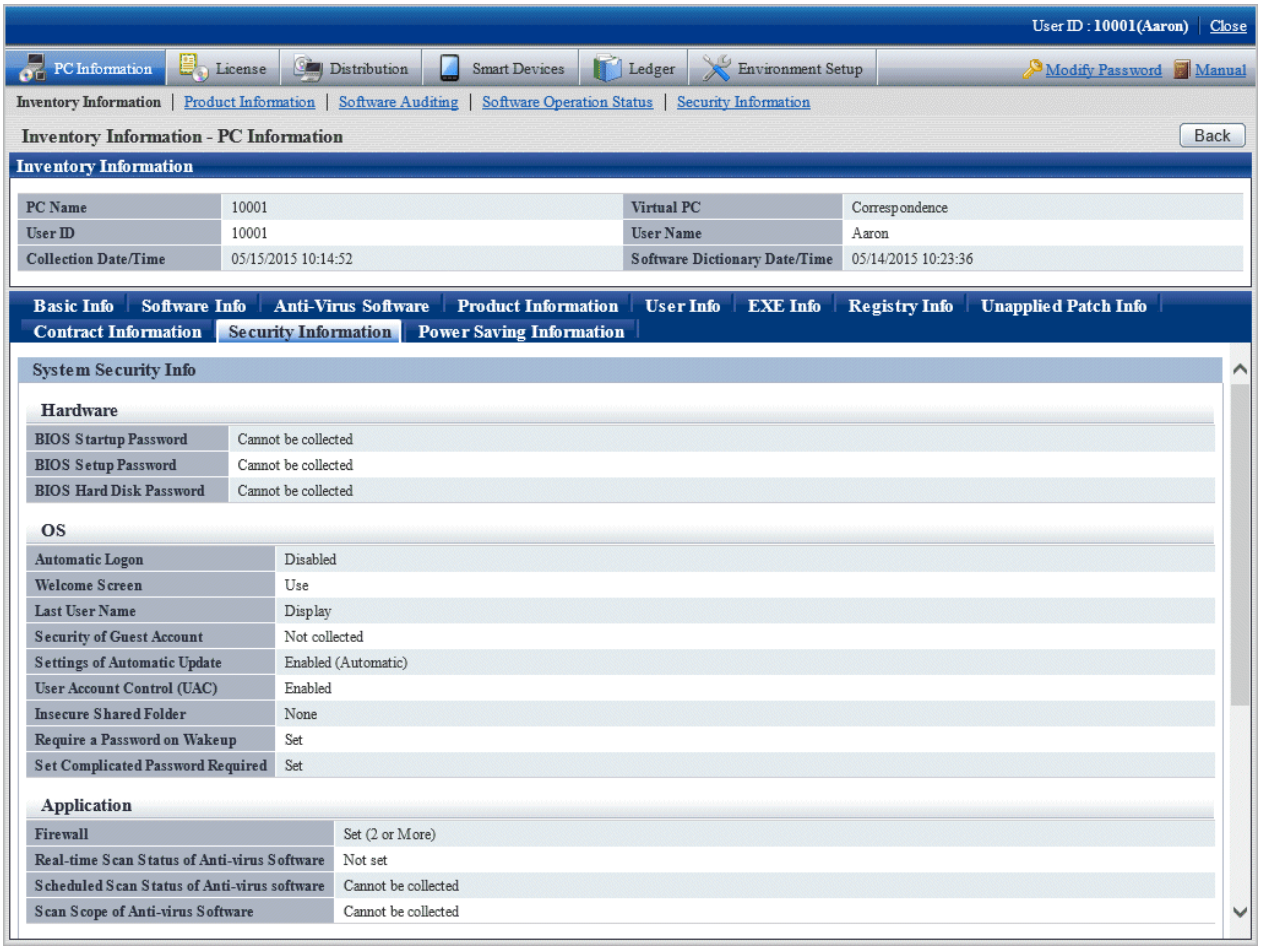
When Contract Information **is selected**

The contract information will be displayed.



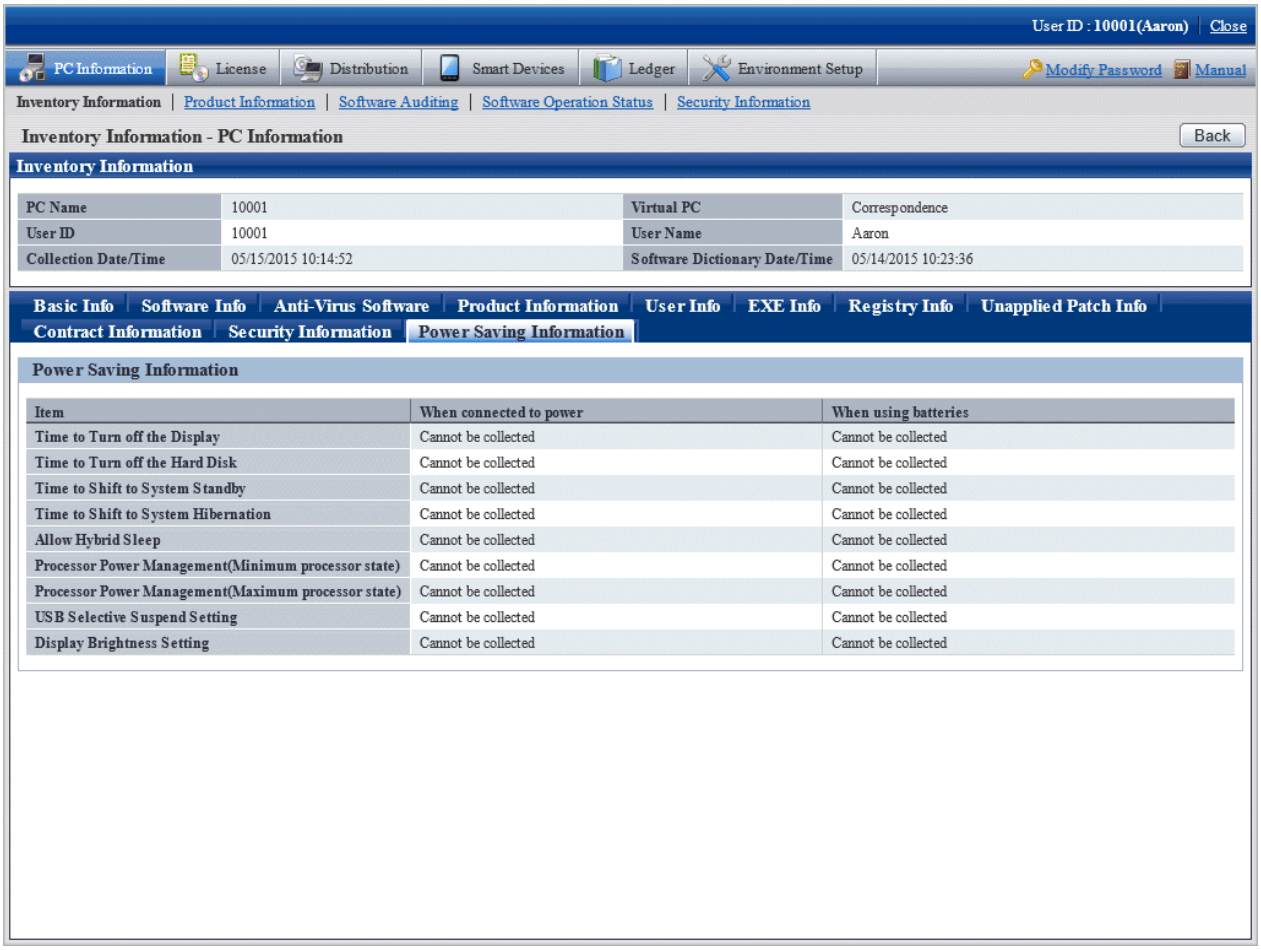
When Security Information **is selected**

The security information will be displayed.



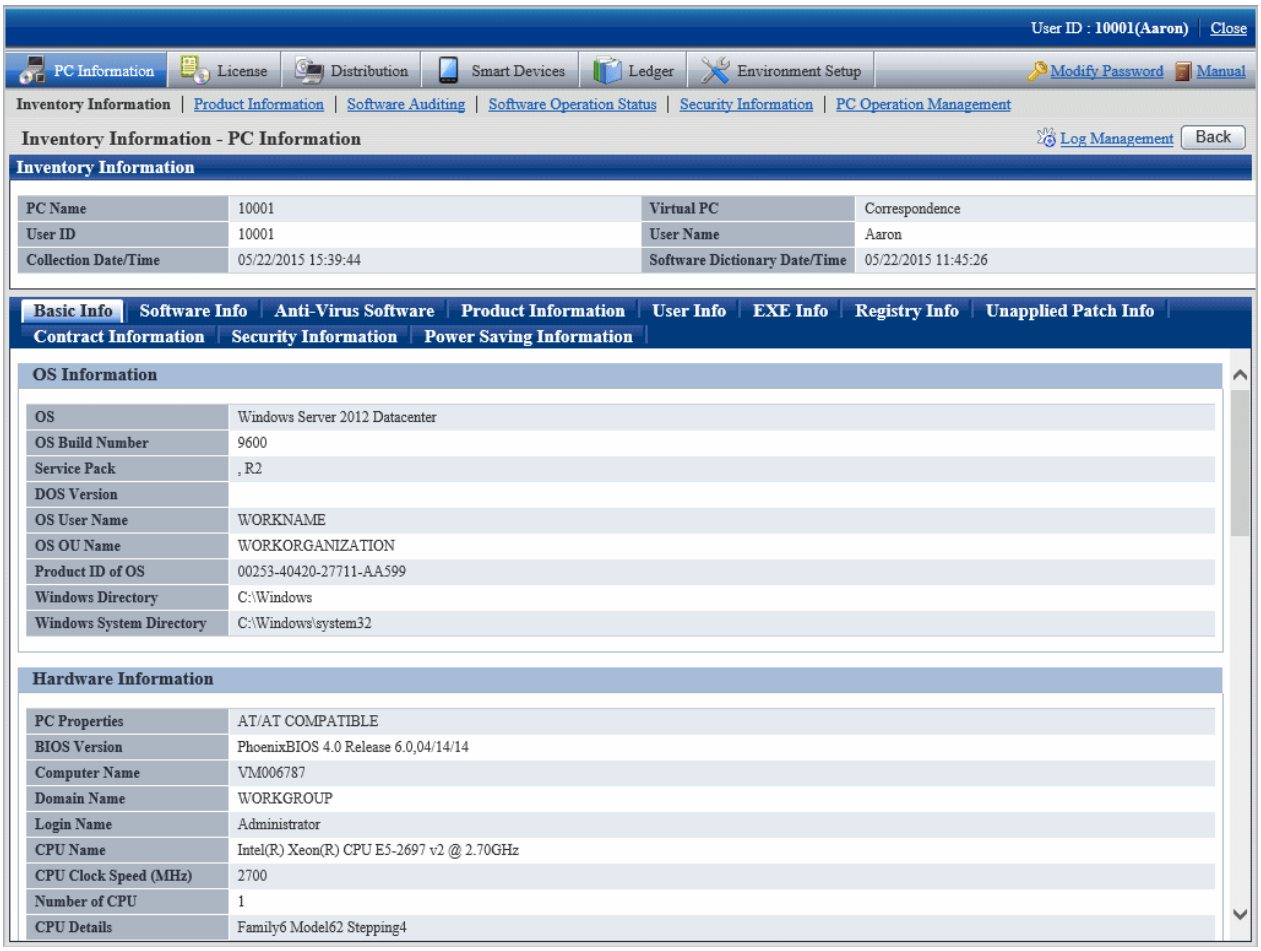
When Power Saving Information **is selected**

The power saving information will be displayed.



Display the log search window of Systemwalker Desktop Keeper

Through selecting the **Log Management** link displayed in the **Inventory Information - PC Information** window, the log search window of the same user ID/same PC name managed in Systemwalker Desktop Keeper can be displayed in a new window.



If **Option** > **Settings of Status** > **URL of Desktop Keeper** is not set in advanced or the automatic authentication of login ID when logged in to the main menu was failed, the link of **Log Management** will not be displayed.

In the log search window of Systemwalker Desktop Keeper that is displayed, log search can be performed. For details of the log search window, refer to *Systemwalker Desktop Keeper User's Guide: For Administrators*.

Point

When multiple the log search windows displayed in the new window are displayed for each PC, click the **Customized Level** button in the zone of use from the **Network Options** of the Web browser being used and modify the **Move window and frame between different domains** to **Enable**, so that the display of multiple windows can be avoided.

How to view after searching

By searching for PC and selecting the PC displayed in window, the inventory information can be viewed.

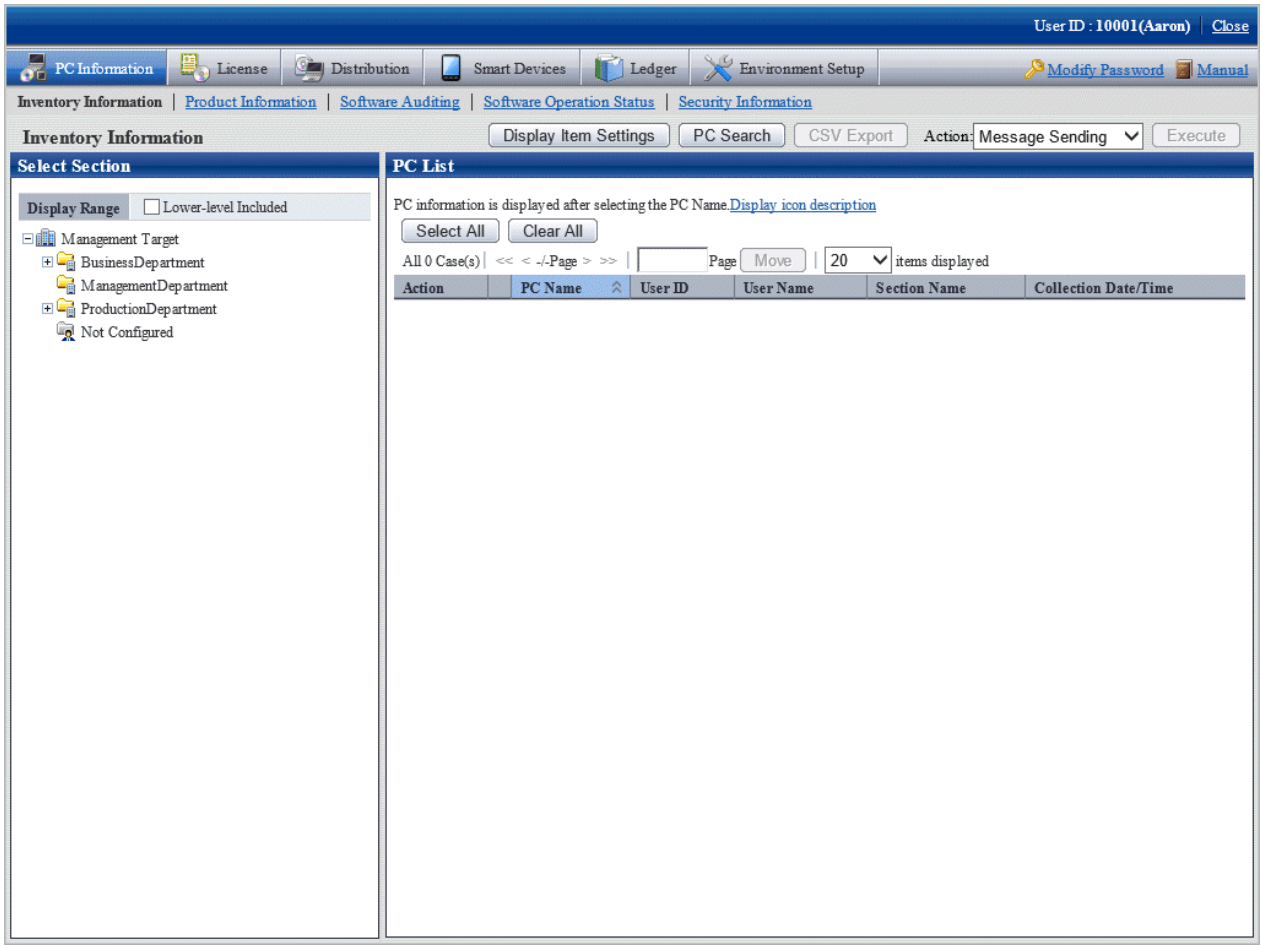
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

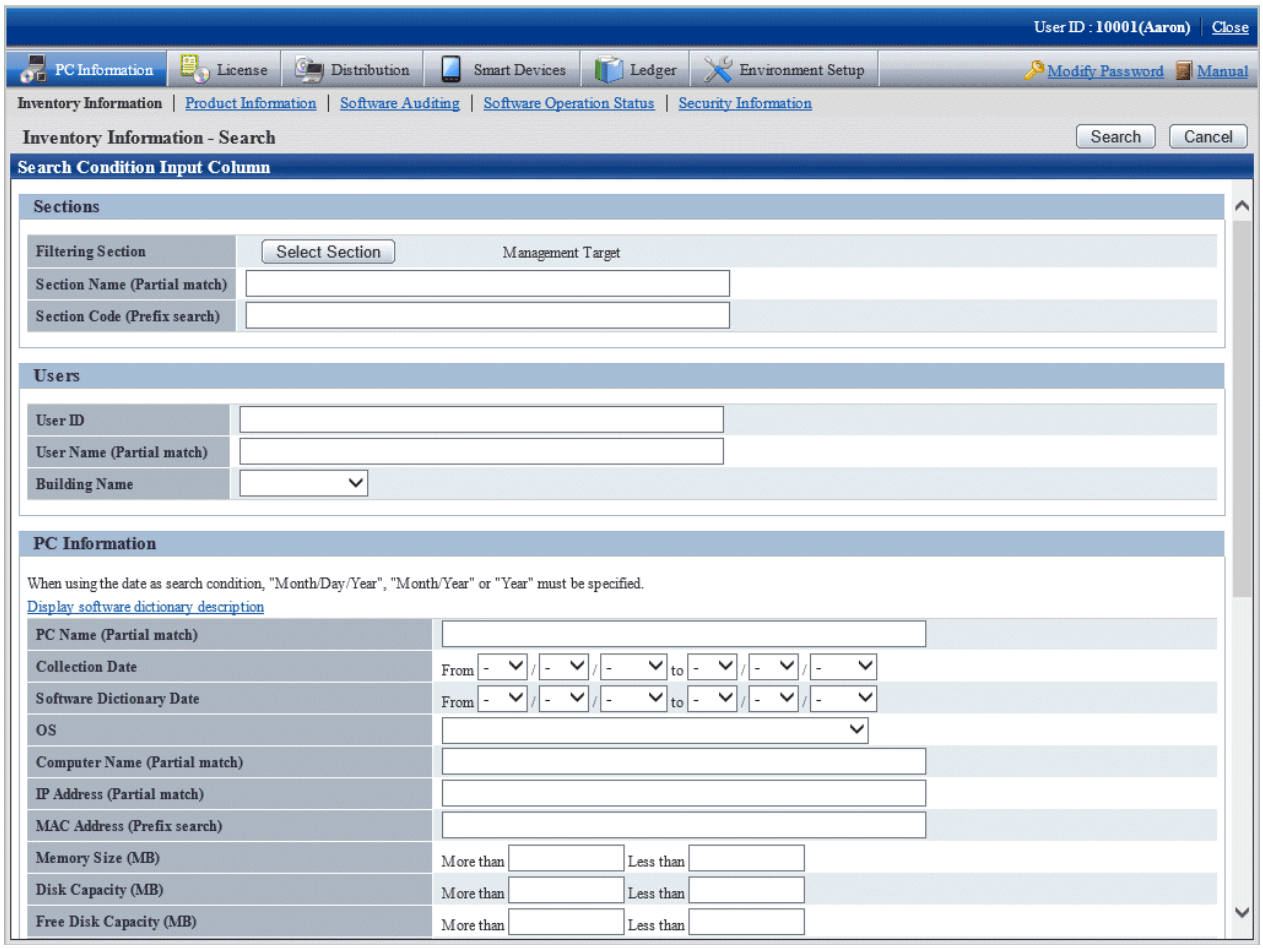
2. Click **Inventory Information**.

   The following window will be displayed.

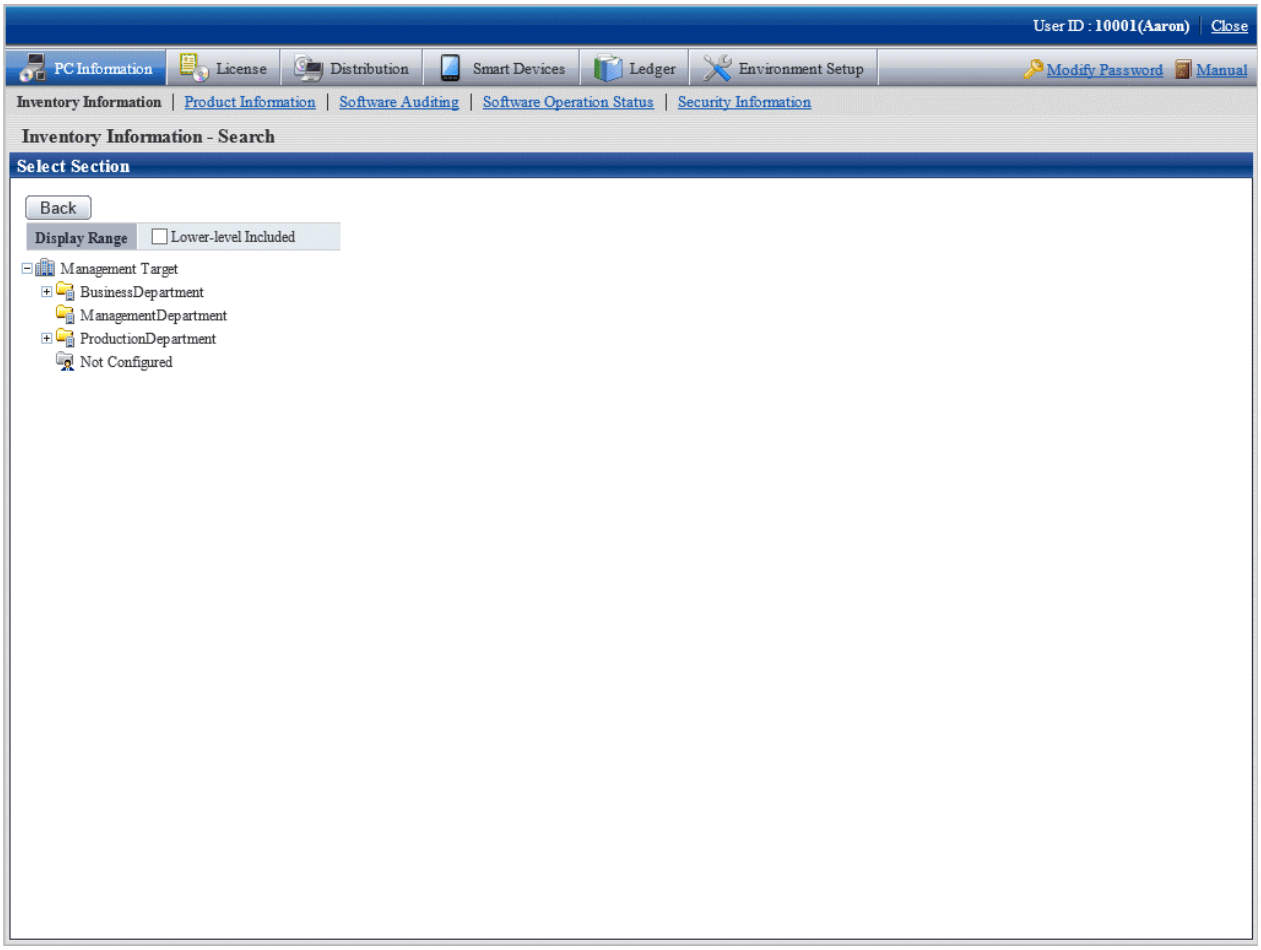


3. Click the **PC Search** button.

   The following window will be displayed.

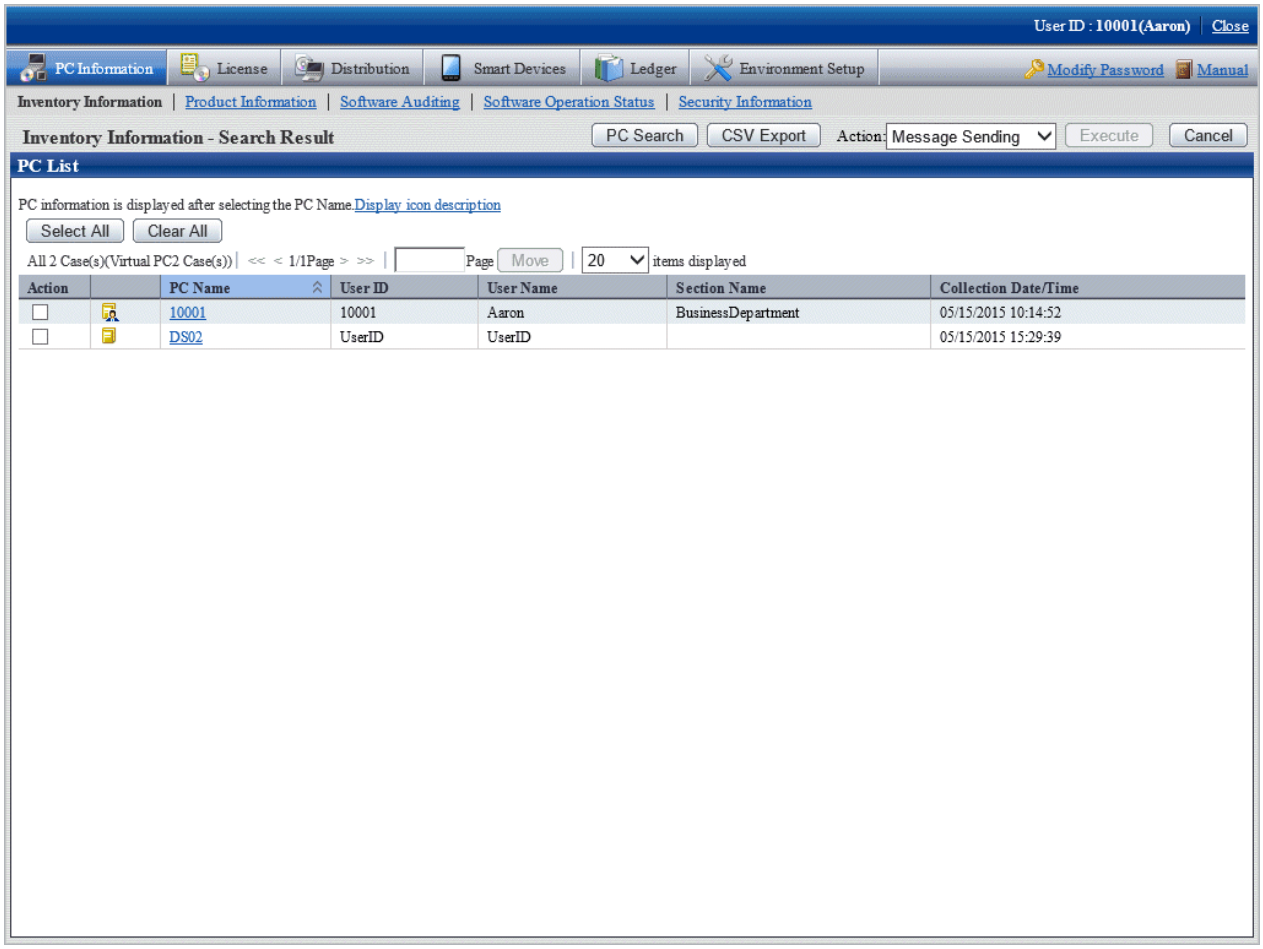


4. Click the **Select Section** button, the following window will be displayed.



5. Enter the information to search PC and click the **Search** button.

   The search result will be displayed.



6. When the hardware information of PC shown in the field on the right is output to the file in CSV format, perform the following procedure. When not to output, proceed to the next step.

   a. Click the **CSV Export** button.

   b. Output the hardware information to a file in CSV format according to the window.

7. Click the displayed PC name.

   The inventory information of the clicked PC will be displayed.

8. Select the displayed item.

   The selected window will be displayed. For the display window, refer to "How to view from section tree".

Point

For **IP Address (Partial match)**, specify ":" to include only IPv6 addresses, or "." to include only IPv4 addresses. If the target is an alphanumeric such as "10", the search will include both IPv4 addresses and IPv6 addresses.

IP addresses are searched according to the display priority specified in **Option** > **Display settings**.

How to modify the items displayed in the PC list

The default items displayed in the **PC List** of the **Inventory Information** window can be modified.

For inventory items except **PC Name**, the item can be displayed/hidden in the **PC List** freely.

This modification can be made only after login with system account, and only one setting can be performed in the system.

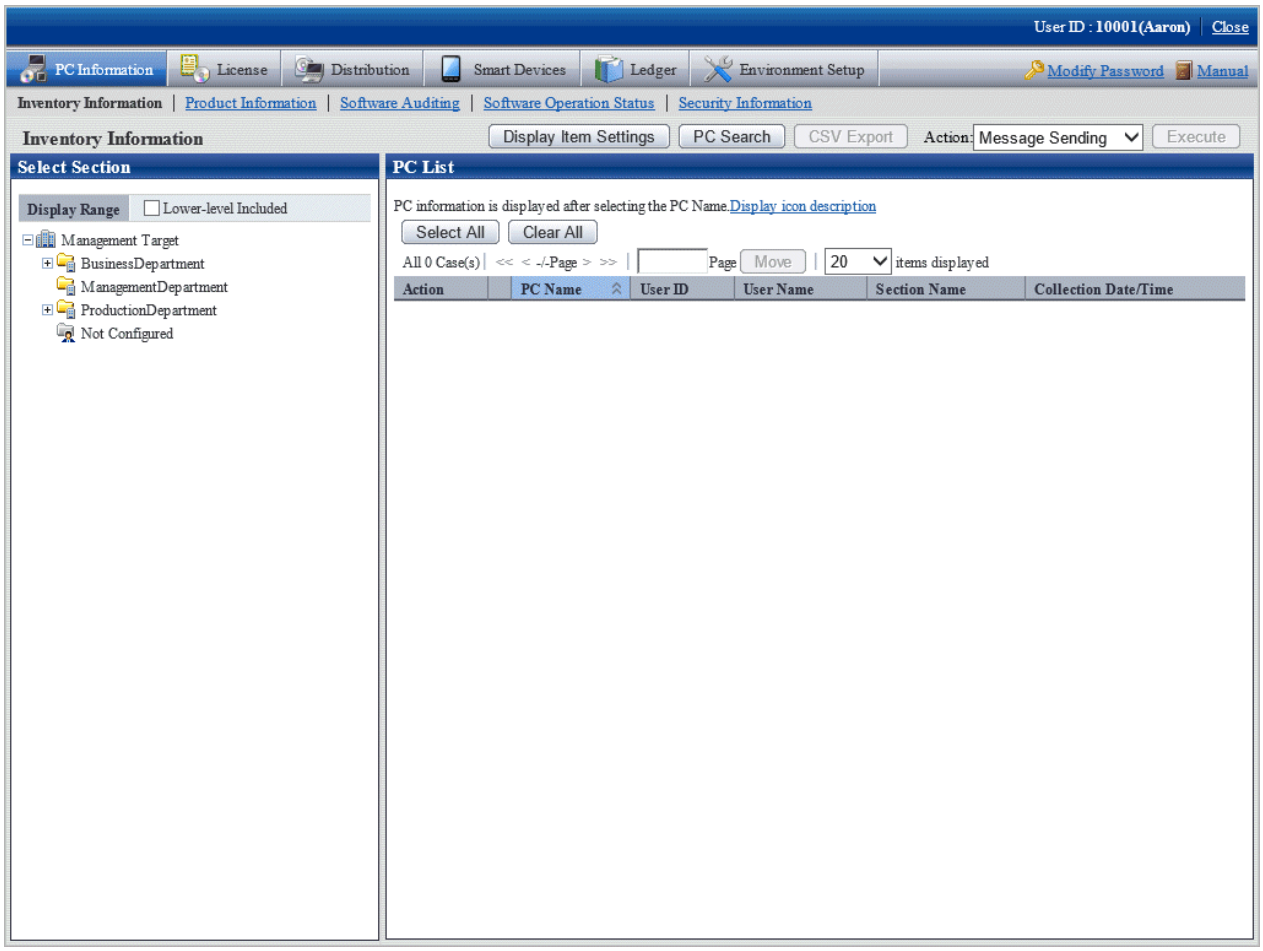
The procedure of modifying the displayed item is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

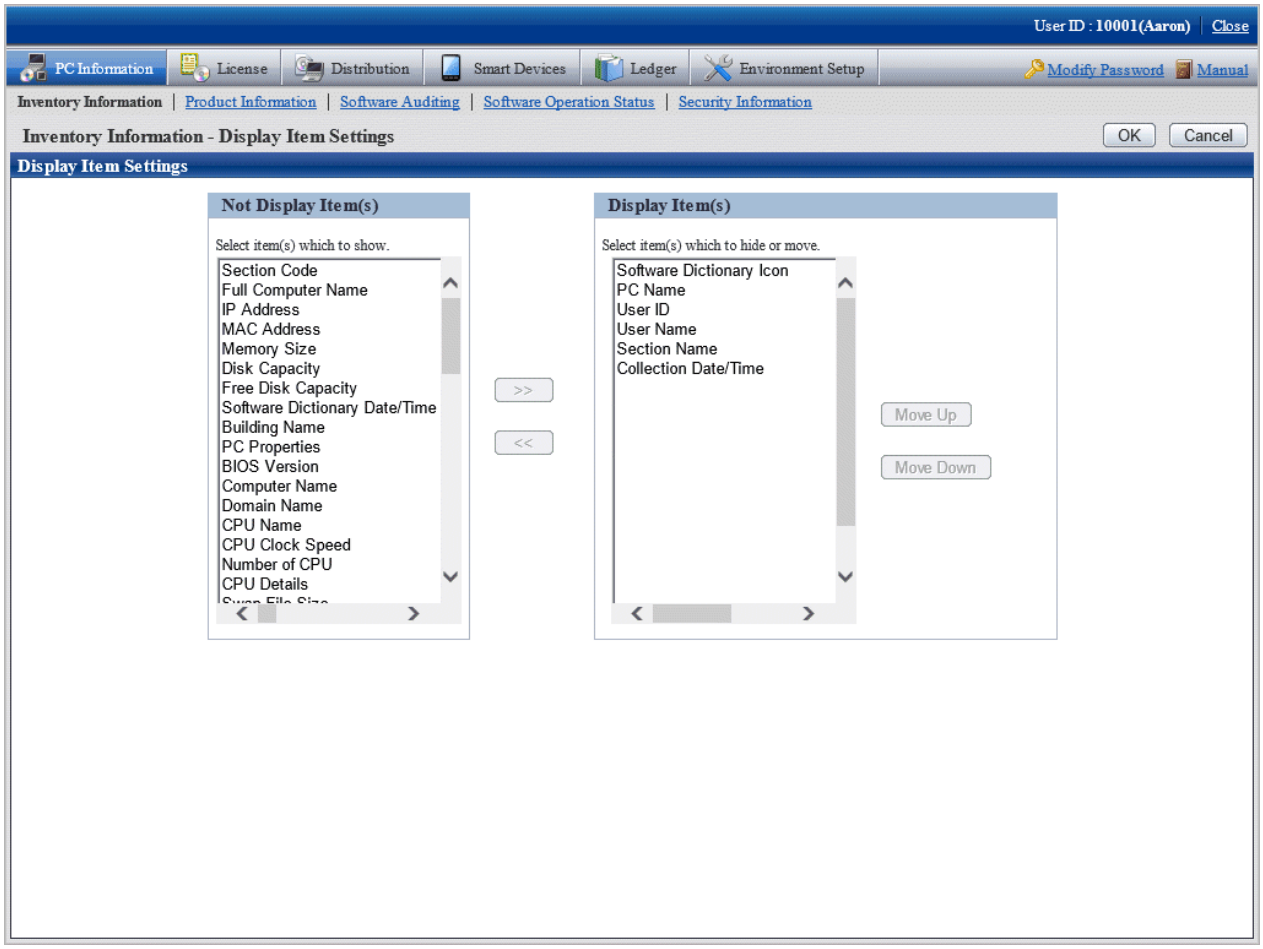
2. Click **Inventory Information**

   The following window will be displayed.



3. Click the **Display Item Settings** button. When logging in with an account that is not system account, the **Display Item Settings** button will not be displayed.

   The following window will be displayed.



4. Perform the setting of displayed items according to the following procedure.

   a. Select the item to be displayed in the PC List from the list of **Not Display Item(s)** on the left of window and click the [>>] button in the center of window. Multiple items can be selected.

      The selected items will be added to the **Display Item(s)** on the right of window.

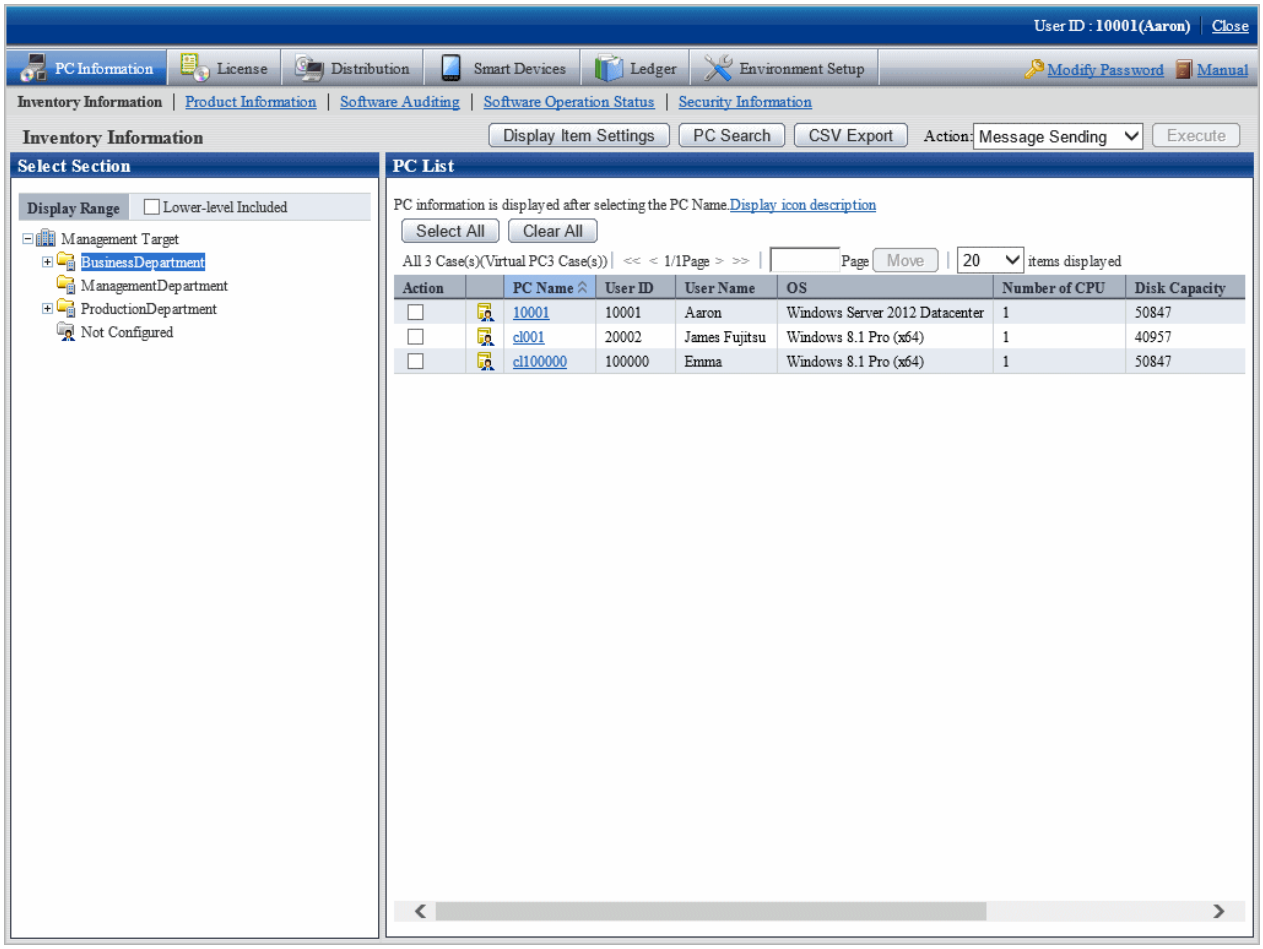
   b. Select the item that does not need to be displayed in the PC list from the list of **DisplayItem(s)** on the right of window and click the [<<] button in the center of window. Multiple items can be selected.

      The selected item will be deleted from the **Display Item(s)** on the right of window.

   c. To modify the sequence of **Display Item(s)**, select items from the list of **Display Item(s)** on the right of window and click the **Move Up** or **Move Down** button.

5. After the setting displayed items has completed, click the **OK** button.

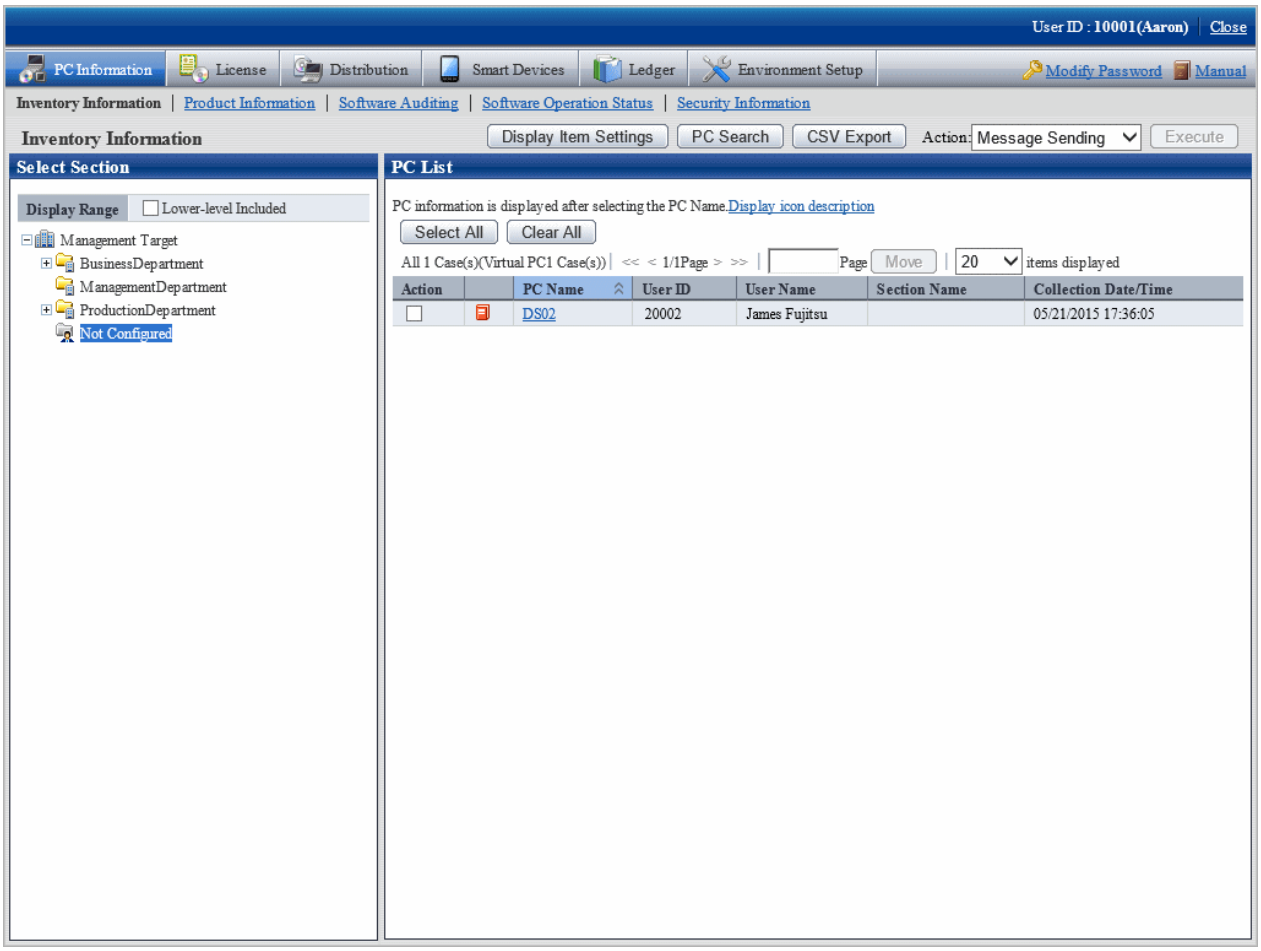
   The items displayed in the PC list will be modified to the items that have been set.



View inventory information of PCs without configuration

A PC without configuration is a PC of the user that is not registered to user management information or a PC of the user that has been deleted in the section tree in **Environment Setup** > **Users** of the main menu.

In the following window, when the section selection tree is in the state that **Not configured** is selected, the PCs displayed in the field on the right are without configuration.



Hardware information of PCs without configuration can be saved to files in CSV format as well. Select **Not configured** in the section tree, click the **CSV Export** button and output according to the window.

In addition, same as the PC of user registered in user management information, inventory information can be viewed.

When PCs without configuration exist, perform the following operations.

- When the PC is required, a PC without configuration can be moved to section in **Environment Setup** > **Users** of the main menu.
- When the PC is not required, a PC without configuration can be deleted in **Environment Setup** > **Users** of the main menu

When PCs without configuration exist, perform the following operations.

1. In **Select section** of entry column of search condition, set selected section to **Not configured**.
2. Output to files in CSV format.
3. Open the file output in CSV format to confirm PC and users, and perform the following operations.
   - When the PC is required
     a. Create the user management information file of the user that owns the PC.
     b. For confirming whether the section to which each user of user management information file belongs is correct, refer to "2.1.5 Create User Management Information" to register a user. When not belonging to a section, refer to "2.1.4 Create Section Management Information" to register a section.
   - When the PC is not required
     a. Create the user management information file of the user that owns the PC.
     b. For confirming whether the section to which each user of user management information file belongs is correct, refer to "2.1.5 Create User Management Information" to delete a user.

How to output CSV files

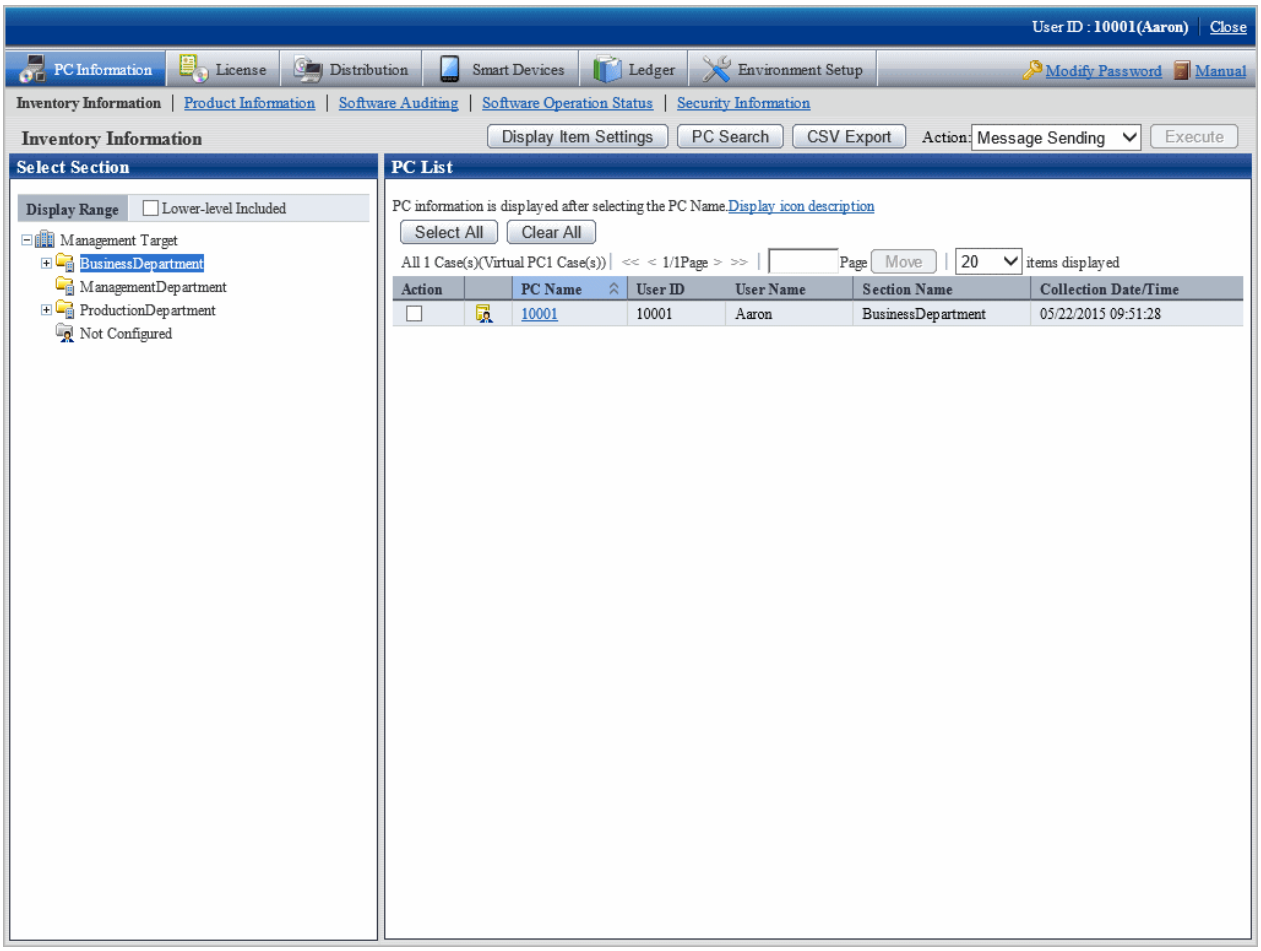
The collected information can be output as CSV file. After searching and refining, the result will be saved to CSV files. When output without searching, all collected information will be saved to CSV files.

To output to CSV file, click the **CSV Export** button to output according to the window.

Operation action

In the inventory information window, the following operation Action can be performed.

- Message Sending
- Inventory Collection
- Inventory Delete



Select the PC that requires processing from the PC list and select the content of processing to be performed from the pull-down menu of **Action**.

Click the **Execute** button and the window for confirming the processing content corresponding to the processing will be displayed. After confirming the content, click the **OK** button.

The corresponding processing will be performed for the selected PC.

About the content of selection item of Processing

In the inventory information window, the following operation Action can be performed (refer to "Operation action", "About the content of selection item of 'Action'" for details).

- Message Sending

- Inventory Collection
- Inventory Delete

3.2.2 Deleting Inventory Information

This section explains how to delete inventory information of PCs no longer required, such as disposed PCs.

Note

On CT, inventory collection is performed with difference collection (default). If inventory information is sent from the CT in question after it has been deleted via the main menu, the information that has not been sent will not be displayed.

If you want to delete inventory information but keep the CT in question installed, inventory information can still be collected using the procedures below:

- Manually perform inventory collection on PCs for the CT in question (refer to "Sending Inventory Information to the Upstream Server" in the *Systemwalker Desktop Patrol Operation Guide for Clients* for details).
- Select **PC Information** in the main menu and then the CT, and execute the actions described in "Inventory Collection" (refer to "Operation action" for details on the actions in "Inventory Collection").

To check the PCs on which inventory information is deleted, refer to the CS operation details log.

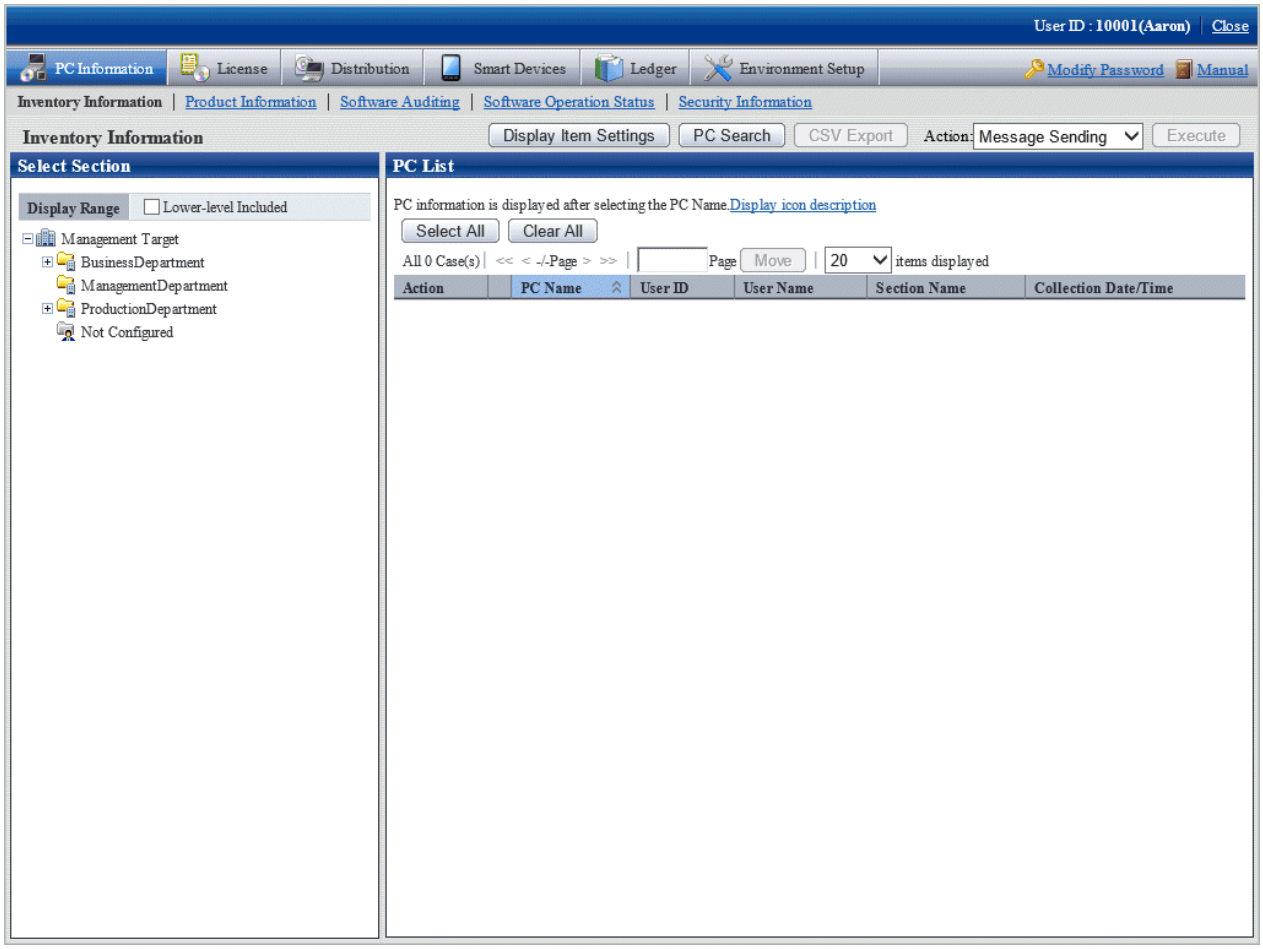
Delete inventory information from the section tree

Inventory information can be deleted by clicking a node in the section tree, then selecting the PC and deleting its inventory information.

Follow the steps below:

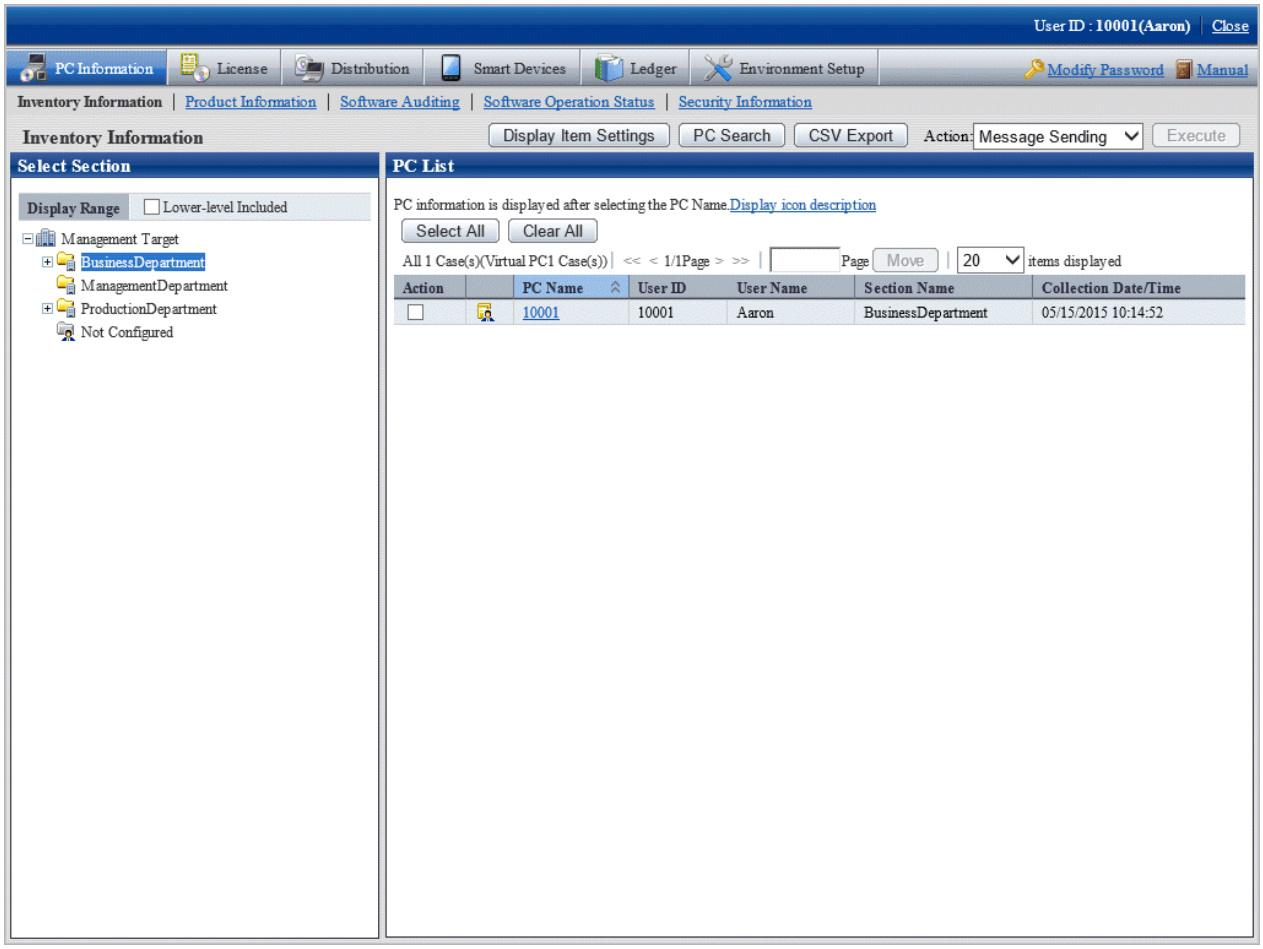
1. Log in to the main menu and click **PC Information**.

   The following window will be displayed.



2. In the left pane, select a section.

   The PCs in the selected section will be displayed in the right pane.



3. Select the PC that contains the inventory information to be deleted.
4. In **Action,** select **Inventory Delete,** and then click **Execute**.

   Inventory information on the selected PCs will be deleted.

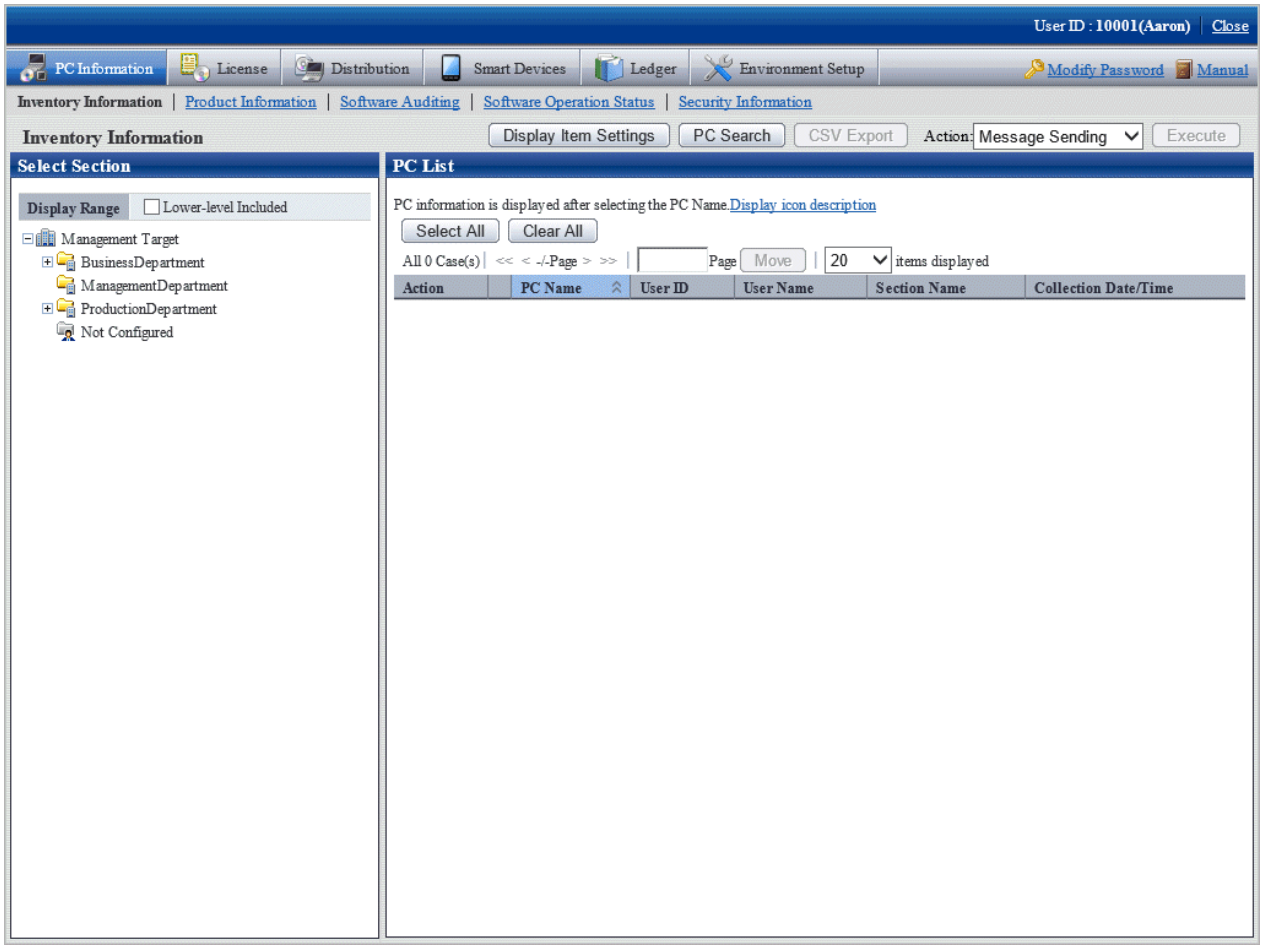
Delete inventory information after search

Inventory information can be deleted by searching for the PC and then deleting its inventory information.

Follow the steps below:

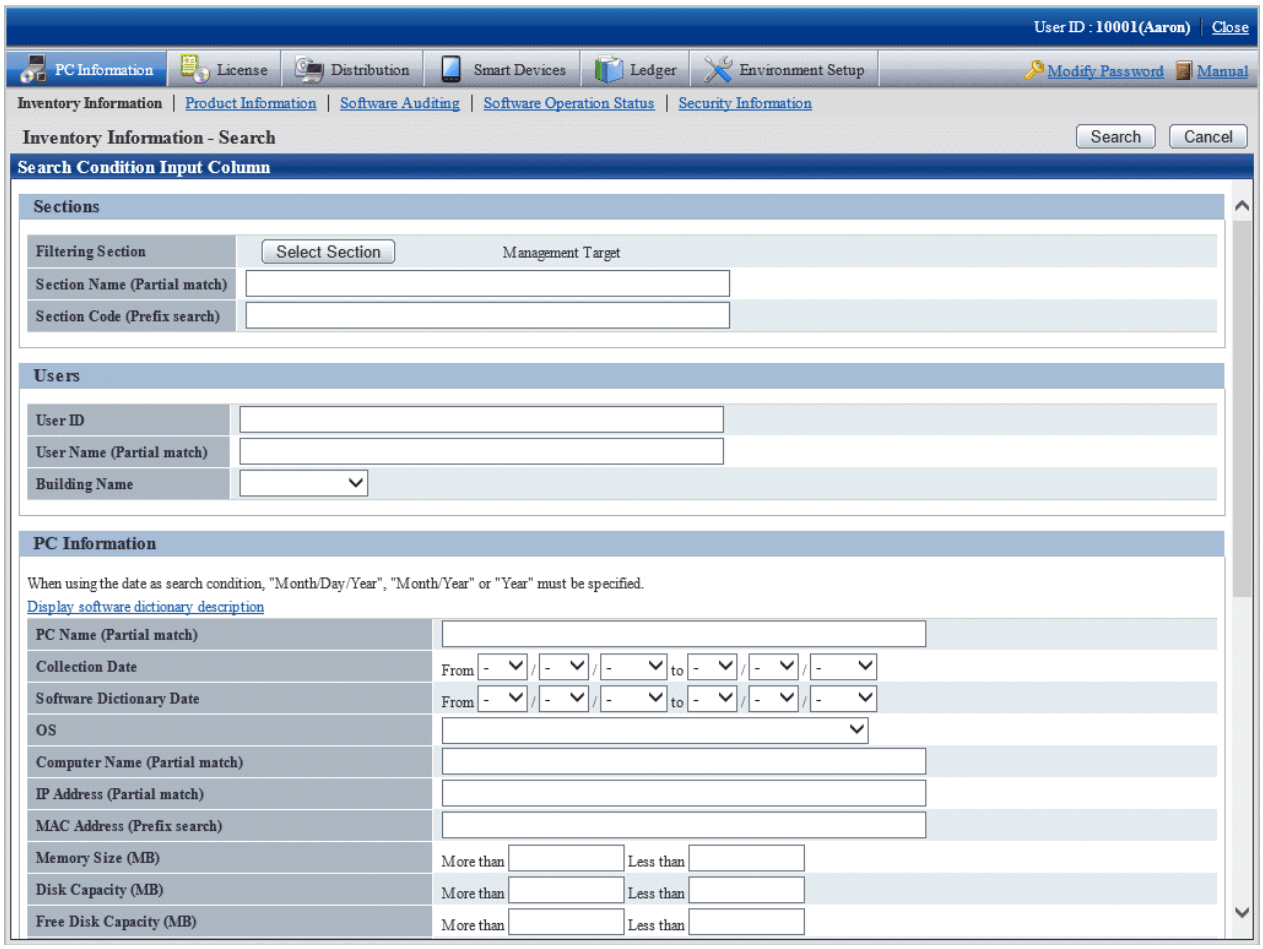
1. Log in to the main menu and click **PC Information**.

   The following window will be displayed.

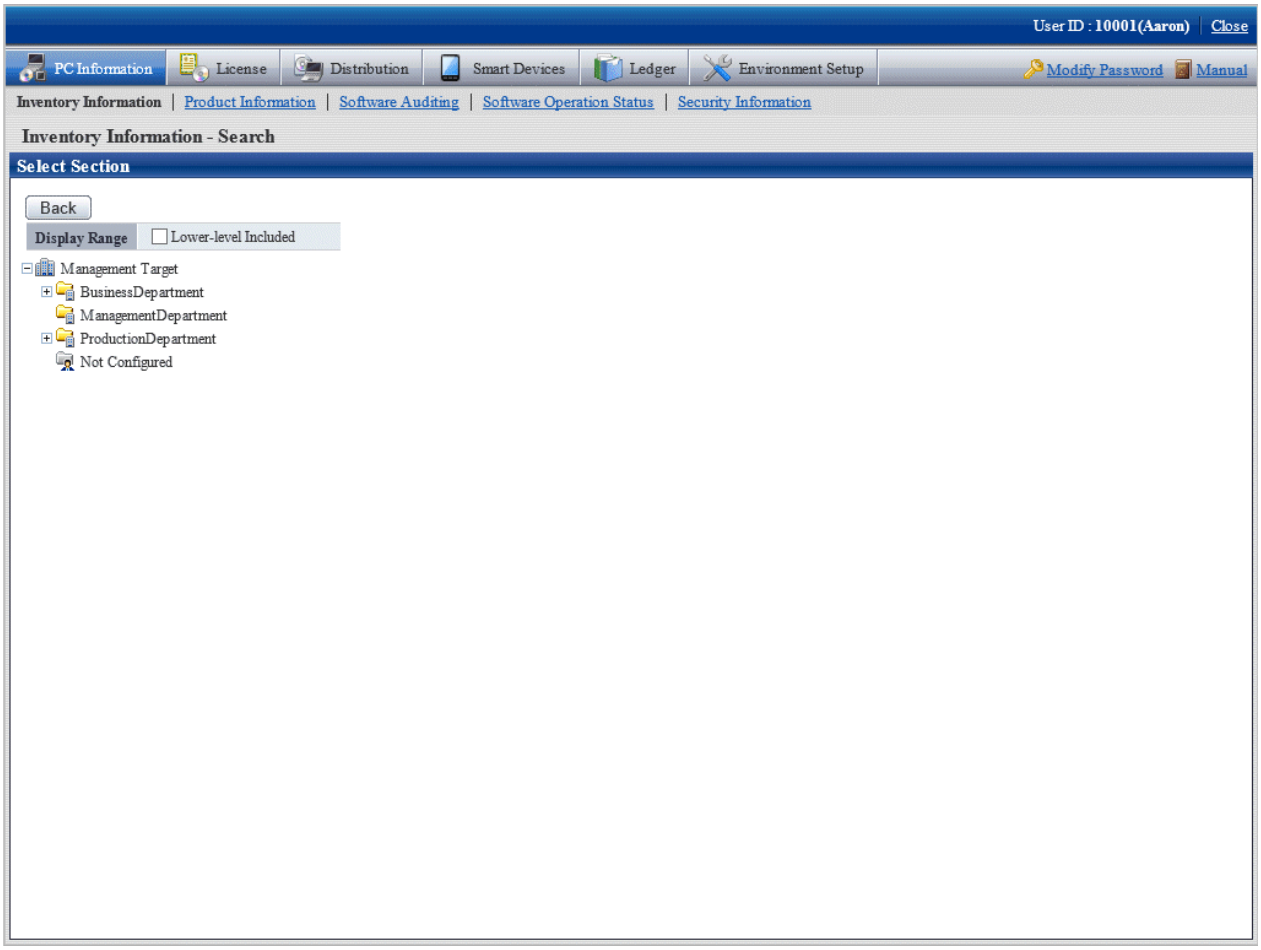


2. Click **PC Search**.

   The following search condition window will be displayed.

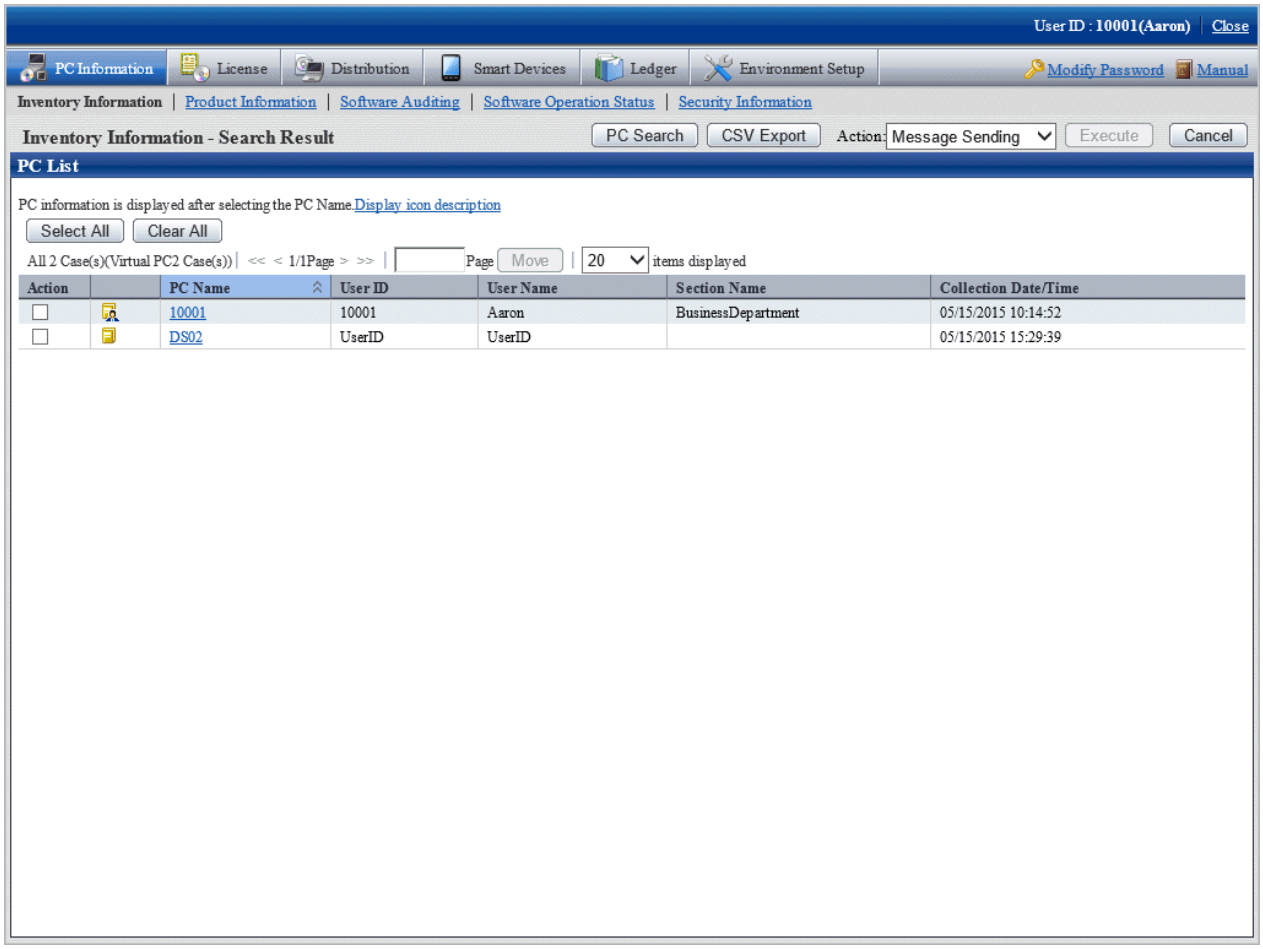


3. If you click **Select Section**, the following window will be displayed.



4. Specify the search conditions, and then click **Search**.

   The following window will be displayed, listing the PCs that match the specified conditions.



5. Select the PC that contains the inventory information to be deleted, then in **Action**, select **Inventory Delete**, and then click **Execute**.

   Inventory information on the selected PC will be deleted.

3.2.3 Viewing the Product Information

The product information of CT can be confirmed according to the collected inventory information. In addition, the product information can also be saved to files in CSV format.

How to view

The methods to view PC can be performed from **PC Information** of the main menu. Select PCs displayed in window, the product information can be viewed.

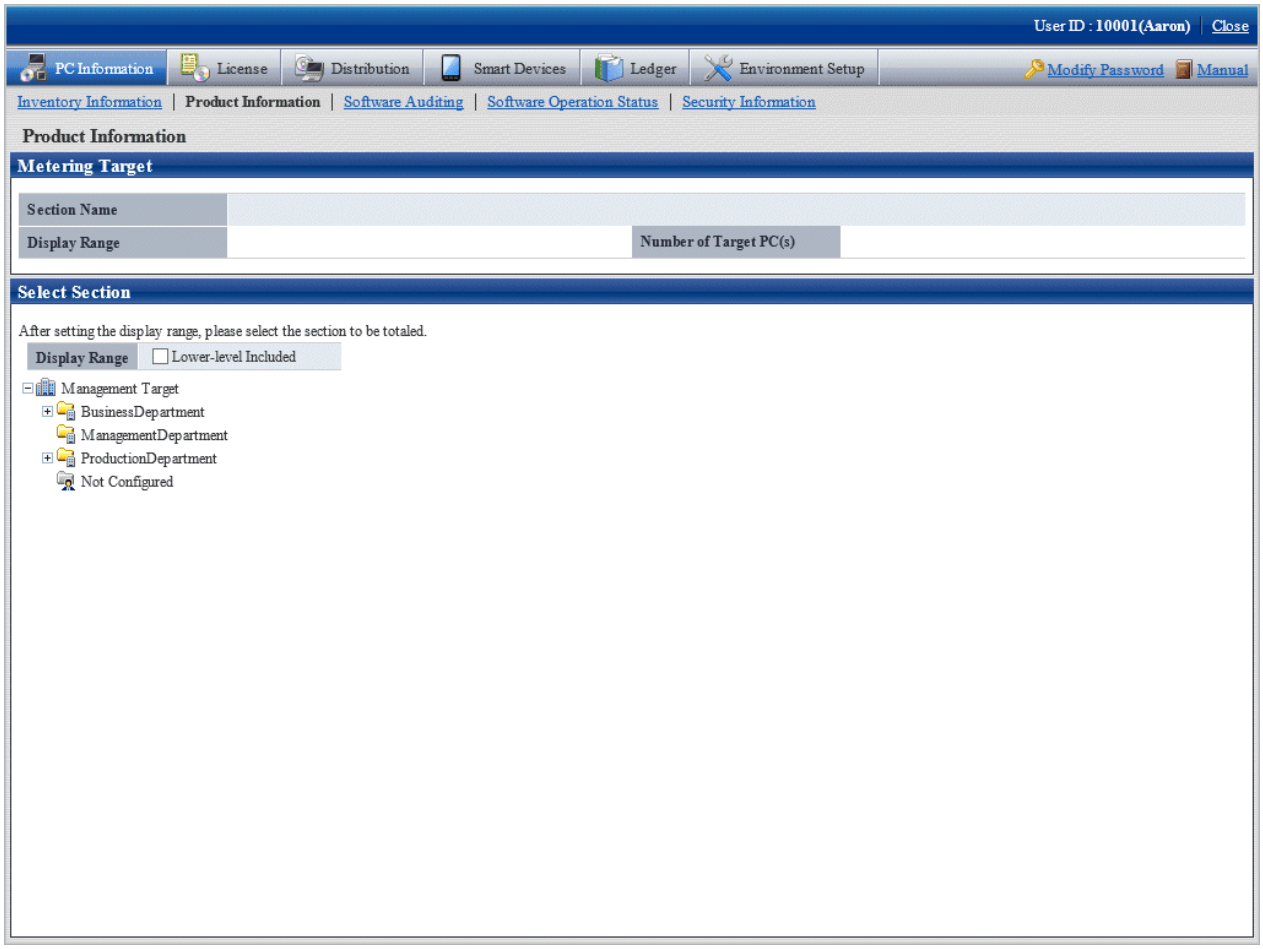
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

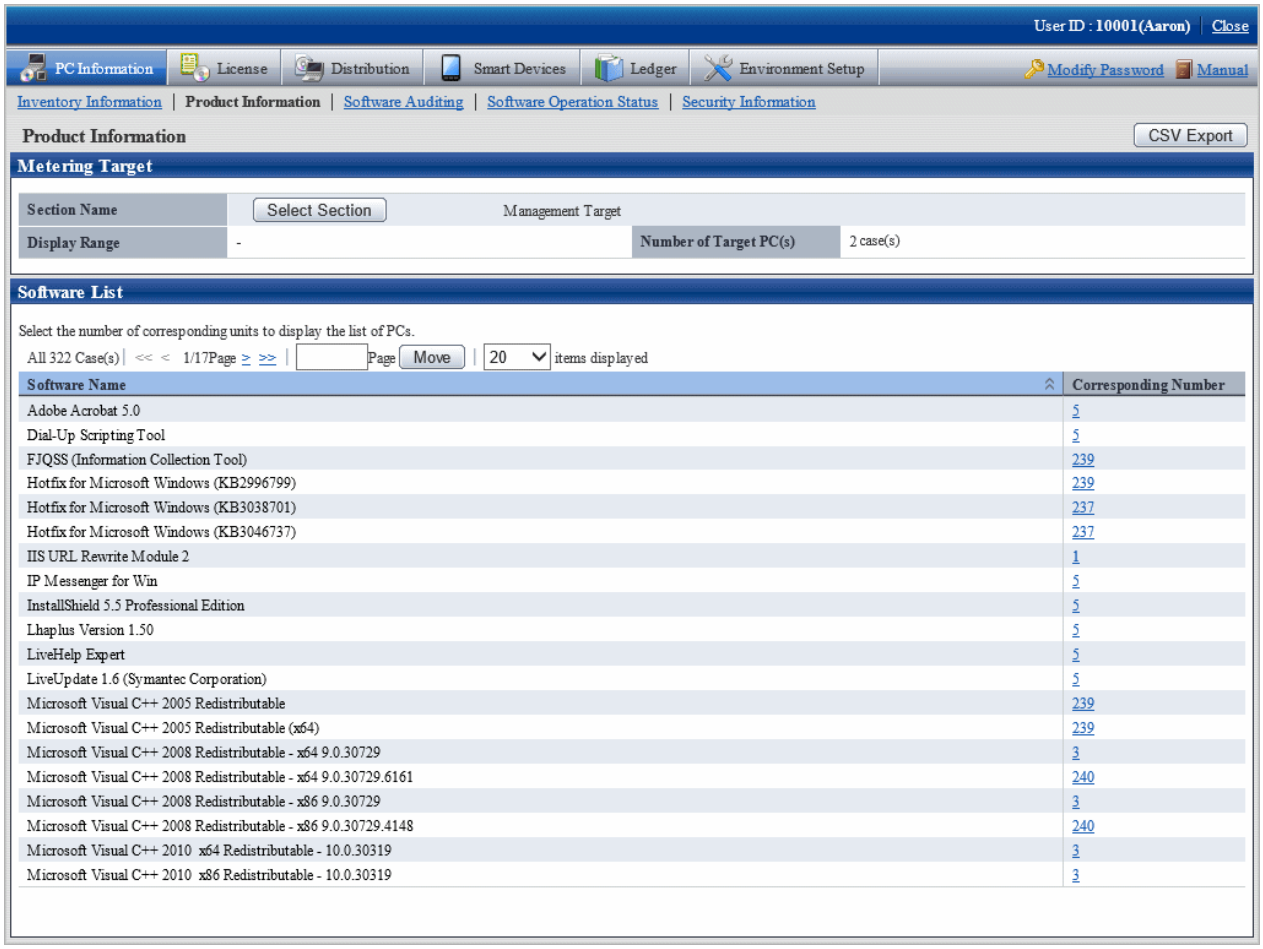
2. Click **Product Information**.

   The following window will be displayed.



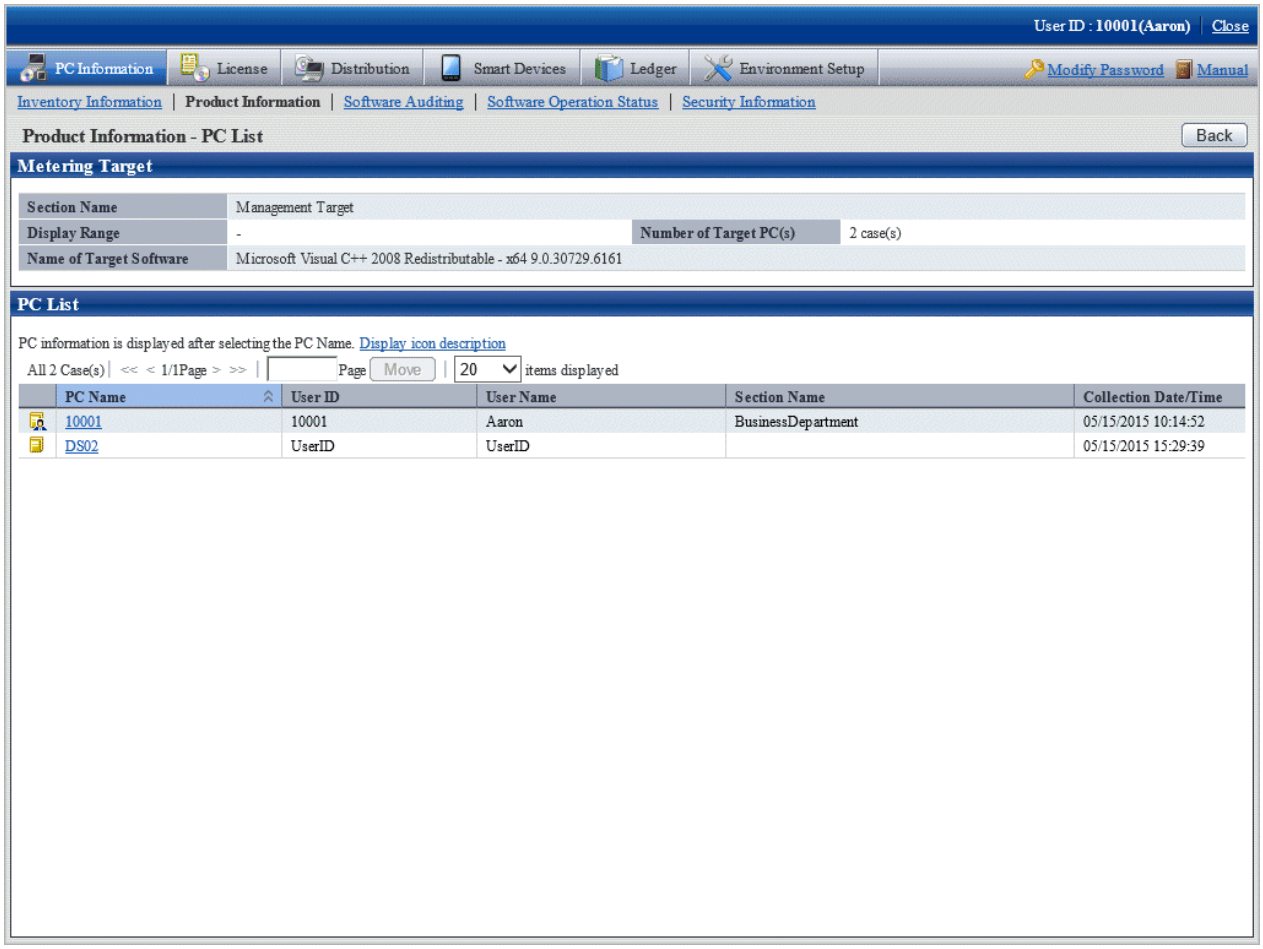
3. Select the section to be displayed.

   The following window will be displayed.



4. Click the Corresponding Number.

   The PC list will be displayed.



5. Click the displayed PC name.

   Inventory information of the clicked PC will be displayed.

6. Select the displayed items.

   The selected window will be displayed. For displayed window, refer to "3.2.1 View Inventory Information".

How to output CSV file

The collected information can be output as CSV file.

To output to CSV file, click the **CSV Export** button to output according to the window.

3.2.4 View Auditing Information of Software

The installation status of software to be audited, the installation status of security patches and installation status of anti-virus software can be confirmed according to the collected information. In addition, this kind of information can also be saved as files in CSV format.

How to view

By selecting the PC displayed in the **PC Information** window of the main menu, the installation status of software to be audited can be confirmed.

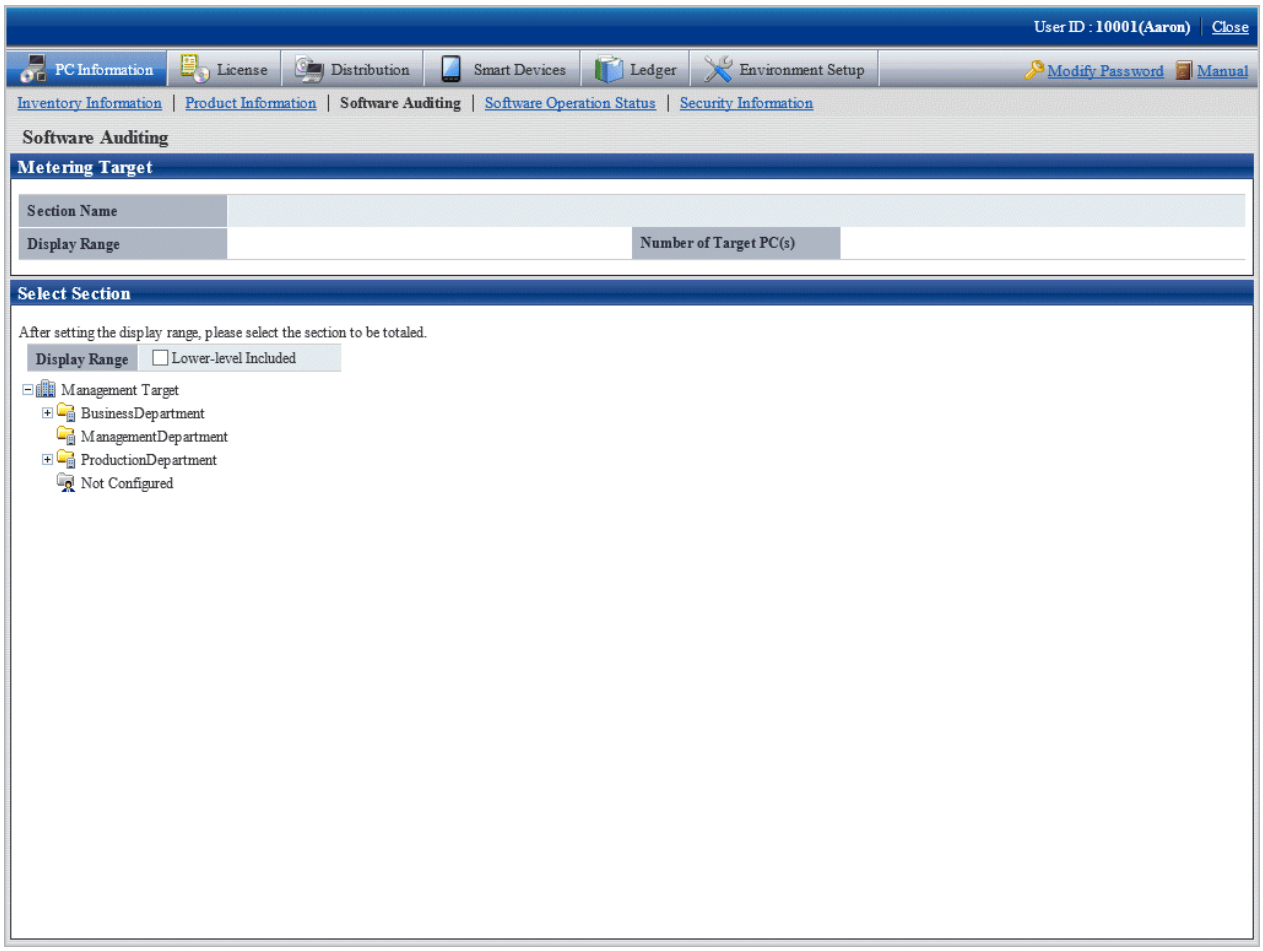
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

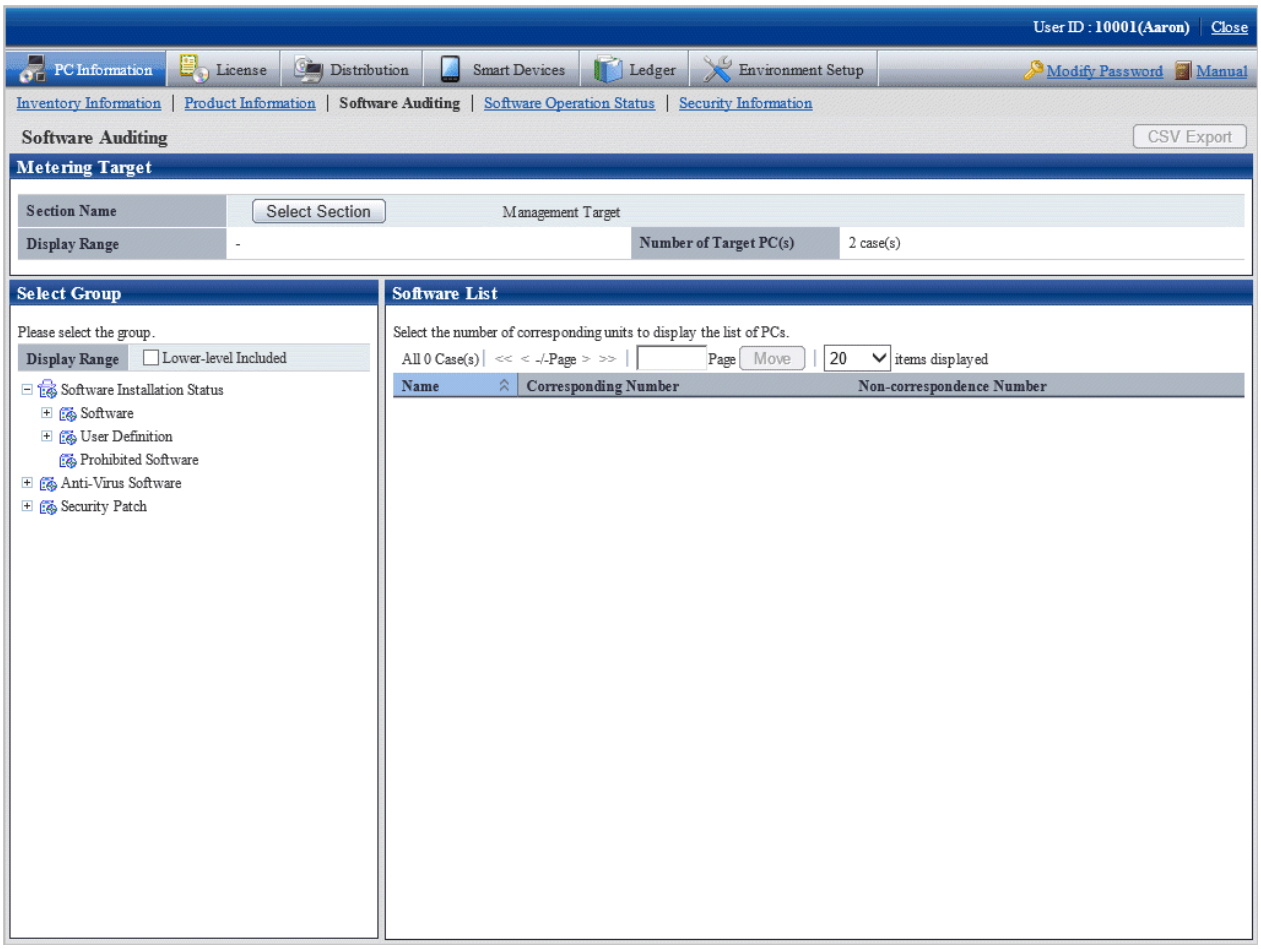
2. Click **Software Auditing**.

   The following window will be displayed.



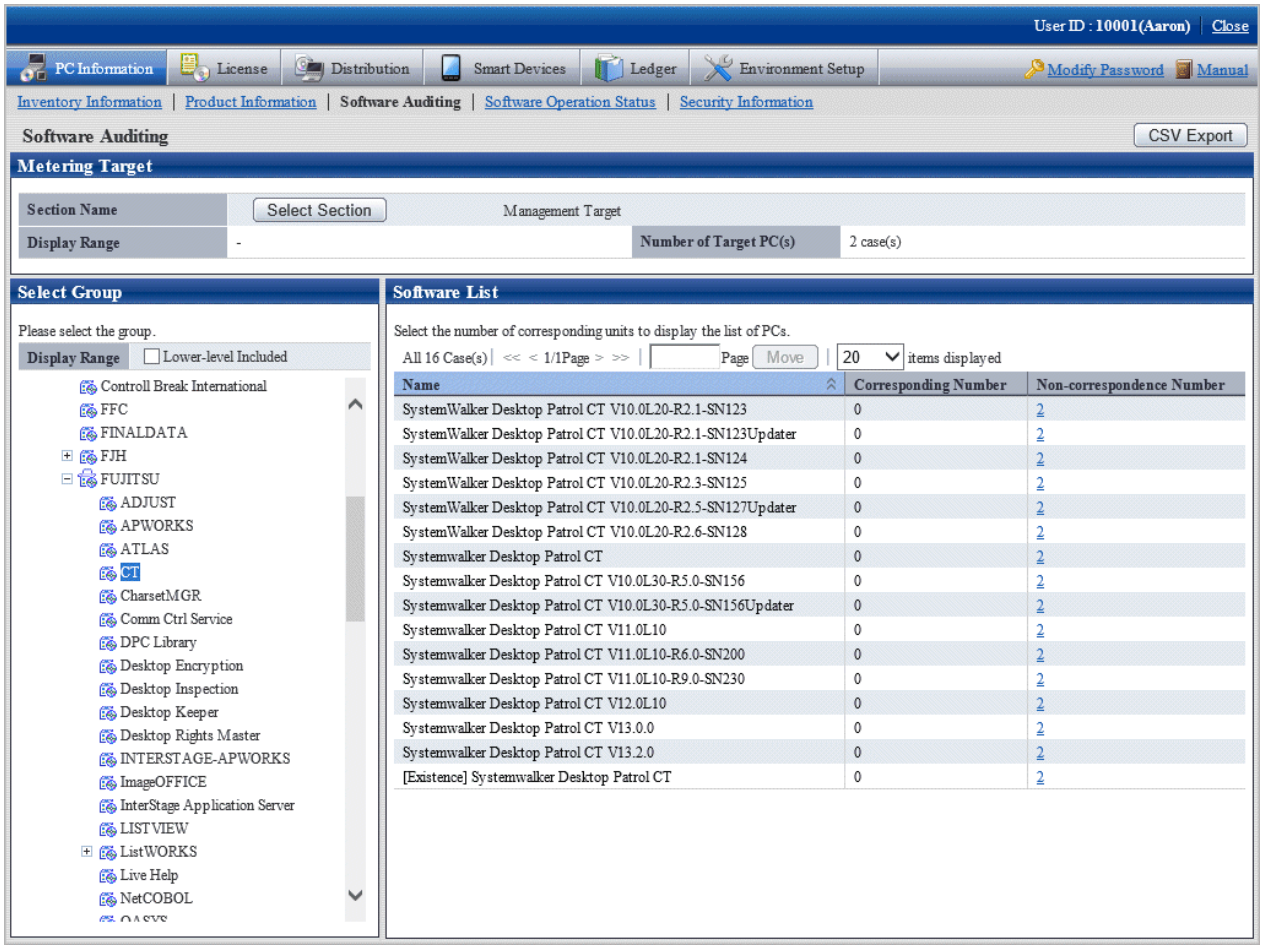
3. Select the section to be displayed.

   The following window will be displayed.



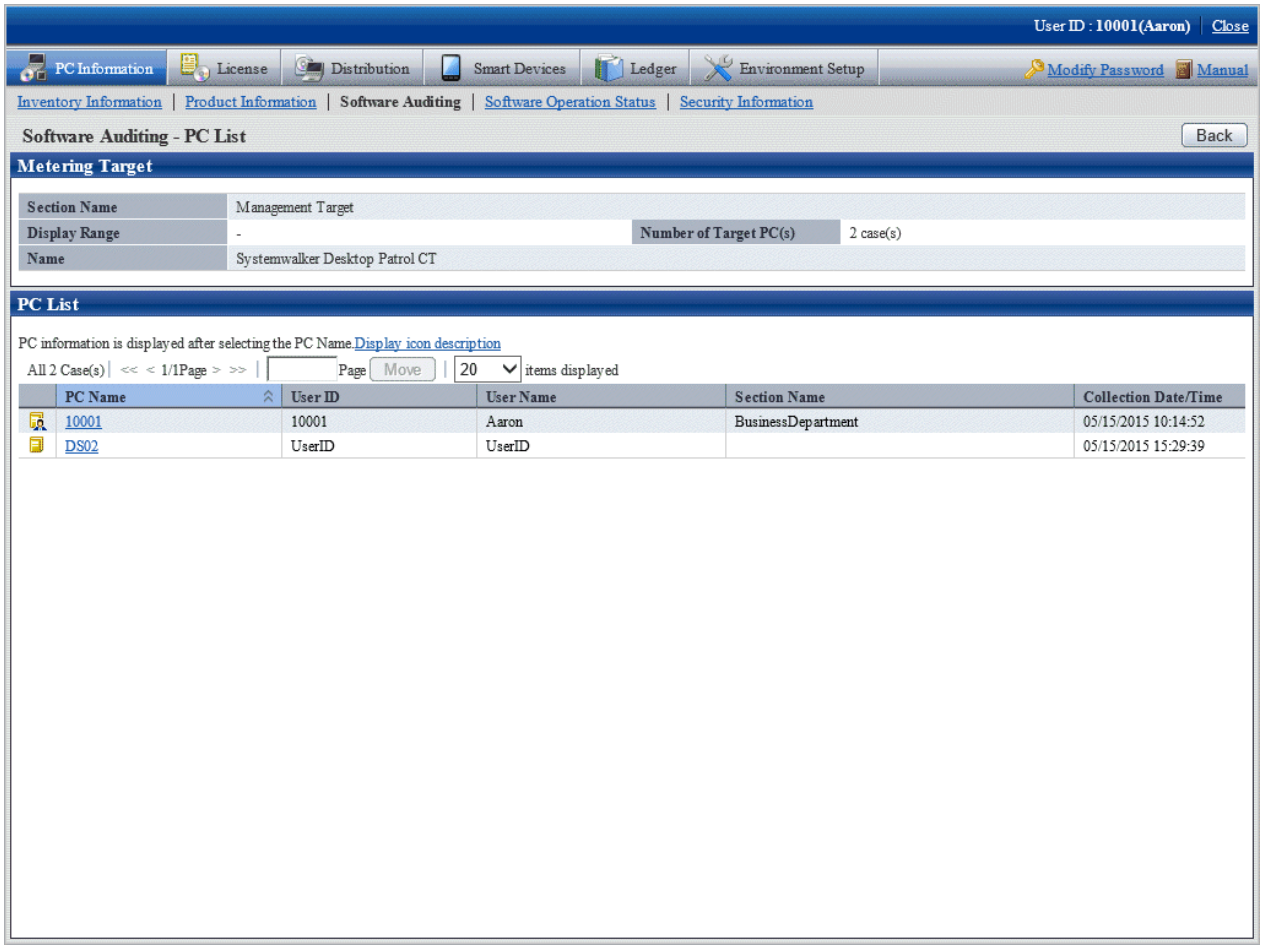
4. Select the software vender from the group displayed under **Software Installation Status** of the tree in the field on the left.

   The list of software provided by the selected software vender will be displayed in the field on the right.



5. Click the Corresponding Number.

   The PC list will be displayed.



6. Click the displayed PC name.

   Inventory information of the clicked PC will be displayed.

7. Select the displayed items.

   The selected window will be displayed. For displayed window, refer to "3.2.1 View Inventory Information".

How to output CSV file

The collected information can be output as CSV file.

To output to CSV file, click the **CSV Export** button to output according to the window.

3.2.4.1 Confirm Installation of Security Patches

Whether the security patch has been installed on CT can be confirmed.

In addition, when setting of alarm notification has been performed, the installation status of security patches can be confirmed by E-mail. For settings of alarm notification, refer to "2.5 Set Alarm Notification".

How to view

The installation status of security patch can be confirmed. In addition, the installation status can also be saved as files in CSV format.

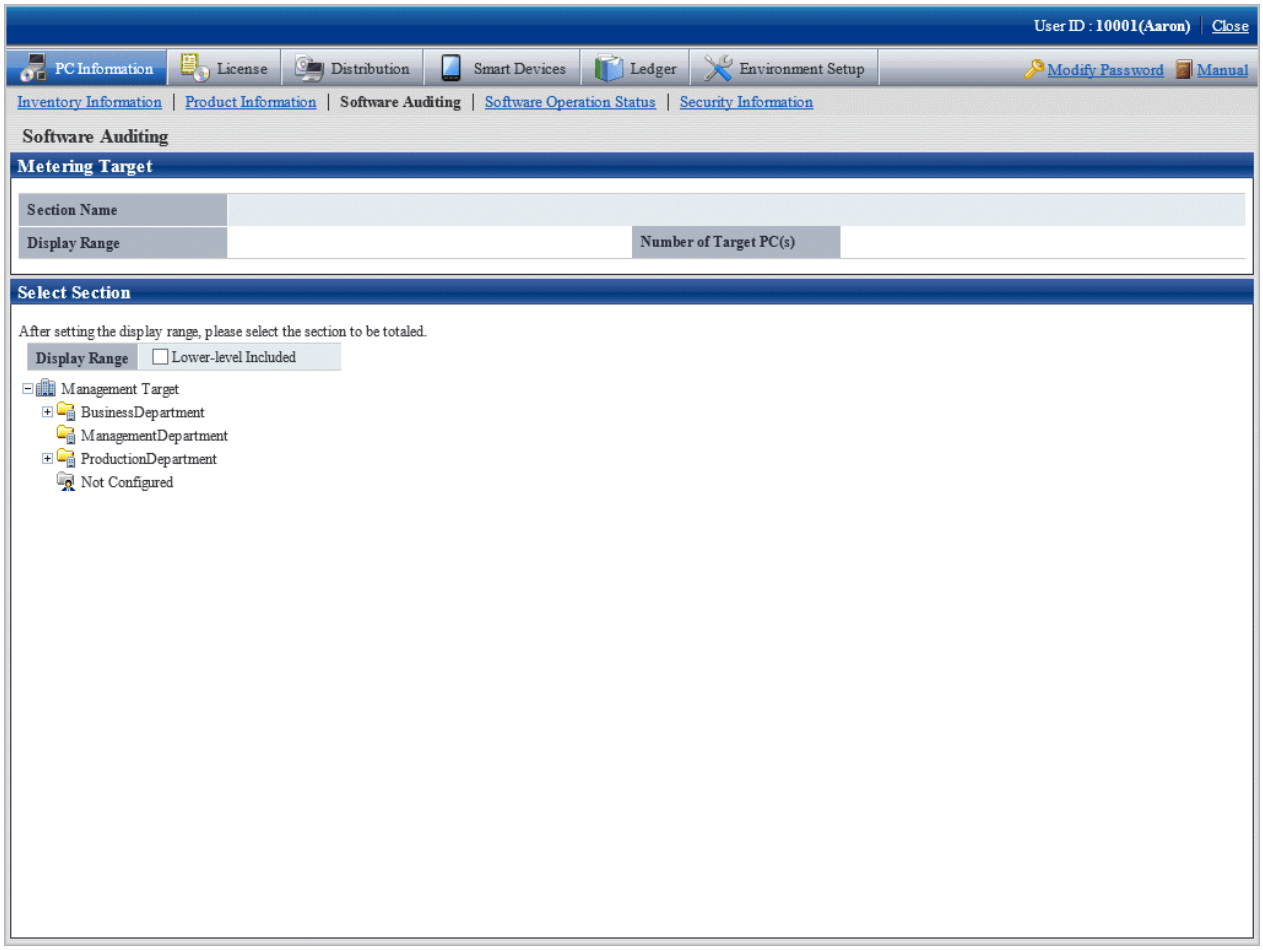
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

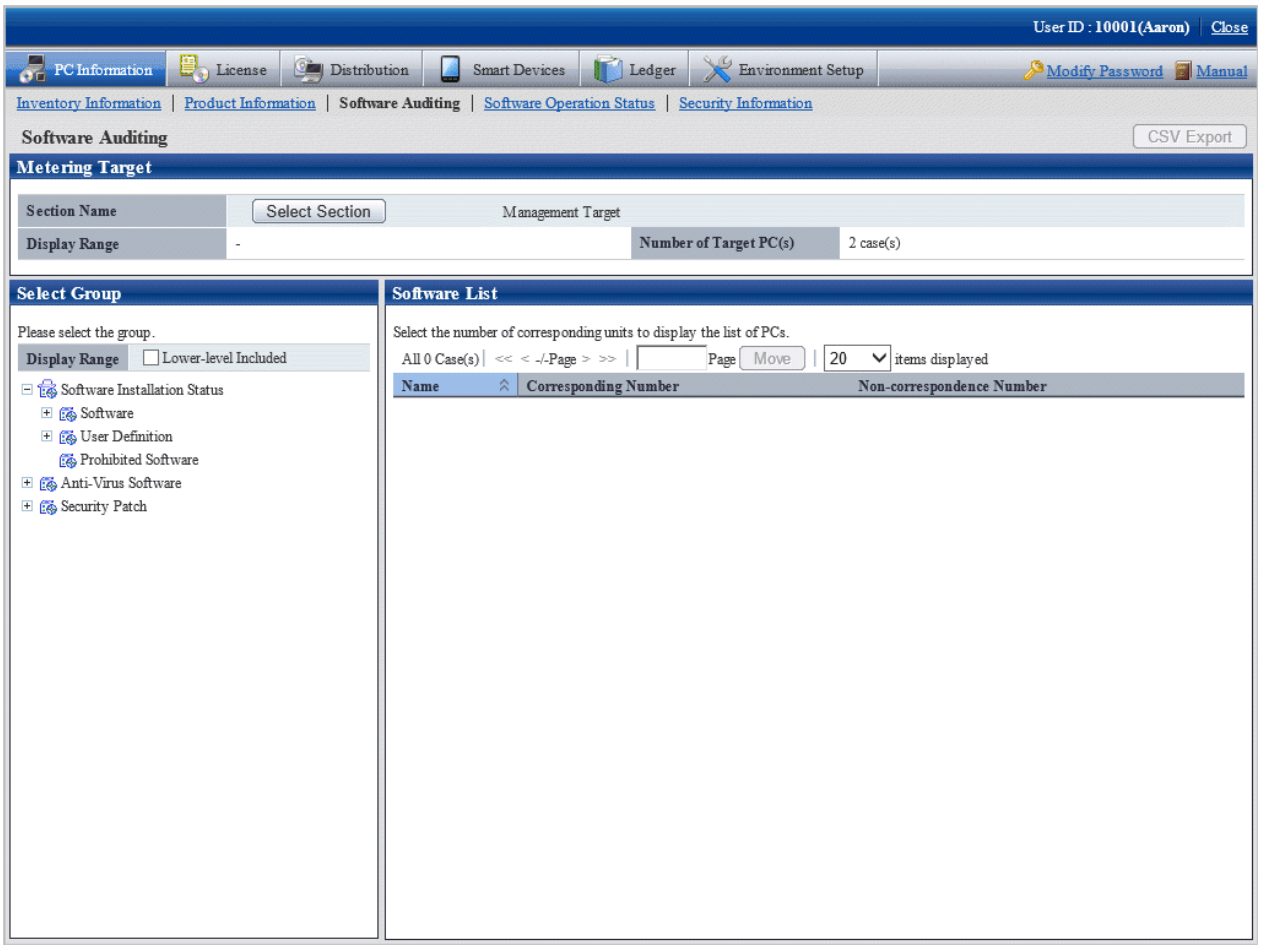
2. Click **Software Auditing**.

   The following window will be displayed.



3. Select the section to be displayed.

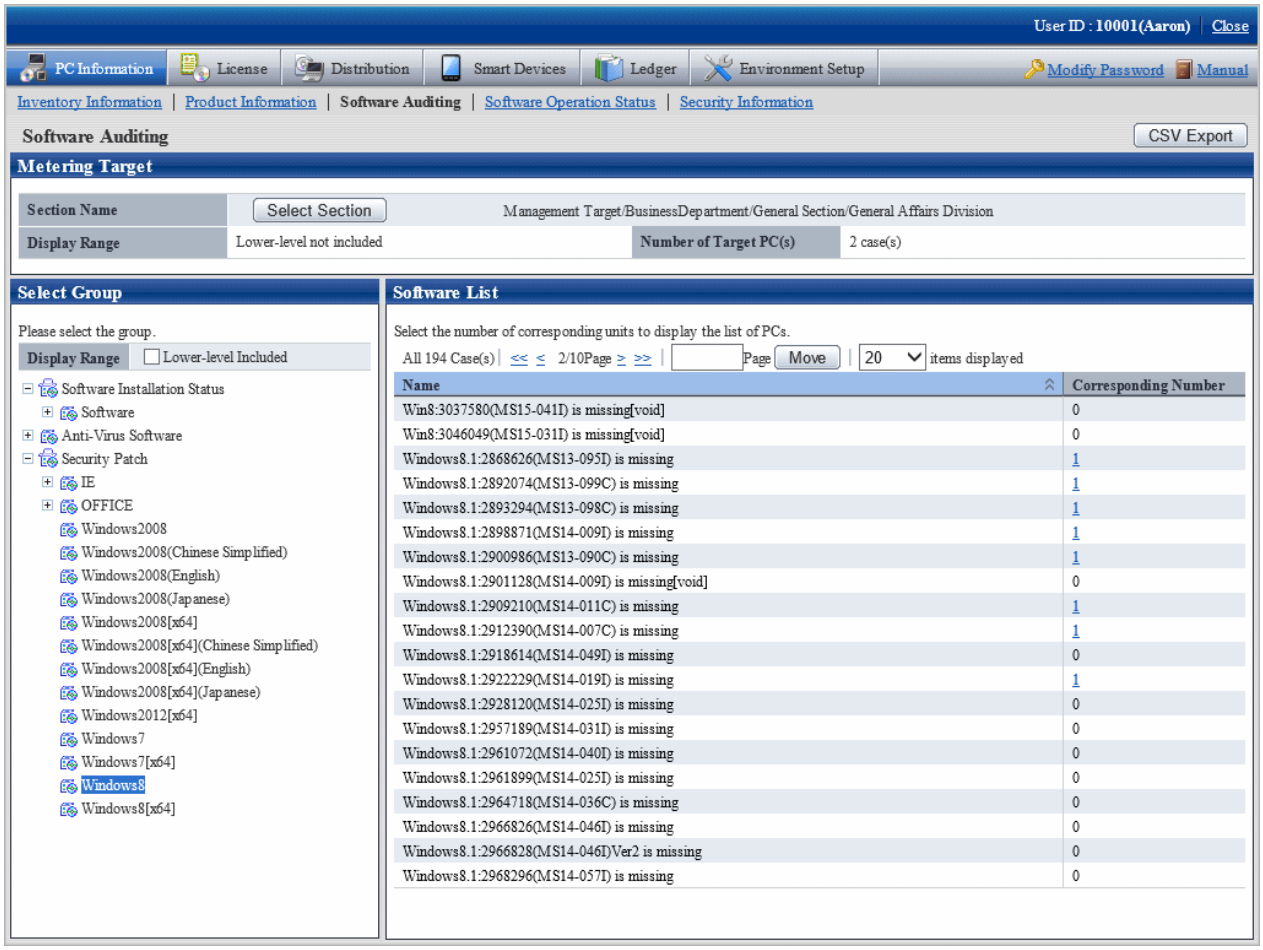
   The following window will be displayed.



4. Select a product from **Security Patch** of the tree in the field on the left.

   The information of the unapplied security patches corresponding to the selected product will be displayed in the field on the right.

5. Confirm the number of corresponding PCs displayed in the software list.



For information on how to view the installation status window of security patch, refer to "6.4.3 Confirmation of Installation of Security Patches".

6. To output the installation status of security patches to files in CSV format, click the **CSV Export** button.

3.2.4.2 Confirm Installation of Anti-Virus Software

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

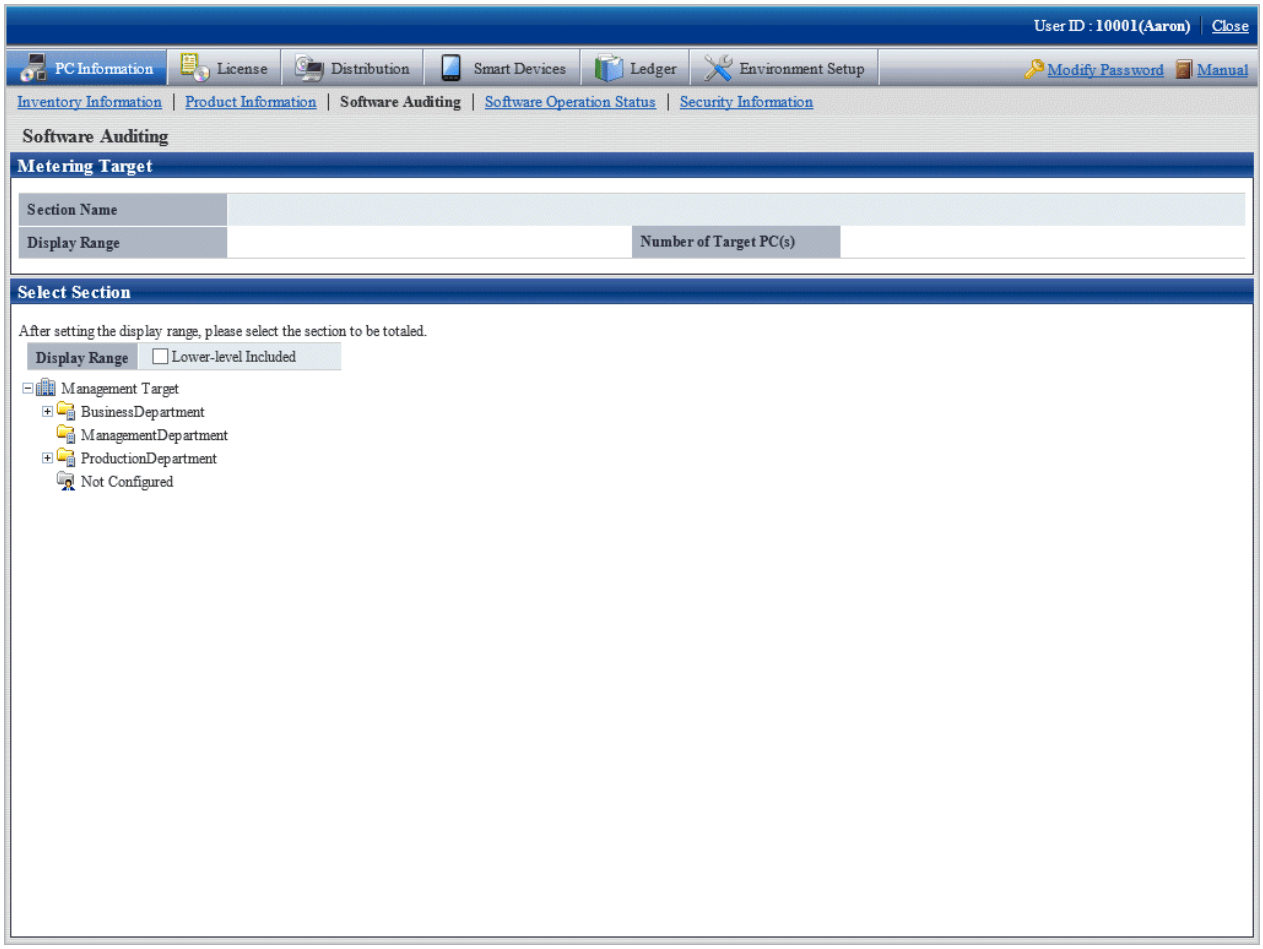
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

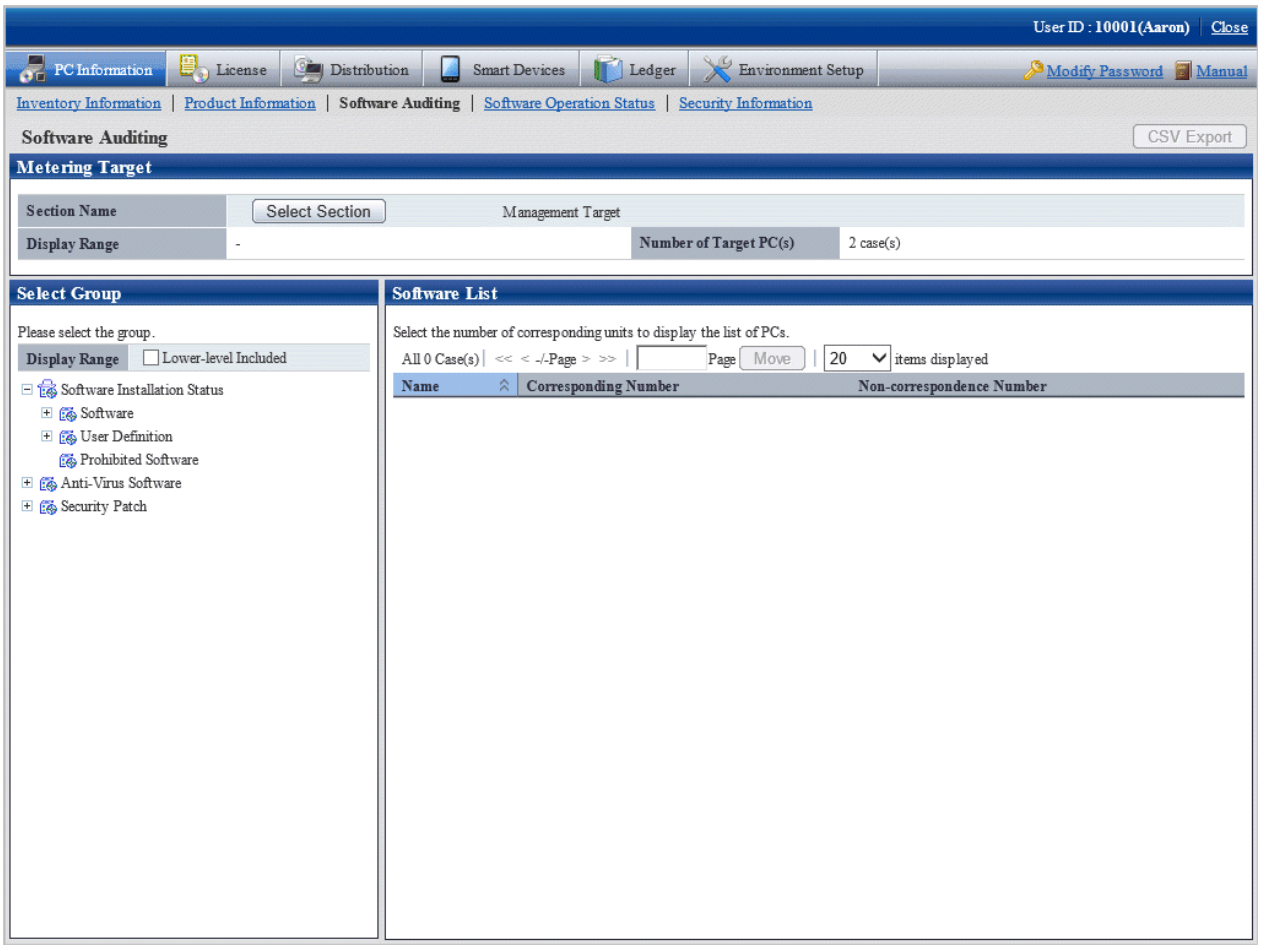
2. Click **Software Auditing**.

   The following window will be displayed.



3. Select the section to be displayed.

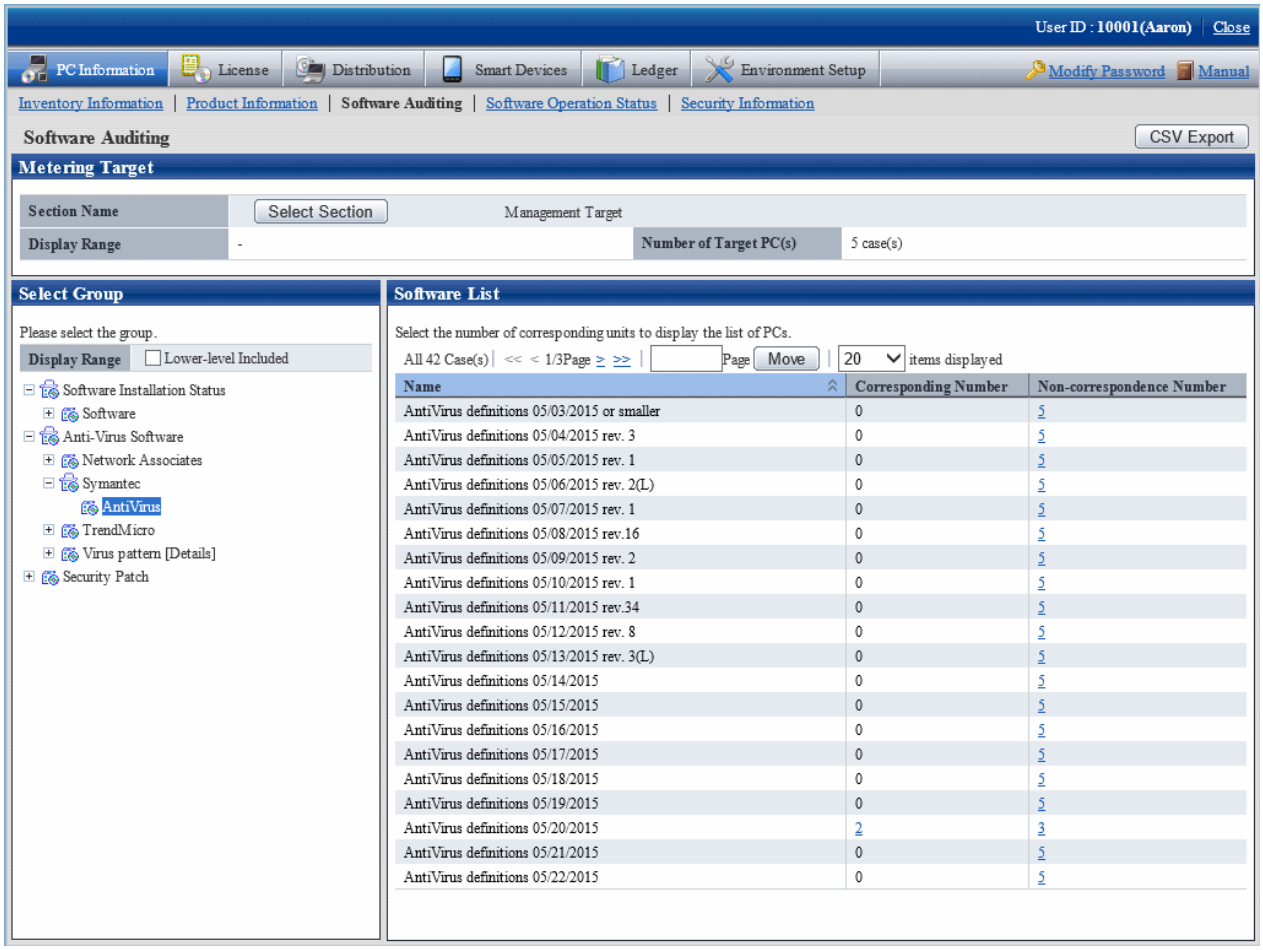
   The following window will be displayed.



4. Select a software vender from **Anti-Virus Software** of the tree in the field on the left.

   The anti-virus software provided by the selected software vender will be displayed in the field on the right.

5. Confirm the Corresponding/Non-correspondence Number of PCs displayed in the software list.



Pay attention to the number of PCs without anti-virus software being installed and the number of PCs without latest virus definition file.

6. To output the installation status of anti-virus software to files in CSV format, click the **CSV Export** button.

Processing when the anti-virus software is not installed

Ask the user of PC selected in the above **Confirm Installation of Anti-Virus Software** that has no anti-virus software installed to install anti-virus software.

Point

The anti-virus software to be distributed can be distributed by the software distribution function. During distribution, specify the downloaded executable file in advance and installation can also be started automatically in the download address. For details, refer to "Chapter 8 Distribute Software".

3.2.5 View Software Operation Status

Software operation status on CT can be confirmed according to the collected inventory information. In addition, software operation status can be saved as files in CSV format.

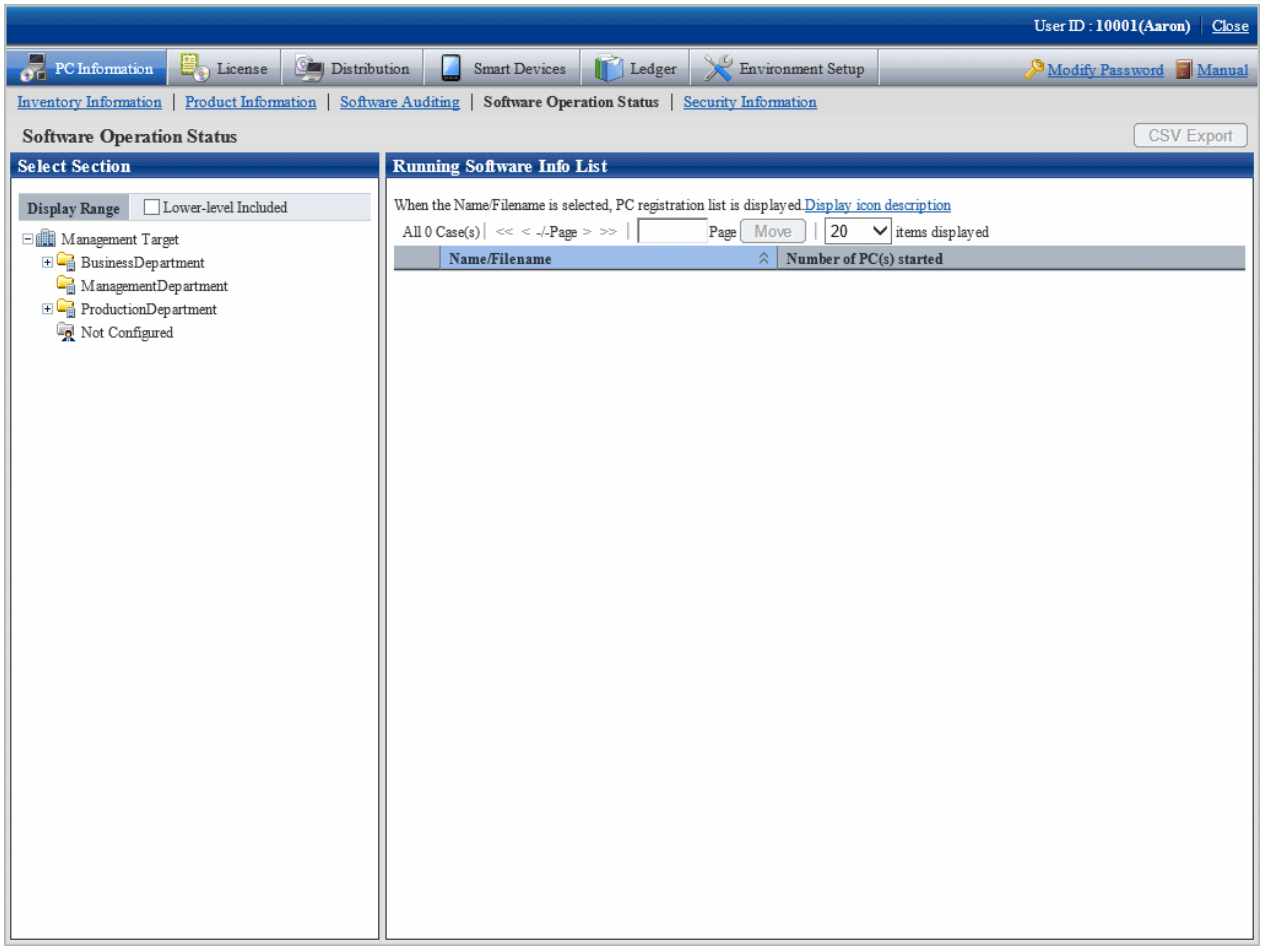
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

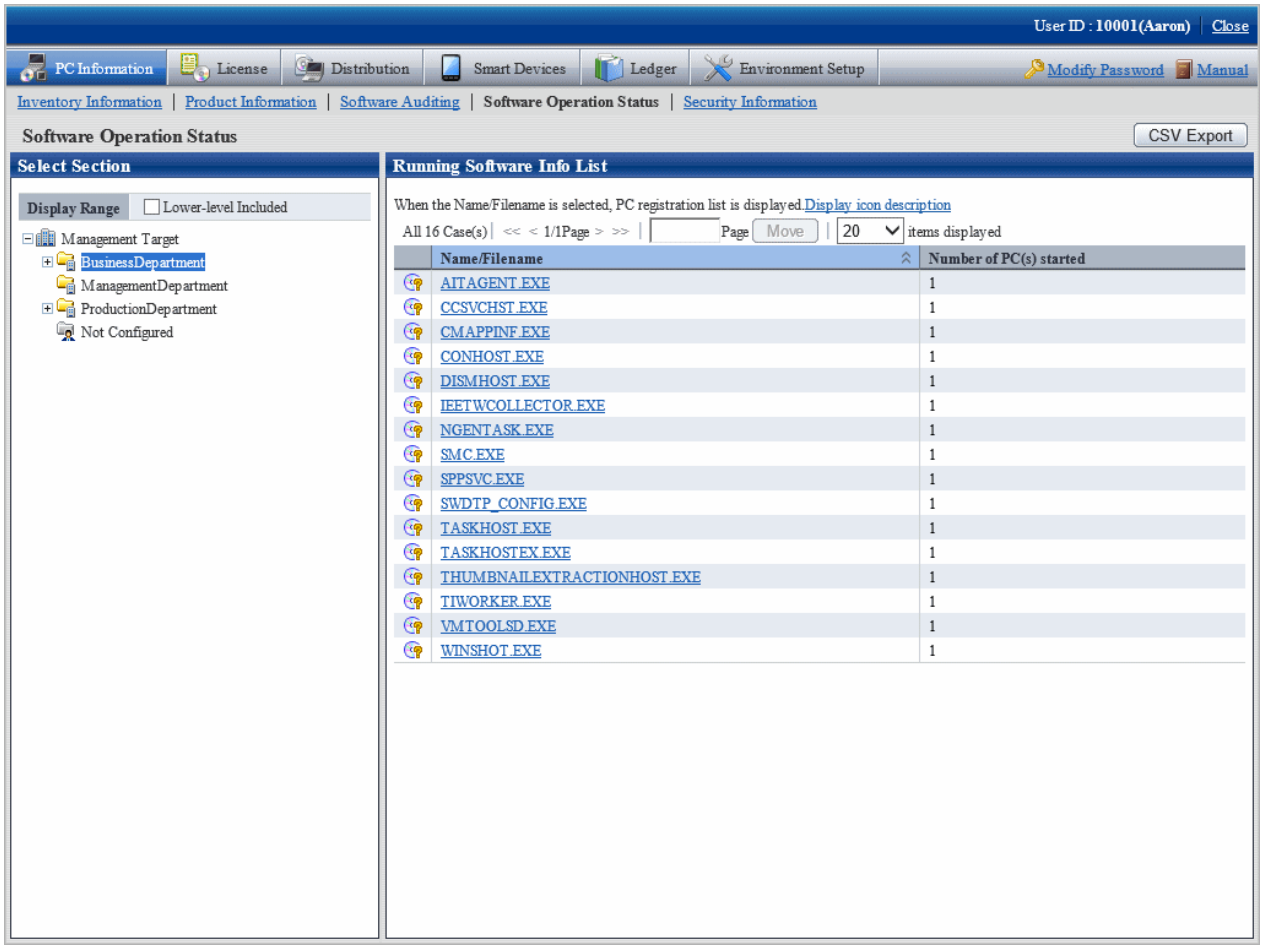
2. Click **Software Operation Status**.

   The following window will be displayed.



3. Select a section from the section tree in the field on the left.

   The software operation information of the selected section will be displayed in the field on the right.



Item	Description
Number of PC(s) started	Number of PC that has started the software

4. To output the software operation information displayed in the field on the right to files in CSV format, perform the following operations. When not to output, proceed to the next step.

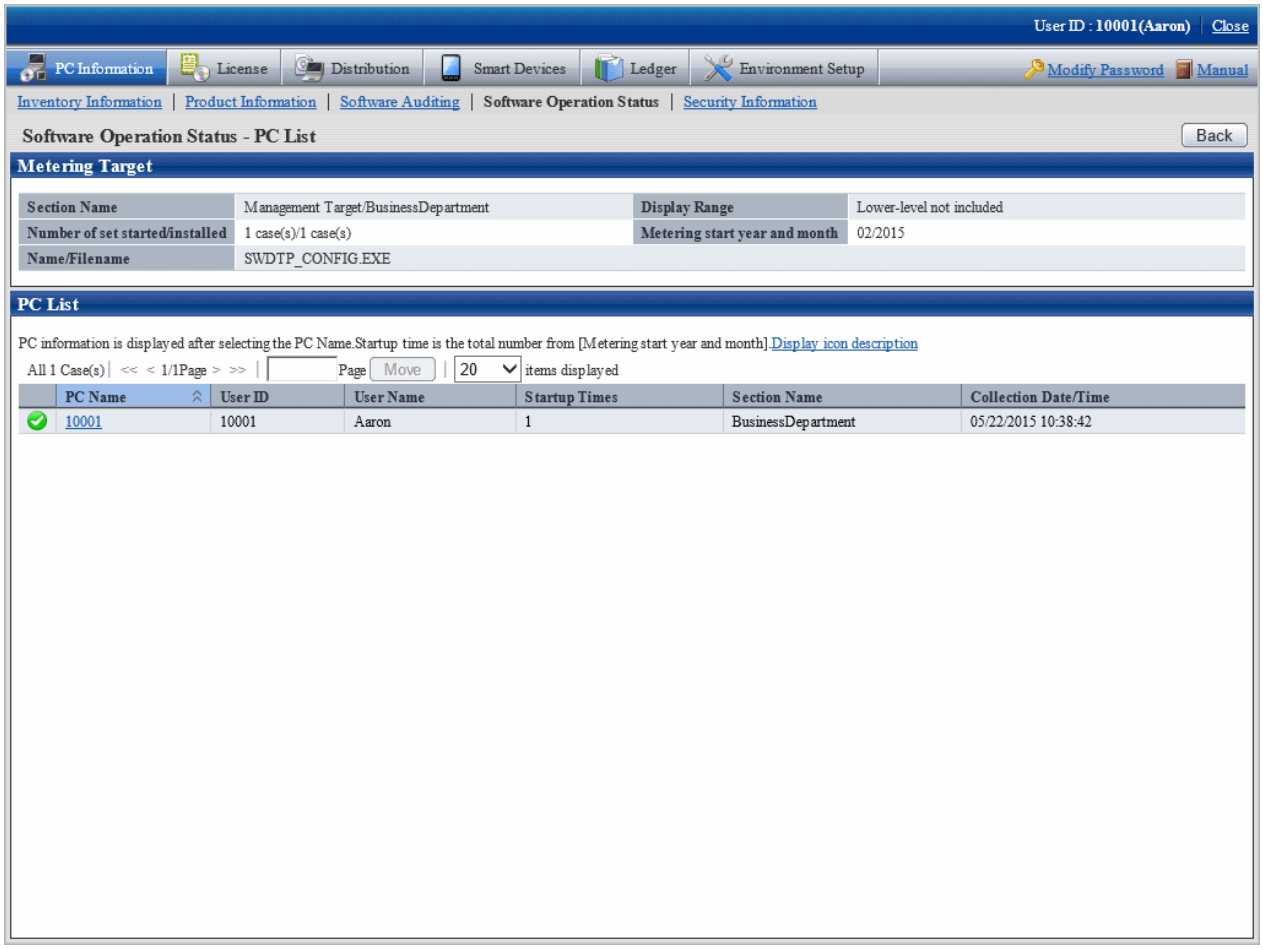
   a. Click the **CSV Export** button.

      The download window will be displayed.

   b. Output the operation status of software to files in CSV format according to the window.

5. To confirm the details such as the user of software, click the software name in the field on the right.

   The following window will be displayed.



3.2.6 View Security Information

The security information of CT that can be collected as inventory information can be confirmed.

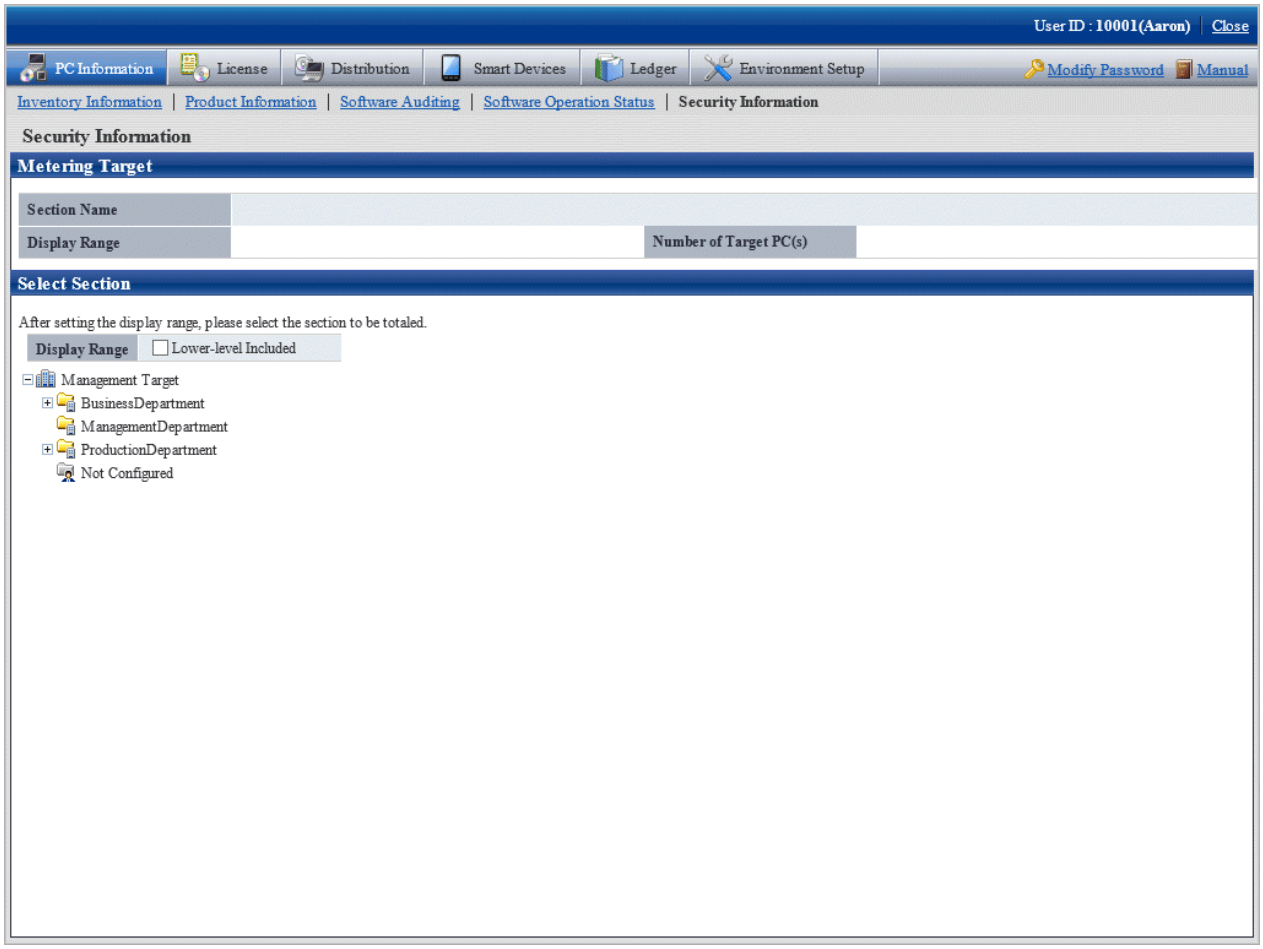
The procedure is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

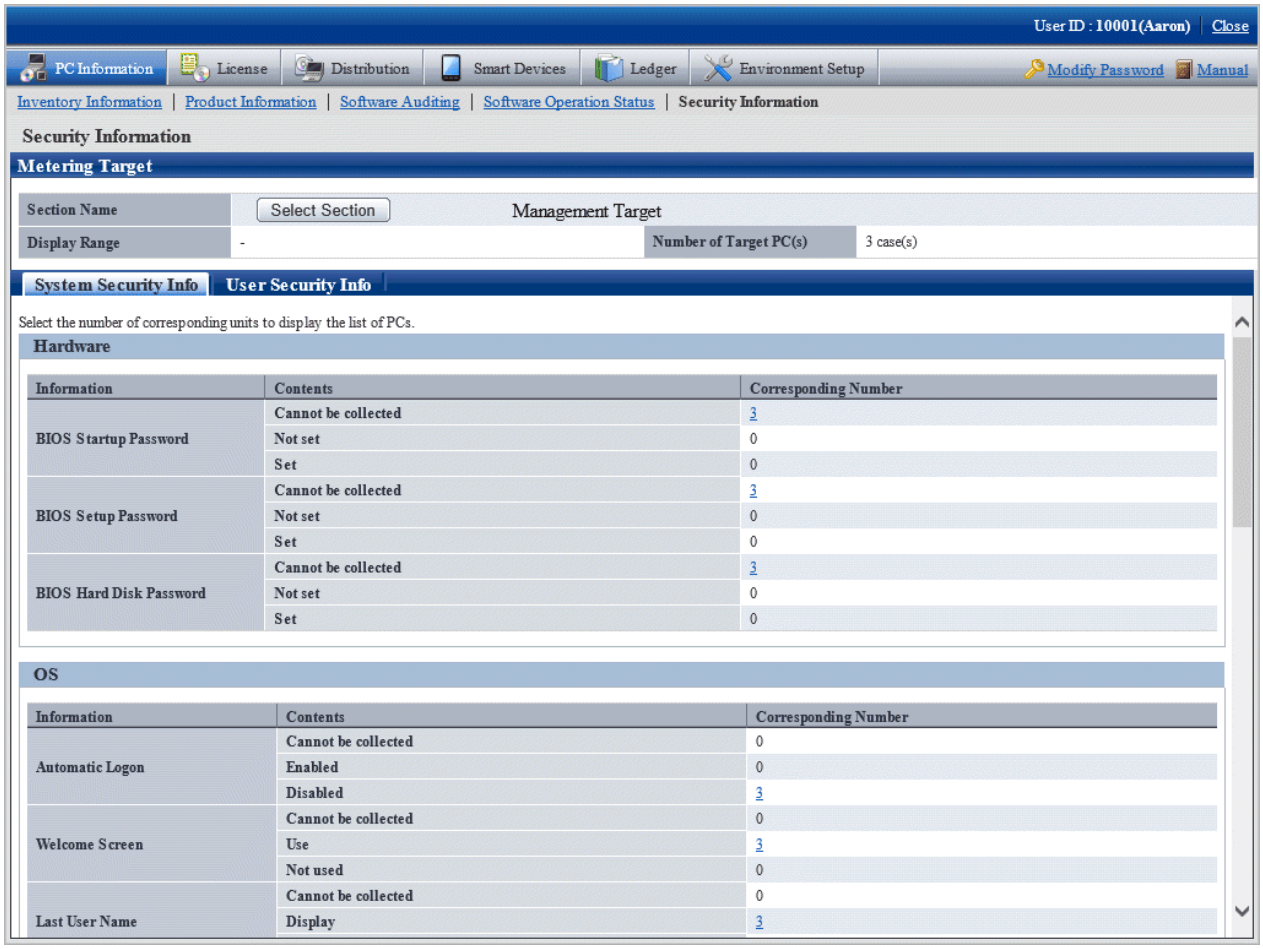
2. Click the **Security Information**

   The following window will be displayed.



3. Select the section to be displayed.

   The following window will be displayed.



4. Confirm the following security information.

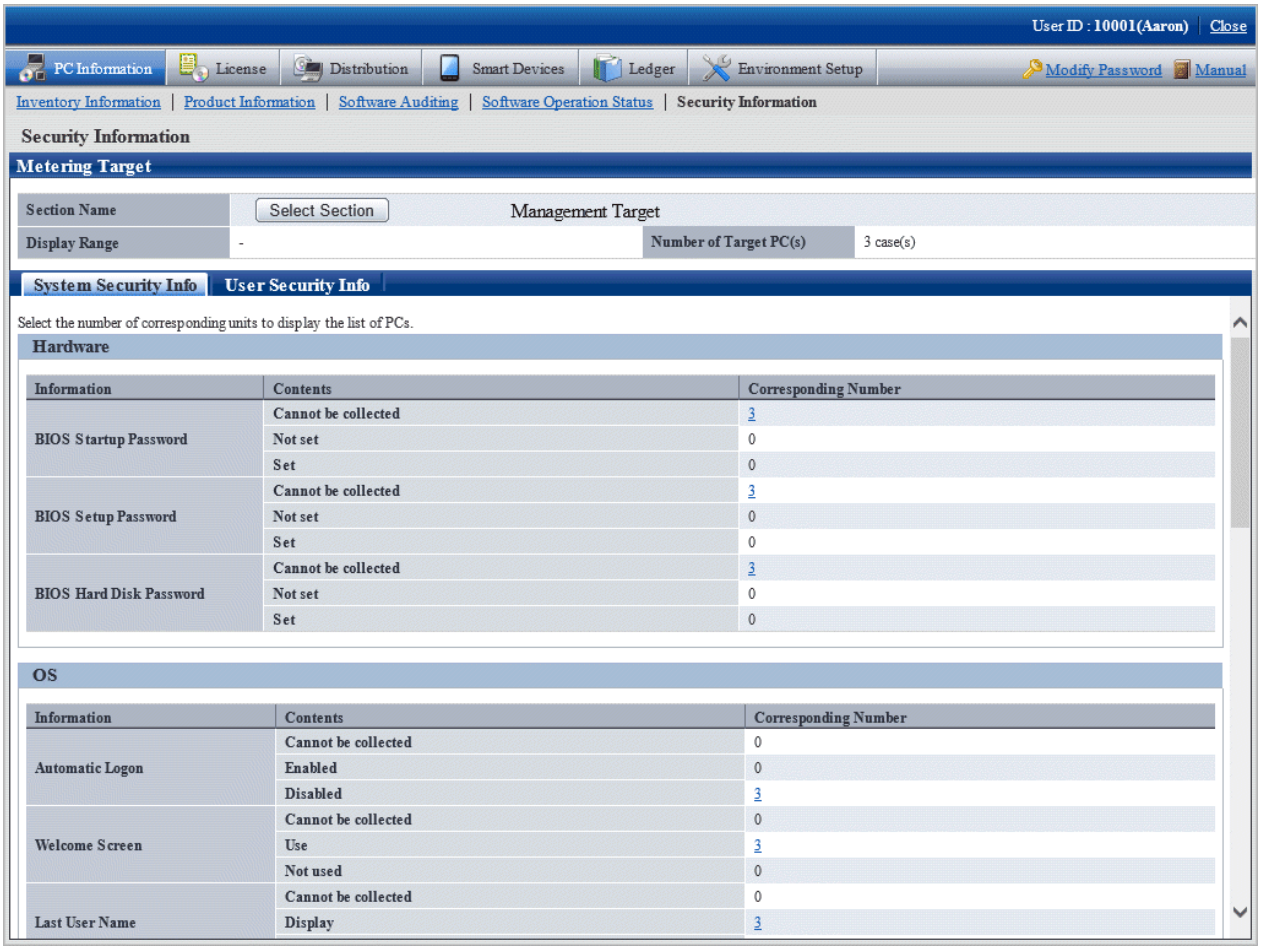
   - System Security Info
   - User Security Info
   - Desktop Keeper Info

   The selected window will be displayed. For display window, refer to the following description.

   In addition, Desktop Keeper information will be displayed when the relevant product has been installed on CT.

When system security info is selected

The following window will be displayed. The number of PCs corresponding to the system security information can be confirmed.



The following items can be confirmed.

Category	Information	Description
Hardware	**BIOS Startup Password**	Settings of startup password (password used by user)
	BIOS Setup Password	Settings of the setting password (password used by administrator)
	BIOS Hard Disk Password	Settings of hard disk password
OS	**Automatic Logon**	Settings of automatic logon
	Welcome Screen	Settings of displaying the welcome window
	Last User Name	Settings of displaying the user name that logged on at last
	Security of Guest Account	Existence of password settings of Guest account and the inappropriate password
	Settings of Automatic Update	Enable or disable the automatic update of WindowsUpdate
	User Account Control (UAC)	Enable or disable the User Account Control (UAC) of Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012
	Insecure Shared Folder	Existence of shared folder that can be accessed by everyone authority

Category	Information	Description
	Require a Password on Wakeup	Set the password when restoring from standby
	Set Complicated Password Required	Existence of complex password setting
Application	**Firewall**	Settings of firewall
	Real-time Scan Status of Anti-virus Software	Settings of real-time search of anti-virus software
	Scheduled scan status of Anti-virus software	Status of scheduled scan of anti-virus software
	Scan Scope of Anti-virus Software	Target scanning range of anti-virus software

The meaning of content of items is as follows.

Cannot be collected**:**

The version level of Systemwalker Desktop Patrol CT indicates the number of PCs of the version prior to V13.0.0 or the number of PCs that does not support collection of information on BIOS.

In addition, for settings items added in each version level, the Systemwalker Desktop Patrol CT lower than each version level will be displayed as **Unable to Collect**.

Not set**:**

Indicates the number of PCs in which the security items are not set.

Set**:**

Indicates the number of PCs in which the security items have been set.

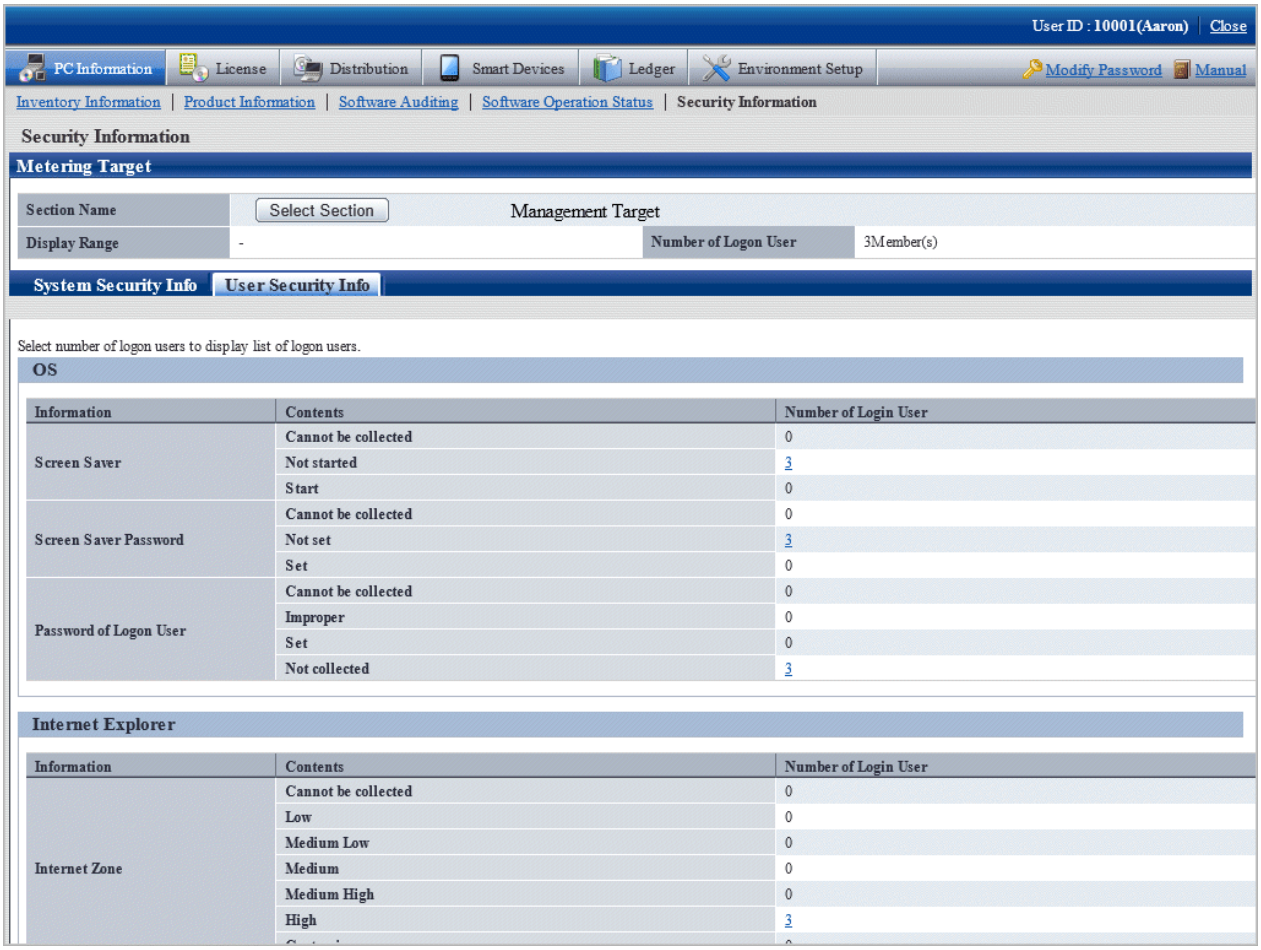
The following describes the point of auditing of system security information.

- Hardware
  - When various passwords of BIOS are not set, it will be audited as in low security.
  - Based on the PC manufacturer/model, part of PC does not enable password settings or the set value of password cannot be adopted.
- Display of **Automatic Logon** and **Last User Name** of OS
  - When displaying the logon name in the logon window, it will be audited as in low security.
  - When setting to automatic logon, it will be audited as in lower security.
- **Welcome** of OS
  - This is an auditing item for Windows(R) XP. The other OS will be included in **Unable to Collect**.
  - **Use** will always be set for operating systems other than Windows(R) XP.
- **Security of Guest Account** of OS
  - When the Guest account is enabled, password is not set or an inappropriate password has been set (the password that is same as the user name), it will be audited as in low security.
    In addition, it is allowed to not audit password, but to audit whether the Guest account is enabled.
    To modify the auditing method, use the CustomPolicy.exe (Modify Policy for Customized Settings) command. For information on how to use the CusttomPolicy.exe command, refer to *Systemwalker Desktop Patrol Reference Manual*.
- **Setting of Automatic Update** of OS
  - When it is not set, it will be audited as in low security.

- **User Account Control (UAC)** on the operating systems
  - If the UAC feature is disabled, or it is set to be promoted without displaying prompts (not notifying), it will be audited as decrease in security strength.
  - In the OS without UAC function, it will certainly be set as **Unable to Collect**.
- **Unsafe Shared Folder** of OS
  - When the folder that can be accessed by the everyone authority, it will be audited as in low security.
- **Setting that Requires Complicated Password** of OS
  - If no complex password is set in the Windows group policy, it will be audited as in low security.
- **Firewall** and **Real-time Search of Anti-virus Software** of application
  - When it is not set, it will be audited as in low security.

When User Security Info **is selected**

The **User Security Info** window will be displayed. The number of users registered to the PC corresponding to the user security information can be confirmed.



The following items can be confirmed.

Category	Information	Description
OS	**Screen Saver**	Start screensaver or not
	Screen Saver Password	Whether password is required when restoring from screensaver

Category	Information	Description
	Password of Logon User	Whether the password of logon user has been set, and inappropriate password
Internet Explorer	**Internet Zone**	Settings of IE security zone - Low - Medium-Low - Medium - Medium-High - High - Customized
Application	**Google Desktop "Search Across Computers"**	Enable/Disable the **Data Search on Multiple Computers** function

The meaning of the content of items is as follows.

Cannot be collected:

Indicates there is no number of logon users of the PC corresponding to the content.

Not set:

Indicates the number of logon user of PC in which the security items are not set.

Set:

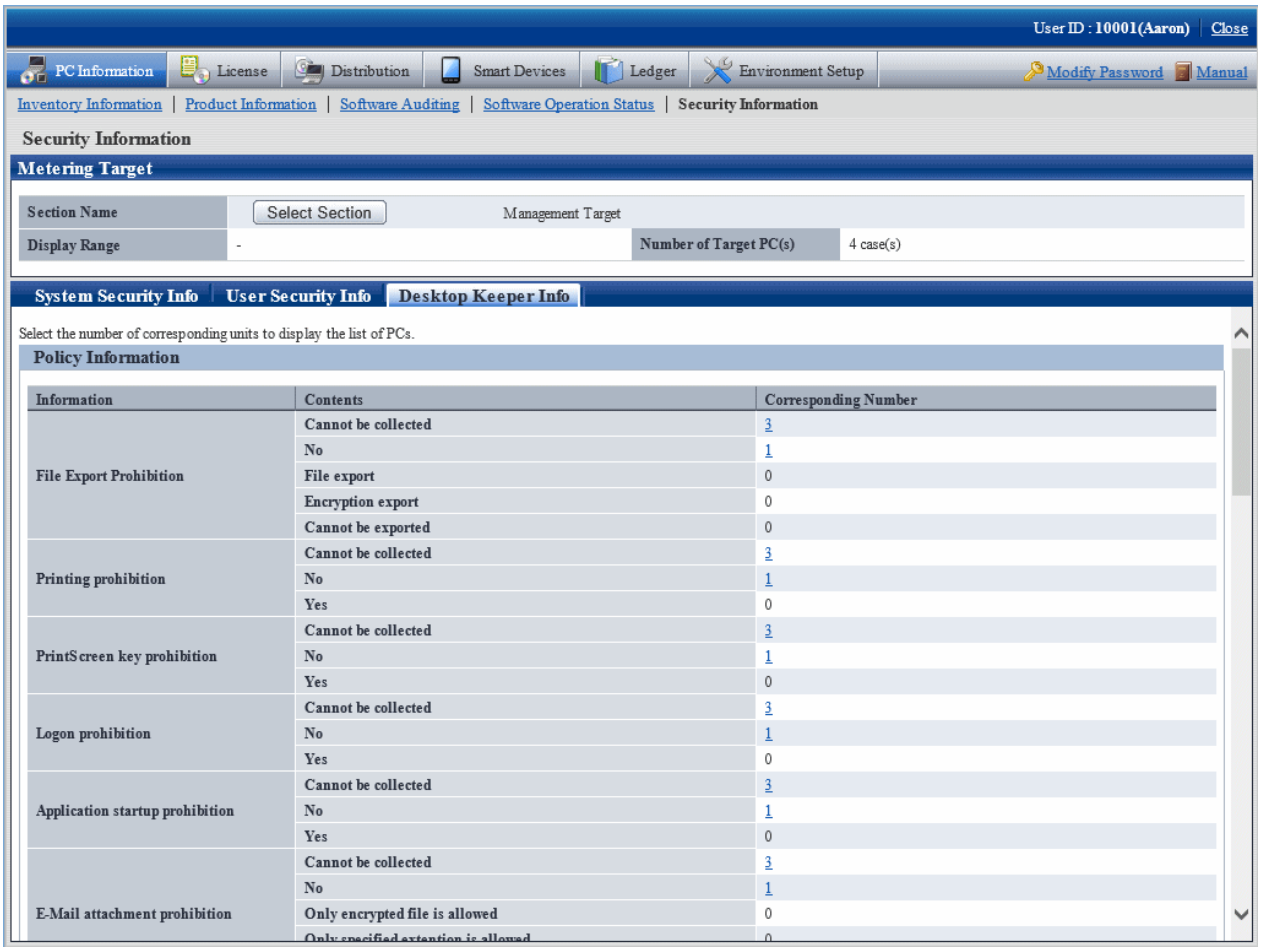
Indicates the number of logon user of PC in which the security items have been set.

The following describes the point of auditing of user security information.

- **Screensaver** and **Screensaver Password** of OS
  - When not to start screensaver or no password for restoring from screensaver, it will be audited as in low security.
- **Password of Logon User** of OS
  - When password is not set or an inappropriate password has been set (the password that is same as the user name), it will be audited as in low security.
- **Internet Zone** of Internet Explorer
  - When the level of Internet zone is low, it will be audited as in low security.
- **Google Desktop "Data Search on Multiple Computers" function** of application
  - When the **Data Search on Multiple Computers** function of Google Desktop is enabled, the index information of PC will be forwarded to the Google Desktop Server, so audit according to the security policy.

When Desktop Keeper Info is selected

The **Desktop Keeper Info** window will be displayed. When Systemwalker Desktop Keeper is installed on client, the number of PC that corresponds to the security setting information of Systemwalker Desktop Keeper can be confirmed.



The meaning of the content of items is as follows.

Cannot be collected:

Indicates the number of PCs without Systemwalker Desktop Keeper installed or the version level is the version prior to V13.0.0.

No:

Indicates the number of PCs in which the security items of Systemwalker Desktop Keeper are not set.

Yes:

Indicates the number of PCs in which the security items of Systemwalker Desktop Keeper have been set.

For each item, refer to the manual of "Systemwalker Desktop Keeper".

In addition, for the setting items added in each version of Systemwalker Desktop Keeper, since it is unable to collect from the Systemwalker Desktop Keeper of a version older than each version level, **Unable to Collect** will be displayed.

3.2.7 Perform Operation Management of PC

Perform the following operations from remote for the PC to perform operation management.

- Immediate collection of inventory information (hardware information)
- Power operation

In addition, when the PC to perform operation management is not registered, it will not be displayed in the **PC Operation Management** window.

For information on how to register the PC to perform operation management, refer to "3.1.4 Perform Settings of PC Operation Management".

3.2.7.1 Collect Inventory Information (Hardware Information) Immediately

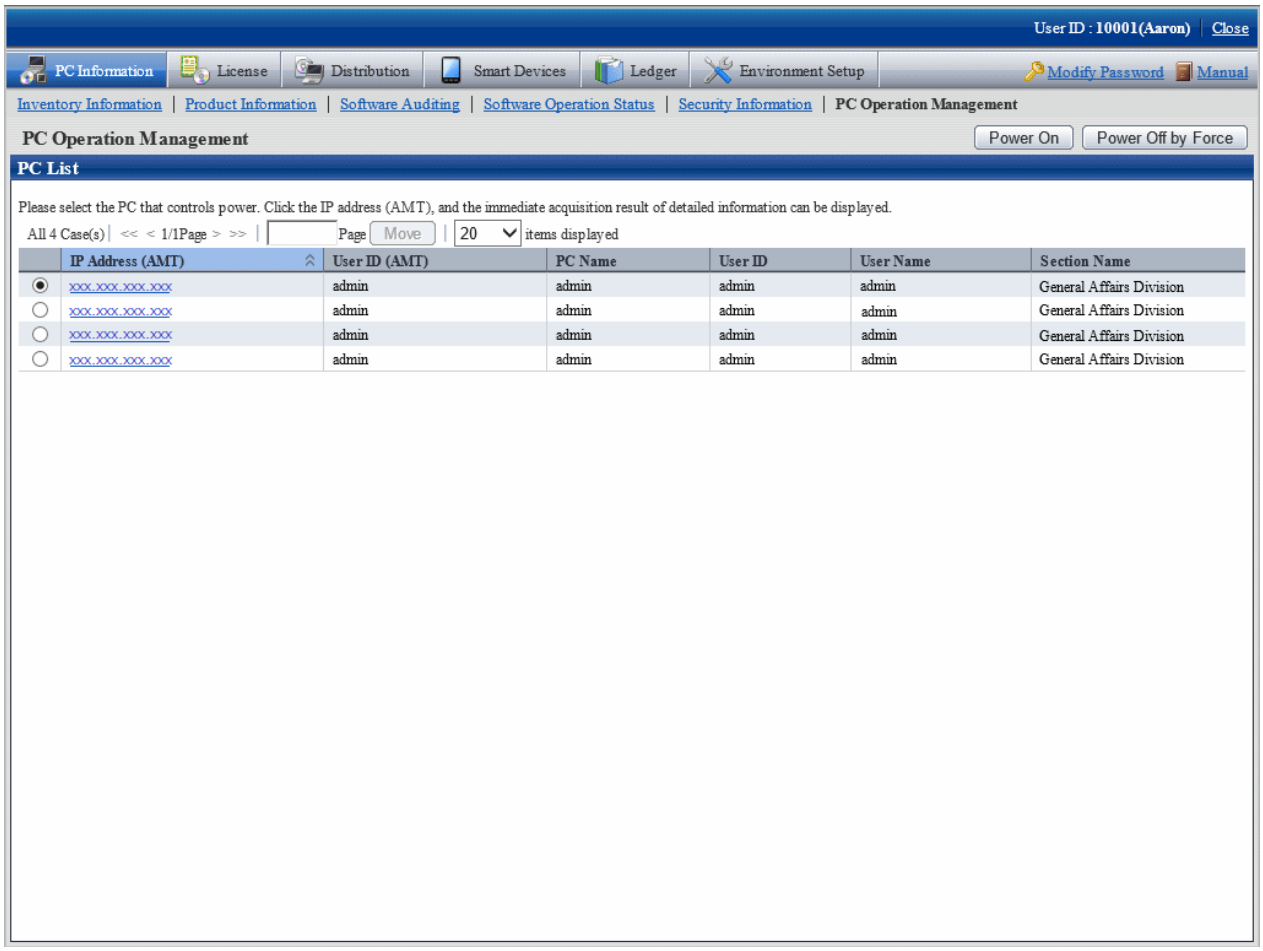
The procedure of immediately collecting and viewing inventory information (hardware information) of PC to perform operation management is as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

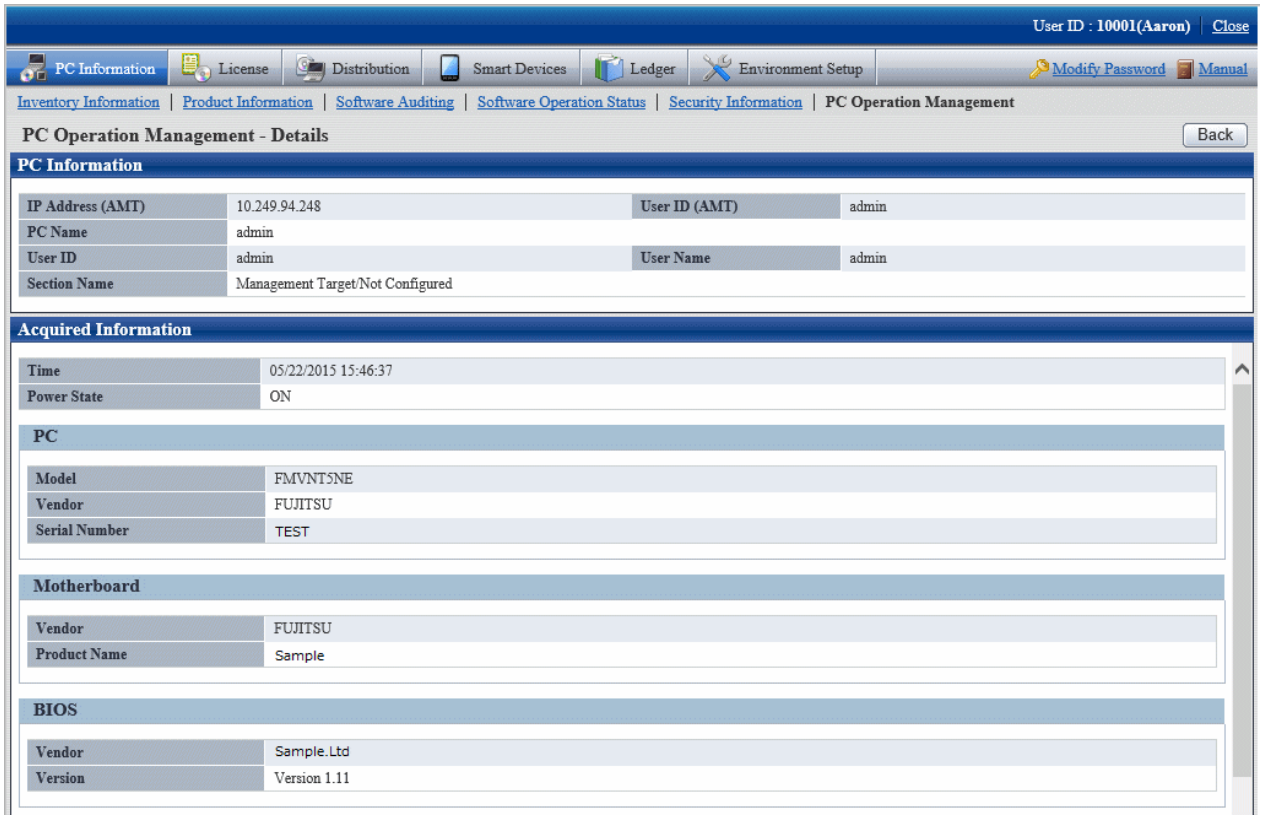
2. Click **PC Operation Management**.

   The following window will be displayed.



3. Click the **IP Address (AMT)** of the PC whose inventory information is expected to be viewed.

   The inventory information of the selected PC will be collected immediately and displayed in the **PC Information** column.



4. View the collected inventory information.

   The collected inventory information is as follows.

Category	Information	Description
-	**Time**	Acquisition time (CS)
	Power State	Power status
PC	**Model**	PC model
	Vender	Manufacturer name
	Serial Number	Serial number
Motherboard	**Vender**	Motherboard vender
	Product Name	Product name
BIOS	**Vender**	BIOS vender
	Version	BIOS version
Processors	**Vender**	CPU vender
	Maximum Speed	Clock number
	Version	CPU version
Memory	**Vender**	Memory vender
	Form Factor	Form Factor
	Serial Number	Serial number
	Size	Size

The following causes should be considered when failed in processing (when error message is displayed). Confirm.

- The IP address (AMT) is incorrect.
- User ID (AMT) or password (AMT) is incorrect.
- The electric socket of the PC to perform operation management has dropped.
- The LAN cable used by AMT of PC to perform operation management has dropped.
- The PC to perform operation management is connecting to wireless LAN and the PC is not connected to power.

3.2.7.2 Operate Power

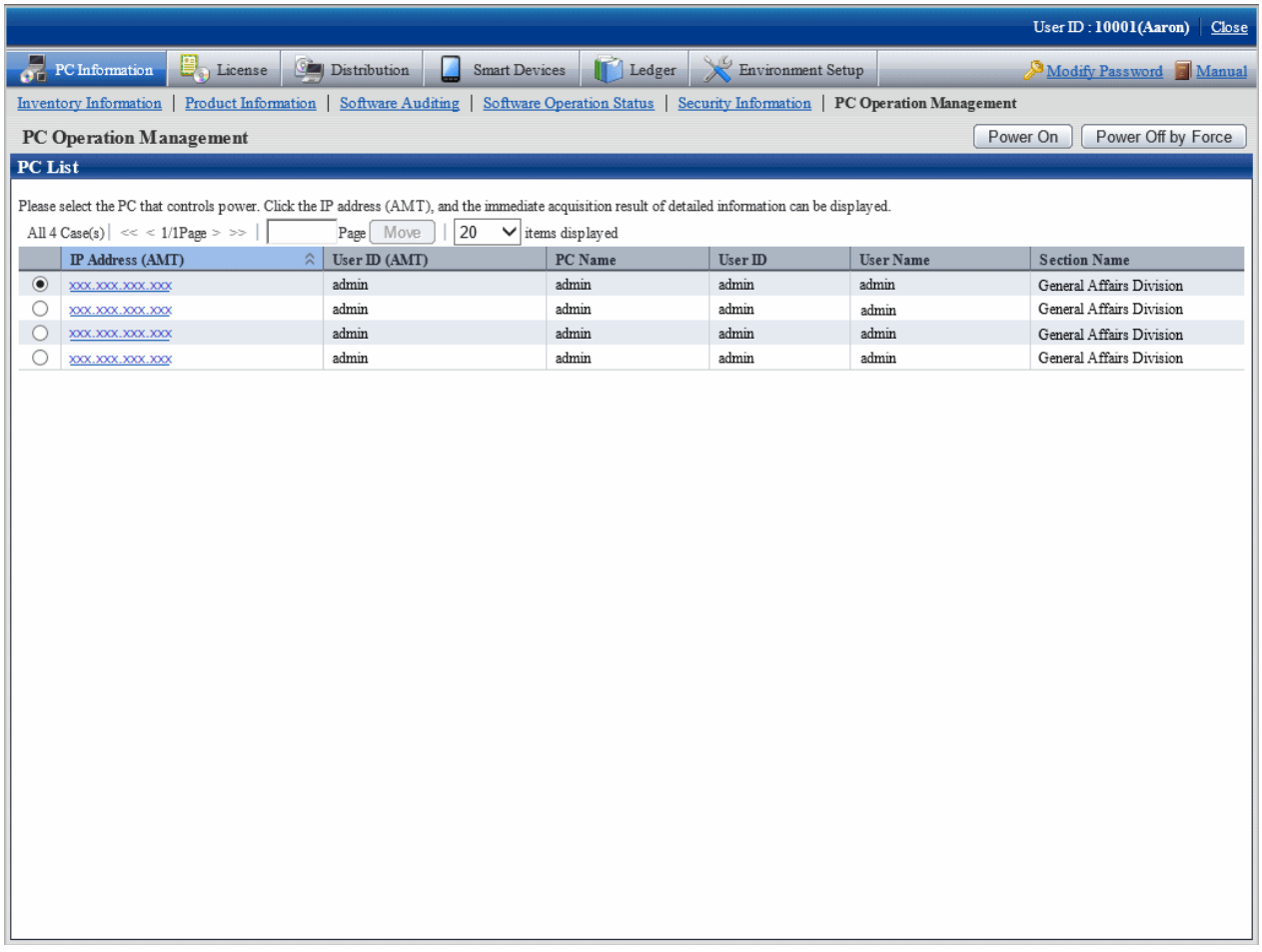
The procedure to operate the power of PC to perform operation management is shown as follows.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

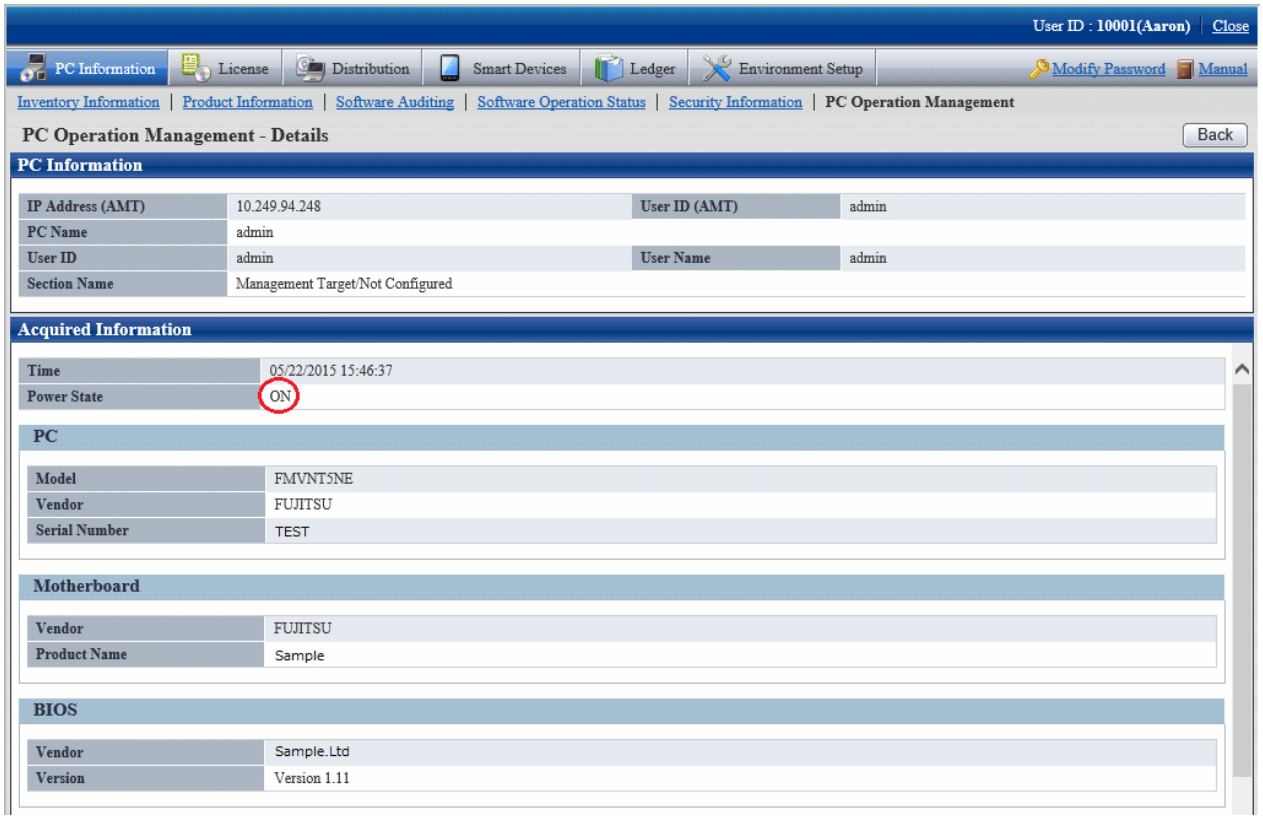
2. Click **PC Operation Management**.

   The following window will be displayed.



3. Click the **IP Address (AMT)** of the PC that requires power operation.

   View **Power State** in Inventory Information and confirm the status of power of PC.

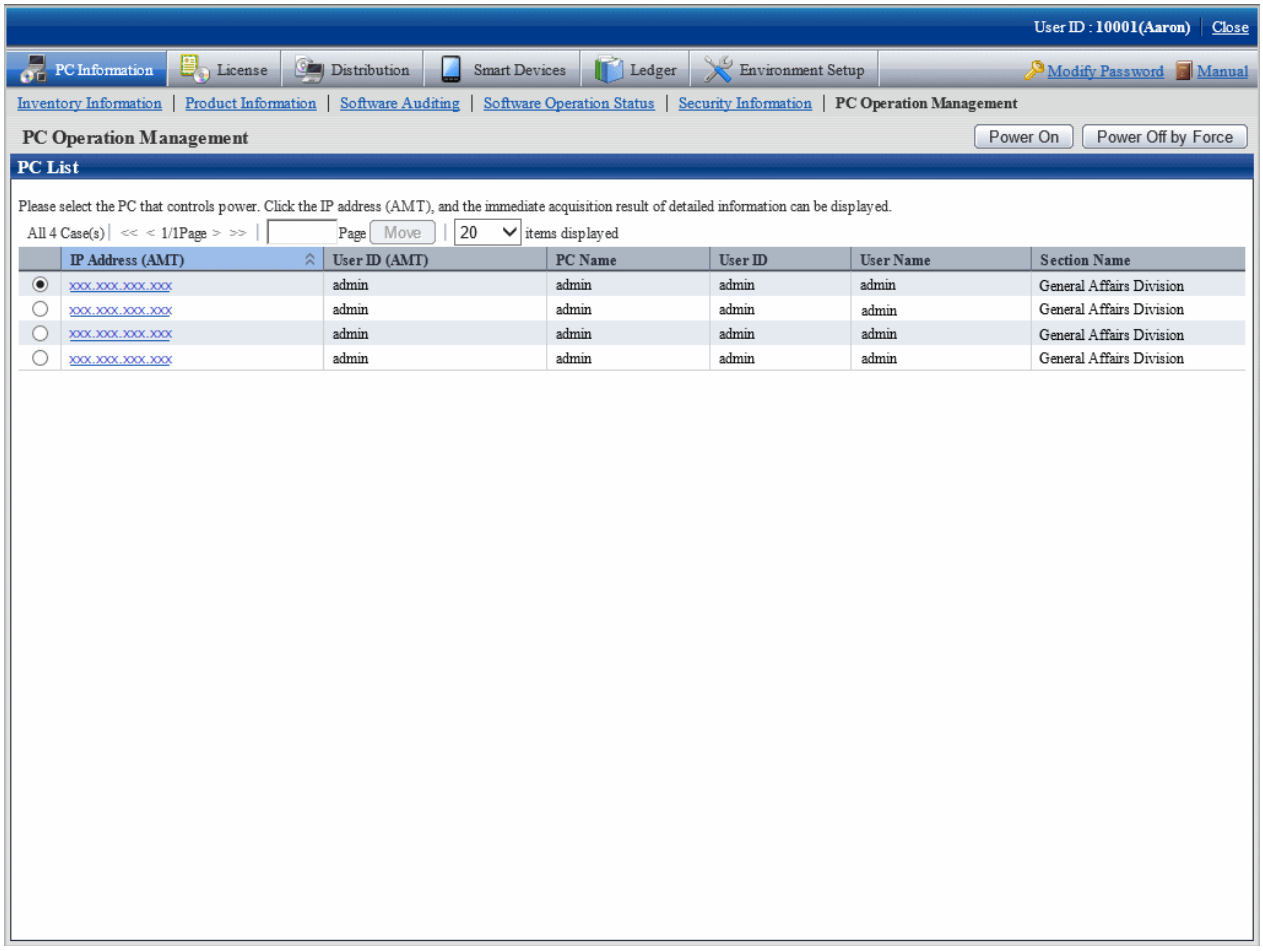


   The following causes should be considered when failed in processing (when error message is displayed). Confirm.

   - The IP address (AMT) is incorrect.
   - User ID (AMT) or password (AMT) is incorrect.
   - The electric socket of the PC to perform operation management has dropped.
   - The LAN cable used by AMT of PC to perform operation management has dropped.
   - The PC to perform operation management is connecting to wireless LAN and the PC is not connected to power.

4. After confirming the power status, click the **Back** button.

   Go back to the **PC Operation Management** window.



5. Select the radio button of the PC to perform power operation and click the following button.

   - **Power ON** button: Turn on the power of the selected PC.
   - **Power OFF by Force** button: Turn off the power of selected PC by force. The shutdown processing of OS will not be performed.

     When the **Power OFF by Force** button is clicked, the following message will be output in the dialog.

     > Power will be OFF by force. Do you want to continue?
     > (The shutdown processing of OS will not be performed.)

Note

- When performing power OFF by force, if the OS is running, since the data that is being operated cannot be saved, pay attention to the operation.
- When performing power ON by force, if BIOS password has been set in the PC to perform operation management, it will be unable to enter the password from Web browser. It is required to enter in the PC to perform operation management.

The following causes should be considered when failed in processing (when error message is displayed). Confirm.

- The IP address (AMT) is incorrect.
- User ID (AMT) or password (AMT) is incorrect.
- The electric socket of the PC to perform operation management has dropped.

- The LAN cable used by AMT of PC to perform operation management has dropped.
- The PC to perform operation management is connecting to wireless LAN.

6. After confirming the power operation has been done successfully, repeat "Step 4." And confirm the power status of PC.

3.2.8 View the Collected File

The administrator can view the collected file directly. The files are saved in the following directory.

Directory for saving collected file

DTP installation directory\FJSVsbinv\collect

In addition, to view the collected files, view the content under the above directory directly using Explorer .etc in CS. (It is unable to view from the main menu).

To view the collected file, refer to the following folder.

DTP installation directory\FJSVsbinv\collect\file\"User ID"+"PC Name" + "Higher Server Name"

Example) When the user ID is 0001, PC name is host1 and the upper server name is upperhost

C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbinv\collect\file\0001+host1+upperhost

See

The directory for saving the collected file 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 *Systemwalker Desktop Patrol Reference Manual*.

Note

The collected file will not be deleted automatically even if the file collection policy settings are changed. Manually delete unnecessary files.

View simple operation log file

The created simple operation log file is saved in the following directory of CT.

Installation directory of CT\invcl\inv\meter\opelog

In addition, when notified to CS, it will be saved under the Directory for saving collected file on CS.

To view, view directly under the directory.

The simple operation log file of maximum 4 months will be saved. The meaning of each created file is as follows.

UserOperation.00.wdu: Simple operation log file of this month

UserOperation.01.wdu: Simple operation log file of last month

UserOperation.02.wdu: Simple operation log file of two months before

UserOperation.03.wdu: Simple operation log file of three months before

For the format of each file, refer to *Systemwalker Desktop Patrol Reference Manual*.

3.2.9 Confirm the Collection Status of PC Information

When the PC information cannot be collected from PC for some reasons, the correct PC information cannot be grasped. This section describes how to confirm the collection status of PC information from PC.

When confirming from the main menu

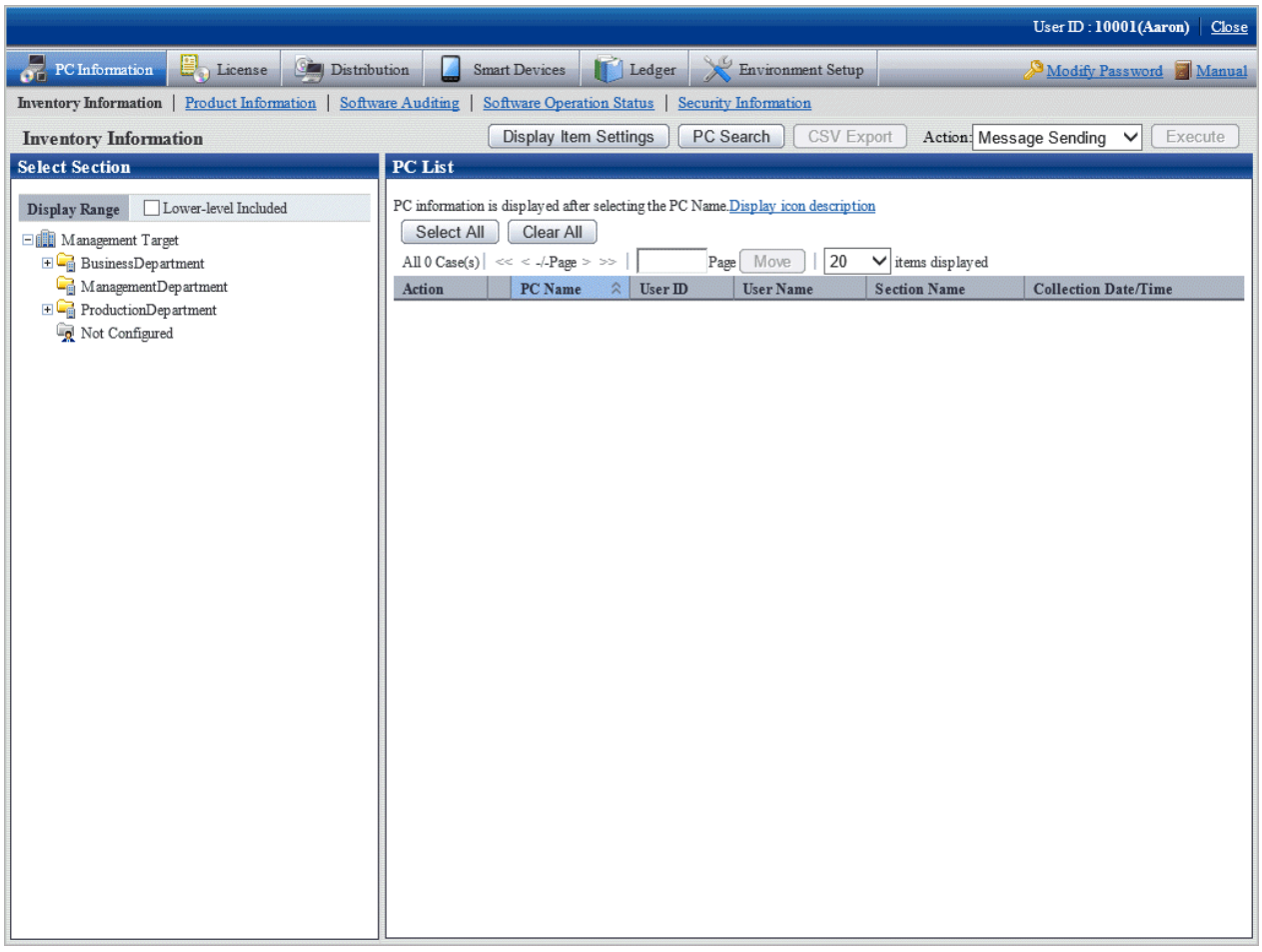
The procedure of confirming the collection status of PC information from the main menu is shown below.

1. Log in to the main menu, and click **PC Information**.

   The **PC Information** window will be displayed.

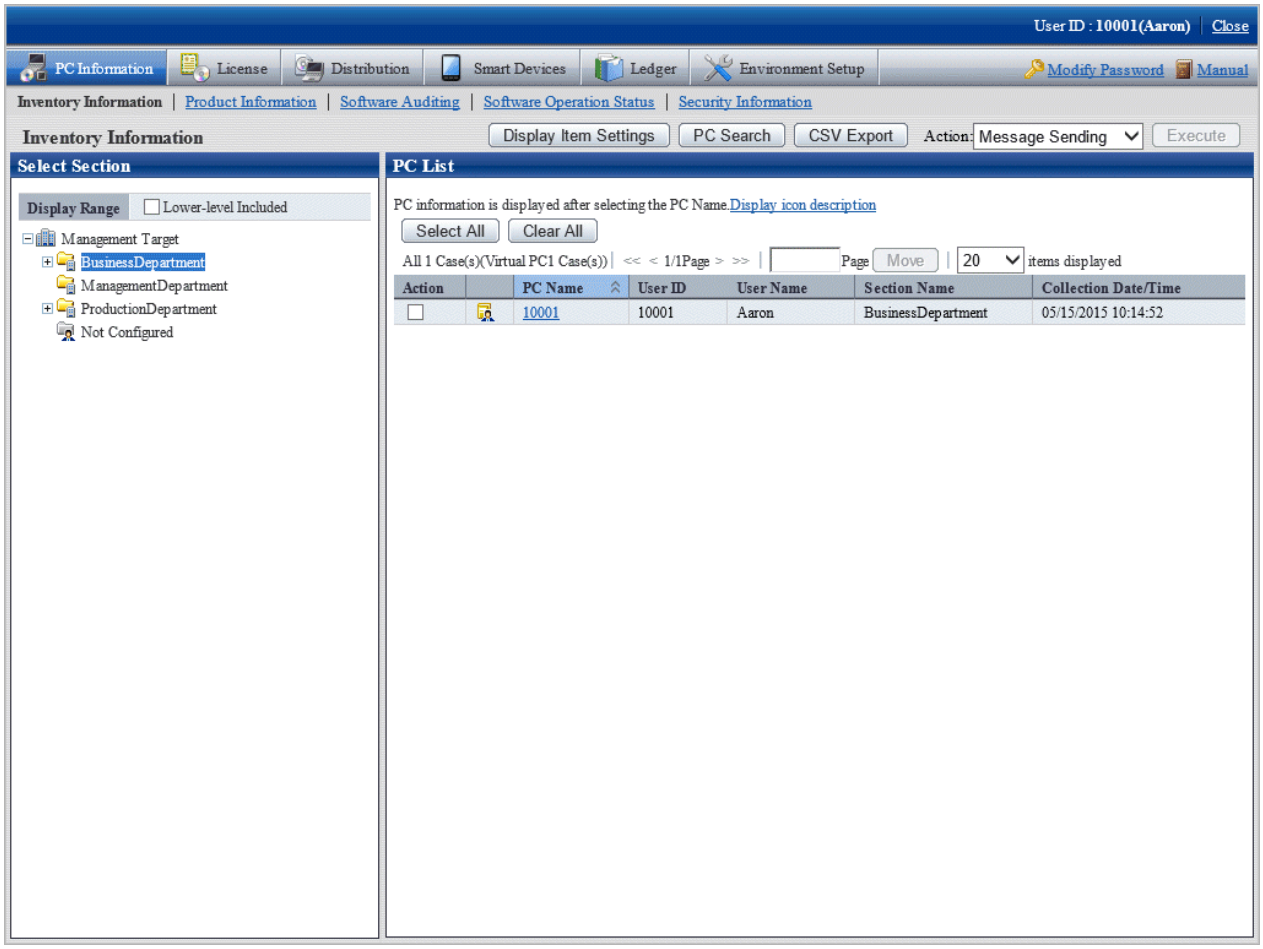
2. Click **Inventory Information**

   The following window will be displayed.



3. Select a section from the section tree in the field on the left.

   The PC under the selected section will be displayed in the field on the right.



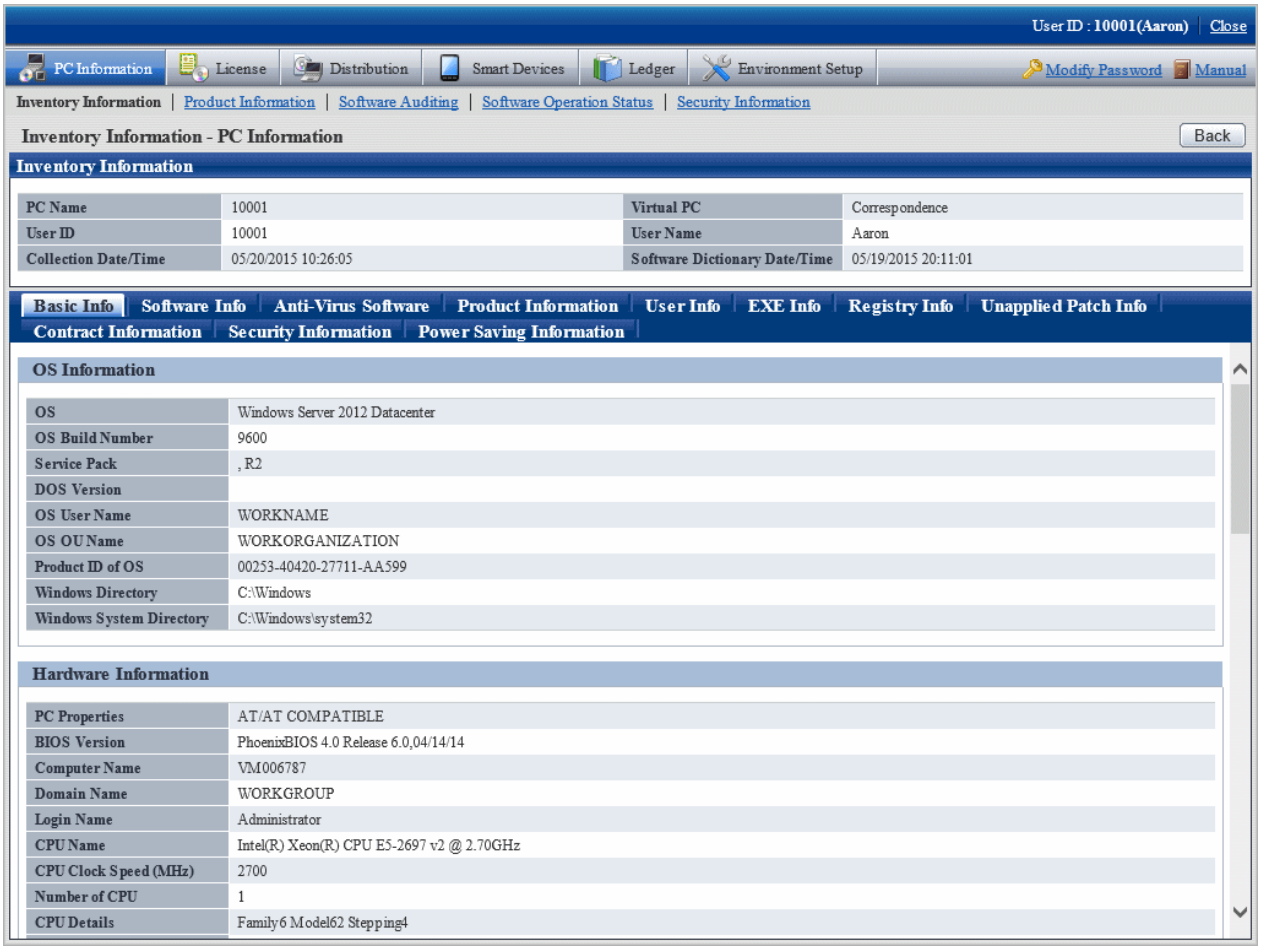
4. Click the PC name in the field on the right.

   The inventory information of clicked PC will be displayed.

Item to be confirmed

Confirmation of collection status of PC information is performed from the **Inventory Information** window displayed in the above procedure. The following shows the **Inventory Information** window.

The **Collection Date/Time** in the following window is the time when PC information is collected.



When Collection Date/Time **is not updated**

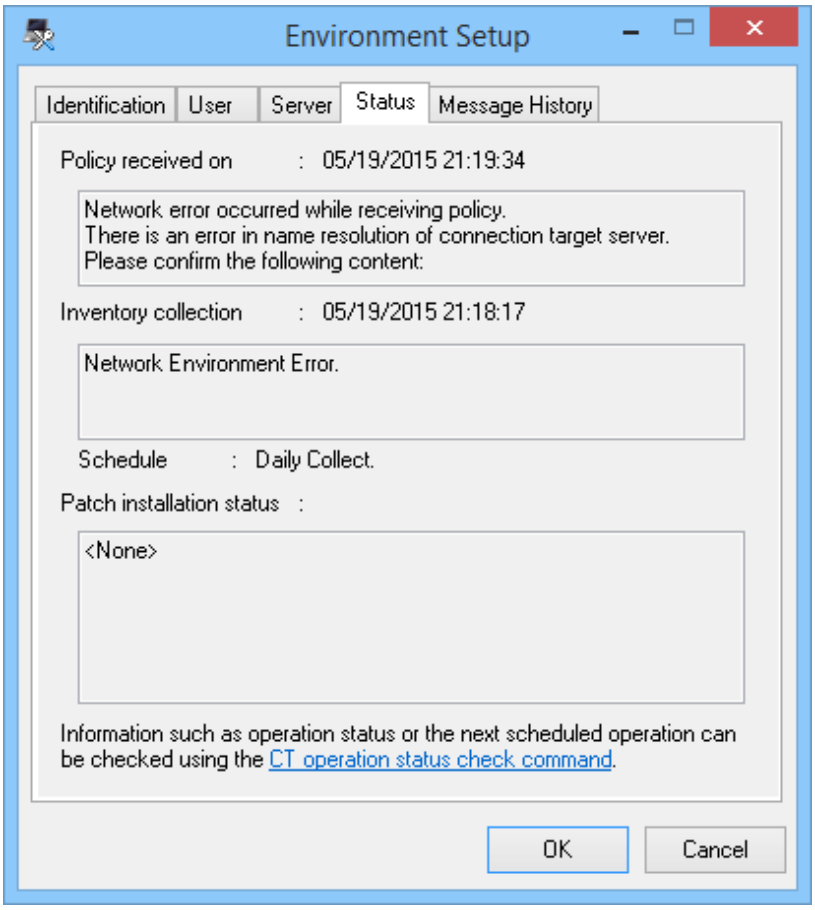
The **Collection Date/Time** cannot be updated in following cases.

- The CT that collects PC information is not connected to power
- The Ct that collects PC information is not connected to network

To collect the latest PC information, solve the above problems first.

When the problem is not solved, it is likely that error will occur in the inventory collection process of client. Refer to CT operation status log and the **Status** tab of the **Environment Setup** window of CT and "Messages of Systemwalker Desktop Patrol CT" of *Systemwalker Desktop Patrol Reference Manual* to find out the cause and solve it.

The example of the **Environment Setup** window of CT is shown below.



Policy received on column: when communication exception occurs, the information will be displayed here.

Inventory collection column: When exception occurs in inventory collection, the information will be displayed here.

When confirming from the CT operation status log

The collection status of PC information can be confirmed from the CT operation status log. The method of confirming CT operation status log is shown below.

1. Confirm the name of PC to confirm operation status of CT in the main menu.
2. In the CT operation status log saved on CS, search the information of PC name and confirm whether the collection of PC information has completed or not.

   Use Microsoft(R) Excel or editor to view and search CT operation status log.

   The CT operation status log is saved in the following directory in default settings.

Installation directory CS\FJSVsbinv\ct_trace\ + PC Name + Higher Server Name \dpsysdYYYYMMDD.log

   Note. The saving location and days managed of Ct operation status log can be modified using the SVPolicy.exe (server environment setup) command.

   For details of CT operation status log, refer to *Systemwalker Desktop Patrol Reference Manual.*

The example of CT operation status log when PC information is not collected is shown below.

- Example 1: when failed to collect PC information

```
user1, pc1, server1, 2007/03/30 20:09:28.270, INFO, DTP, SVCSTART,
user1, pc1, server1, 2007/03/30 20:01:10.544, INFO, WINDOWS, LOGON,
```

```
user1, pc1, server1, 2007/03/30 20:15:55.717, INFO, POLICY, RECEIVE, OK
user1, pc1, server1, 2007/03/30 20:15:55.717, INFO, POLICY, UPDATE, OK
user1, pc1, server1, 2007/03/30 20:15:55.717, ERROR, INVENTORY, COLLECT, Failed(7)
```

Pay attention to the line in red. Since exception occurred in the collection process of PC information, it can be known that the PC information is not notified to higher server from CT.

- Example 2: When PC information cannot be collected due to failure in policy receiving

```
user1, pc1, server1, 2007/03/30 20:09:28.270, INFO, DTP, SVCSTART,
user1, pc1, server1, 2007/03/30 20:01:10.544, INFO, WINDOWS, LOGON,
user1, pc1, server1, 2007/03/30 20:15:55.717, ERROR, POLICY, RECEIVE, Failed (2)
```

Pay attention to the line in red. Since it failed to receive policy and information cannot be collected on CT, it can be known that the PC information is not notified to higher server.

- Example 3: When no exception is recorded in CT operation status log

  When no exception is recorded in CT operation status log, it indicates that there is no problem on CT. Confirm whether CS and DS are running in **Environment Setup** > **Settings and Operation Status of Server** of the main menu.

3.2.10 Timing of Collecting PC Information

Through viewing PC information, the status of CT can be confirmed. However, if the collected PC information is not the latest, the latest status of CT cannot be confirmed.

Therefore, when collecting PC information, it is required to grasp the timing of collecting PC information. After grasping the timing information, the latest status of CT can be confirmed when viewing PC information.

Timing of collecting PC information

There are following five types of collection opportunity of PC information, and the collected timing is also different. The collected PC information will be sent after collection.

	Collection Opportunity	Frequency	Collected Timing	Sending Target
1	At installation (Note 1)	Only once after installation	After installation has completed	All information (Note 2)
2	Time when client policy is set in schedule	Specified day of a week (specify a day of a week) or Once a day (everyday)	Timing of confirming the first new arrival that exceeds 24 hours (Note 3)	Difference information (Note 4)
		At new arrival confirmation of client policy	When software dictionary has changed (user definition) (Note 3)	
			When re-collection process (-cl.recollect.inventory on) is specified for CustomPolicy.exe	All information (Note 2)
3	At automatic installation of security patches	When automatic installation of security patches is performed at new arrival confirmation of client policy (Note 5)	When the last automatic installation of security patch to PC has completed After security patch has been installed, when restart is required and collection will be performed	Difference information (Note 4)

	Collection Opportunity	Frequency	Collected Timing	Sending Target
			after restart. When restart is not required for installing security patches and collection will be performed immediately.	
4	When the diagnosis result window of operation settings is displayed	When the diagnosis result window of operation settings is displayed at specified timing after performing the setting to display the diagnosis result window of operation settings in client policy and the setting of selecting **Perform Inventory Collection at Display**	When the diagnosis result window of operation settings is displayed	Difference information (Note 4)
5	During operation action-triggered inventory collection	When operation action-triggered inventory collection is instructed by the administrator	When operation action is performed	All information (Note 2)

Note 1)

When the registered updater is applied during installation, collect PC information after the PC has been restarted.

Note 2)

Send all information of PC information ((hardware information, software information, program information, user information, software operation status, EXE file information, registry information and file collection) *, security information, power saving information, link with Systemwalker Desktop series and software dictionary version number information).

*It is the time when setting to collect such information in client policy only.

Only the difference part of data changed from the last collection will be sent for software operation status. Considering the load on CPU, when collecting PC information, collection will be performed when the CPU load is lower than 50%. If the CPU load is not lowered after 1 hour, collection will be performed by force.

Note 3)

For the PC that is connected to power on the day, inventory collection will be performed at next confirmation of new arrival.

Note 4)

Hardware information and software dictionary version information are sent even when there is no difference.

Note 5)

When performing new arrival confirmation of client policy, if the software dictionary has changed and security patches are installed automatically, PC information will be collected after automatic installation of security patches.

If the disk capacity information contained in hardware information has changed more than 10% comparing to last inventory collection, it will be collected and sent.

Note 6)

The following settings can be performed.

- Display at logon

- Display at logon and specified time

Remarks. After inventory collection has started, even if logoff, the collection process will be completed.

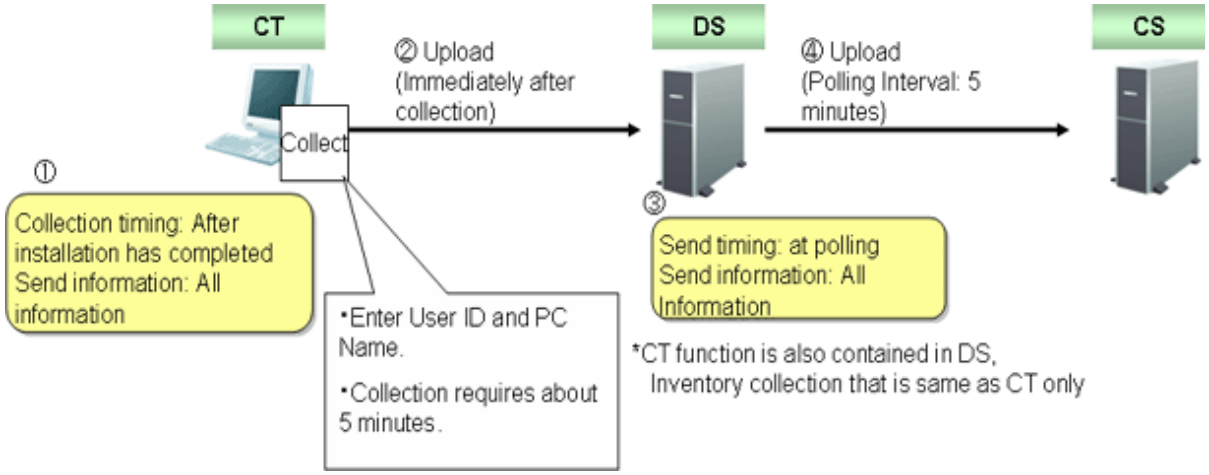
Flow till PC information has been collected

For the flow till the PC information has been collected, it describes according to the collection opportunity shown below.

- Collection at installation
- Collection at the time set in schedule
- Collection after automatic installation has completed

3.2.10.1 Collection at Installation

The summary of collection at CT installation is shown below.



3.2.10.2 Collection at the Time Set in Schedule

The flow of inventory collection according to schedule is shown below. In addition, the relationship among CS, DS and CT for collecting inventory information within the time frame from power on to power off is described in time series.

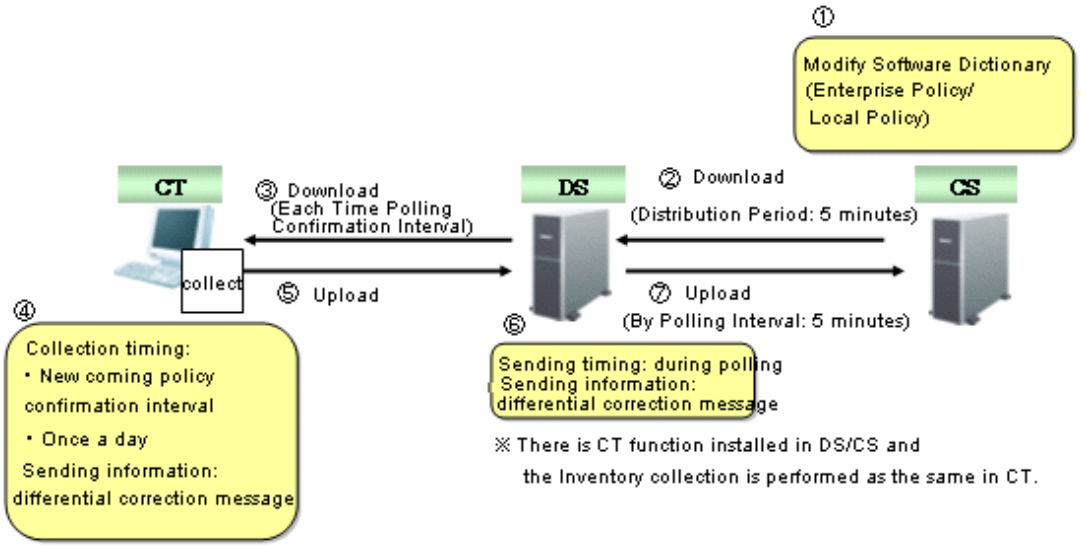
The collection condition of PC information is considered as the following settings (the value is the initial value after installation).

[Settings of Client]

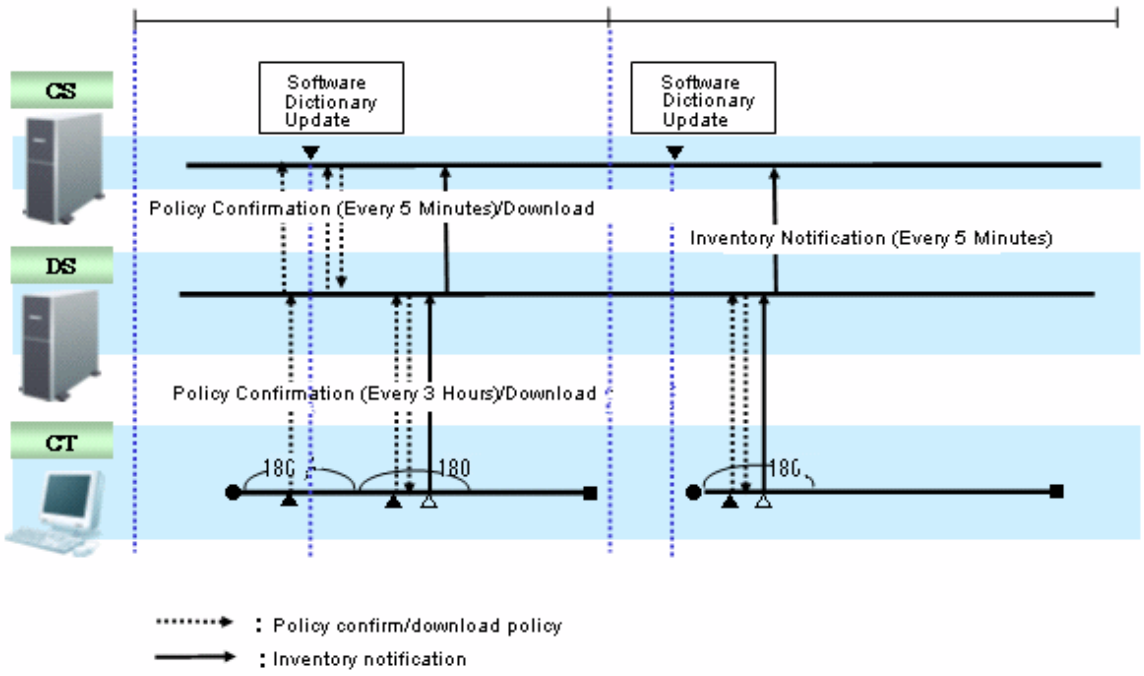
- Set in the basic policy of **Environment Setup** > **Policy Groups** > **Customize Various Policies** of the main menu.
  - **Common Settings** tab:

    Interval of Confirming Policy: 180 minutes

Summary



Time series (in normal operation)



●: Connect to power

■: Cut off power

▲: Policy confirmation

△: Inventory collection

Inventory collection is executed according to the following procedure.

1. Start the inventory collection function when power is connected.

2. Confirm policy according to the interval specified in **Interval of Confirming Policy** (Note).

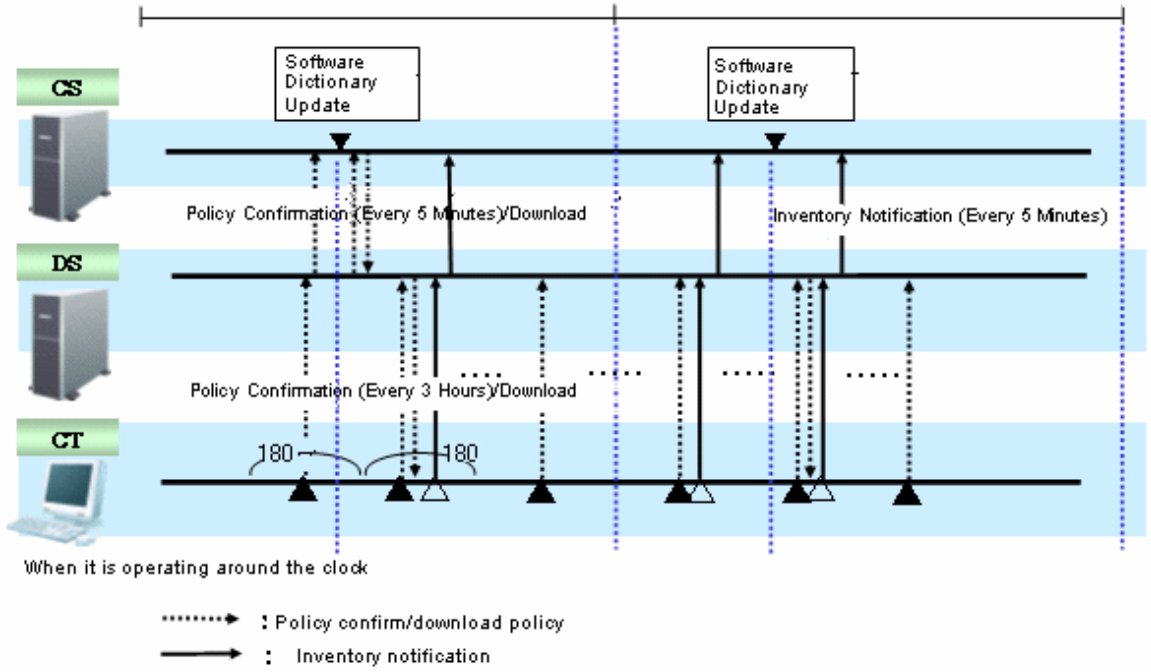
   When software dictionary or client policy is updated, download policy and collect PC information (inventory information).

   When software dictionary or client policy is not updated, policy download and inventory collection will not be performed.

3. If the collected inventory information is different from the last time, the difference will be notified to DS.

   Note) The timing to confirm policy is in the range of time specified in **Interval of Confirming Policy** from the time when power is collected, so that collective access to DS can be prevented.

Time series (in 24-hour operation)



: Connect to power

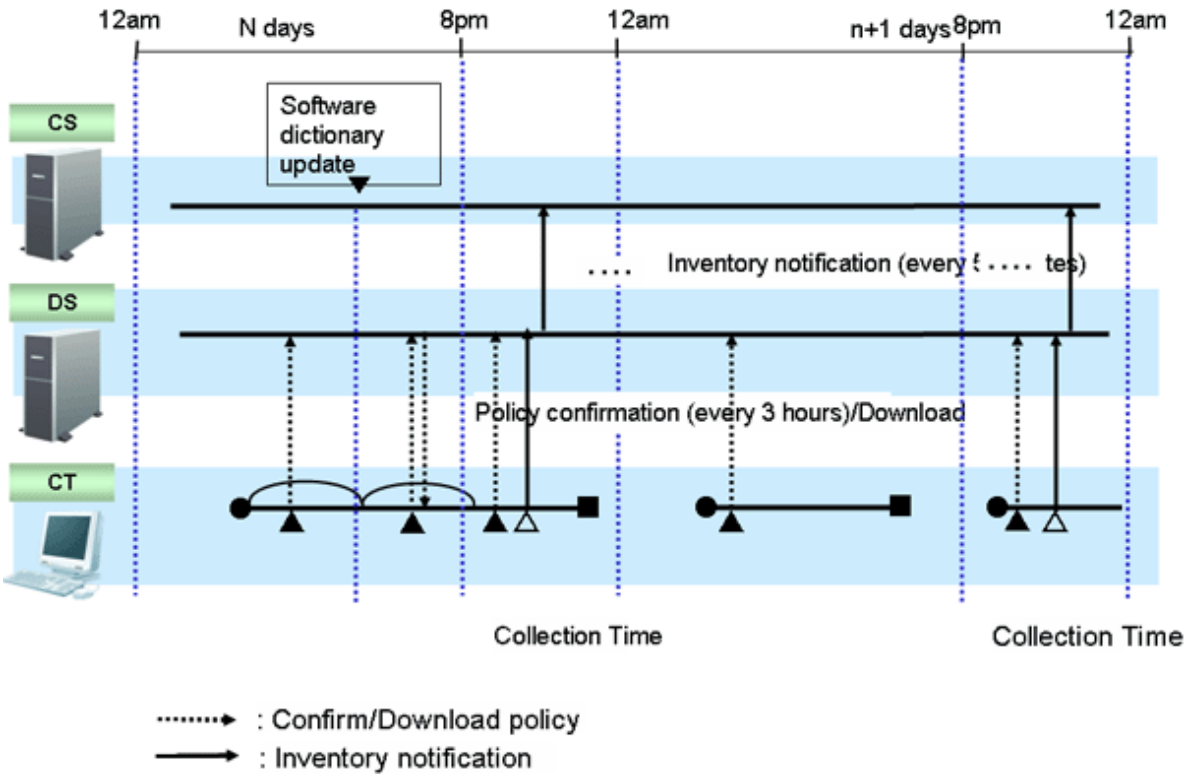
: Cut off power

: Policy confirmation

: Inventory collection

In case of 24 hours running, the procedure of inventory collection is the same as "in normal operation", but after date has been updated, even if the software dictionary or client policy is not updated, inventory collection will still be performed. If the inventory information is different from the last time, the difference will be notified to DS.

Time Series (When specifying inventory collection time)



●: Connect to power

■: Cut off power

▲: Policy confirmation

△: Inventory collection

Specify the time frame and inventory can be collected.

The time interval of confirming policy and the condition of downloading policy is the same as "In normal operation" and "In 24-hour operation", but inventory collection is performed at the time specified in the collection time only.

At the time outside the specified time frame, even if policy has been updated and downloaded, inventory collection will not be performed.

When specifying collection time, the inventory collection within specified time is performed once a day. Inventory collection will not be performed twice even if restarting in the same day.

3.2.10.3 Collect after Automatic Installation of Security Patches has Completed

The inventory collection flow after the automatic installation of security patches has completed is as follows. In addition, the relationship among CS, DS and CT for collecting inventory information within the time frame from power on to power off is described in time series.

In addition, the relationship between the type of security patch and inventory collection is described.

The collection condition of PC information is as follows.

[Settings of Client]

- Set in basic policy of **Environment Setup** > **Policy Groups**> **Customize Various Policies** of the main menu
  - **Common Settings** tab:

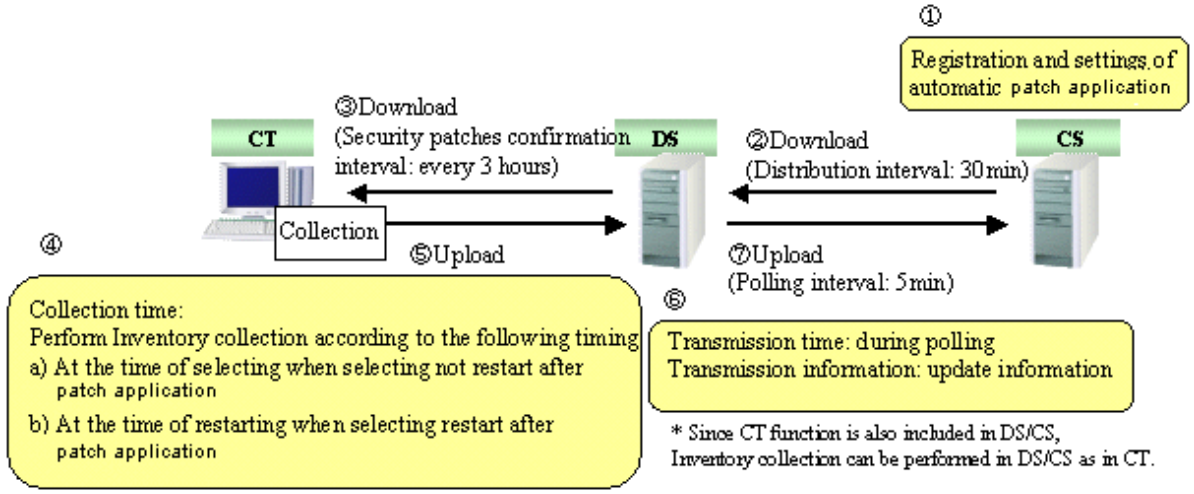
    Interval of Confirming Policy: 180 minutes

The automatic installation condition of security patch is as follows.

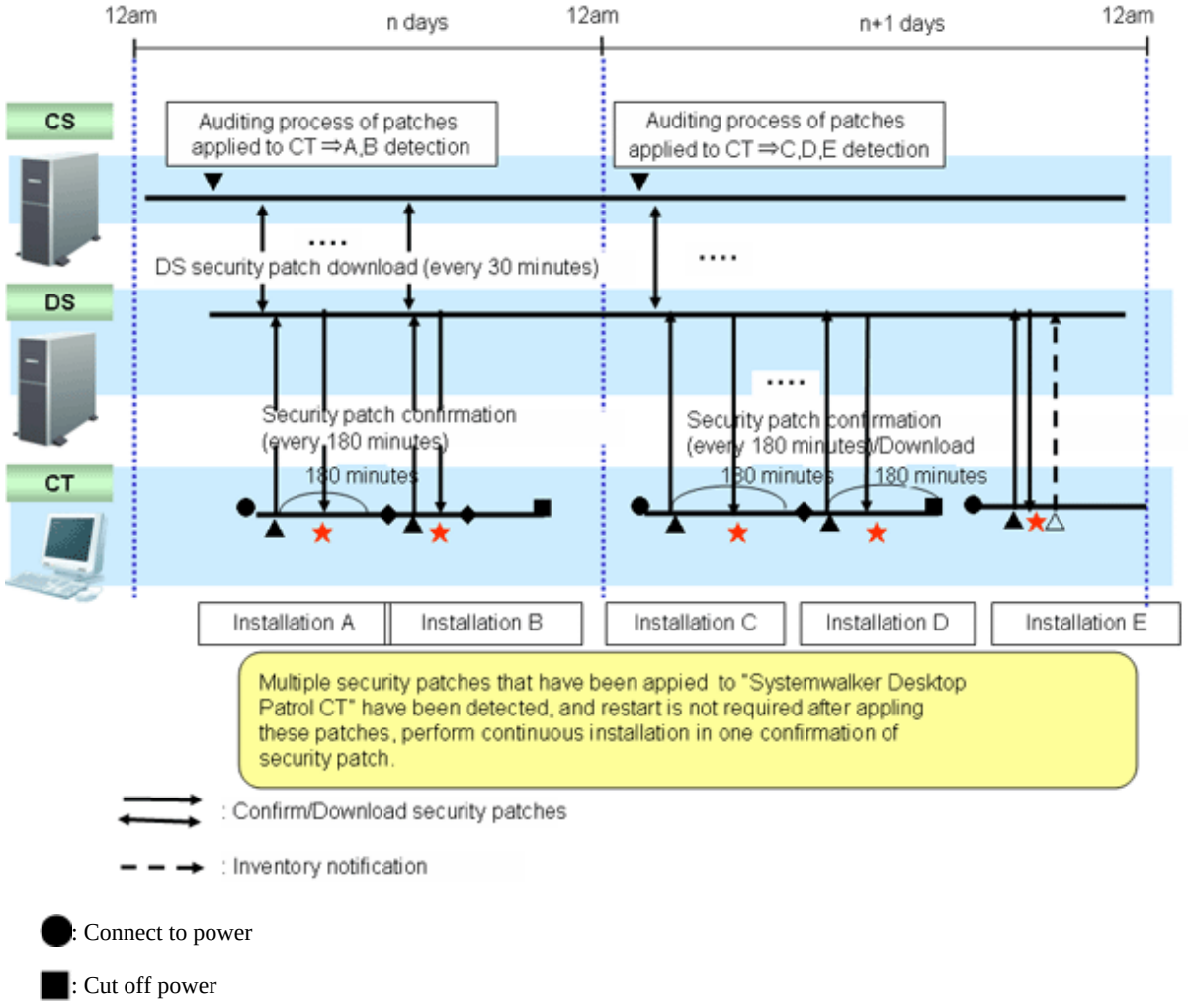
- Security Patch A, B C: required to restart

- Security Patch D, E: no need to restart

Summary



Time series



: Connect to power

: Cut off power

▲: Policy confirmation

△: Inventory collection

★: Download and installation of security patches

◆: Restart

Confirm the security patches in **Interval of Confirming Policy** specified based on power connection.

When not to restart is selected in the message after security patch installation, inventory collection will be performed immediately.

When restart is selected in the message after security patch installation, inventory collection will be performed according to the value set in **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** tab > **Common Settings** tab > **Interval of Confirming Policy**.

3.2.11 Display Operation Status and Perform Operation Processing

This section describes he operation of displaying operation status and performing operation processing in the status window.

The operation processing in the status window can be performed in the window for viewing the PC corresponding to aggregation item. Refer to "3.2.11.4 View Corresponding PC according to Aggregation Item".

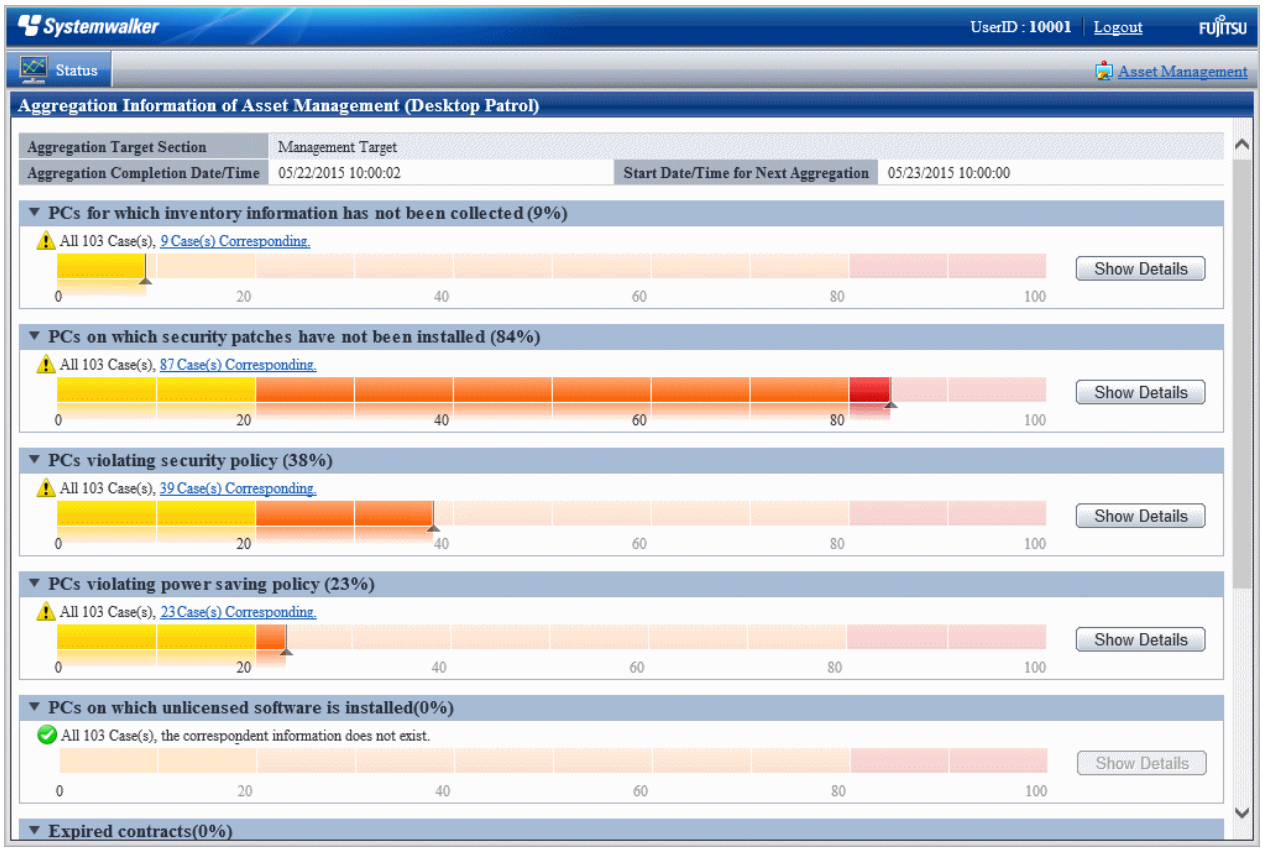
3.2.11.1 View Status Window from Login

The status window will be displayed after logging in as system administrator and section administrator.

The procedure of viewing from the main menu is shown below.

1. Log in to the main menu.

   The status window will be displayed.



   The range of status can be confirmed varies depending on operation authority.

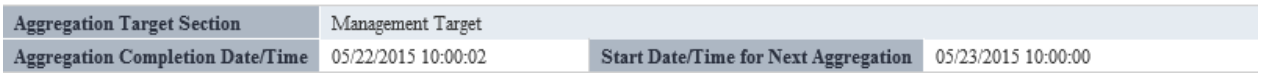
Operation Authority	Confirmation Range
System administrator	The status of the whole system of Systemwalker Desktop Patrol can be confirmed. Status relating to **Without Configuration** can also be confirmed.
Section administrator	The status of the entire section to which the section administrator belongs can be confirmed.

Displayed items

The displayed items are shown as follows.

Item	Content
Status	It is a window in which the operation status can be confirmed at one view.
User ID	The user ID that has logged in will be displayed.
Assets Management	When viewing details relating to asset management or performing settings relating to the status window, click this link.

Information relating to aggregation

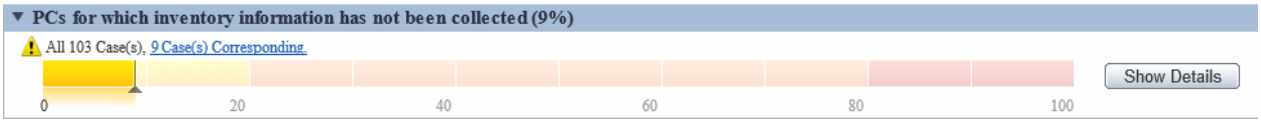


Item	Content
Aggregation Target Section	It shows the range of aggregation sections output to the status window. The range of department to be aggregated varies depending on the authority of login ID. System administrator: managed target (target at the whole section) Section administrator: Section to which it belongs (include lower level)
Aggregation Completion Date/Time	It shows the time when aggregation has completed. This information can help determining the time point when the aggregation information is output to status window. When it is in aggregation, "(Aggregating)" will be displayed after the time. When the time is not displayed, it means aggregation has not been performed yet.
Start Date/Time for Next Aggregation	It shows the time when next aggregation will be started. The timing when the information of status window is updated can be predicted through this information.

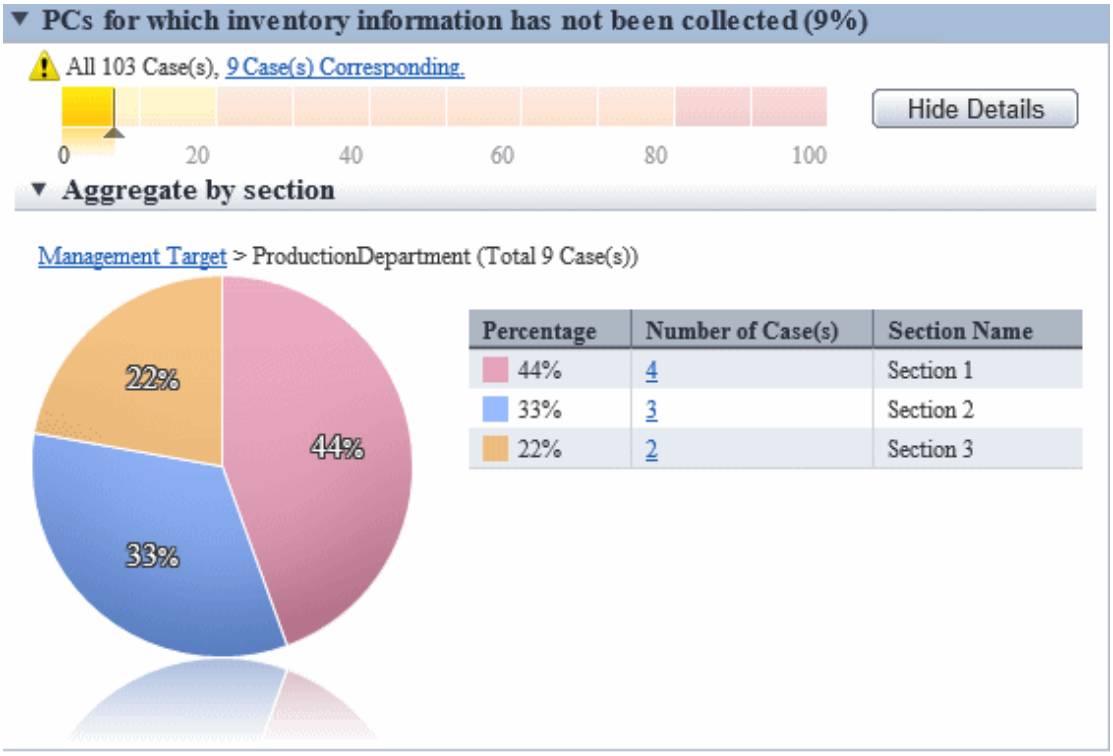
Each aggregation item

The display format of each aggregation item is described by taking **PCs for which inventory information has not been collected** as an example.

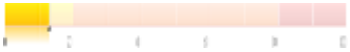
When the Show Details button is not clicked



When the Show Details button is clicked



Item	Content
(50%)	Percentage of PCs/devices/contracts that fall into each aggregation item in the aggregation target section. If the aggregation item is **Devices detected as unregistered devices**, then the number of devices is displayed instead of the percentage. The percentage is an integer value, rounded up to the first decimal point if the value is less than 50%, or truncated to the first decimal point otherwise.
	It means the ratio is 0%. If the aggregation item is **Devices detected as unregistered devices**, then this means that no unregistered device has been detected.
	It means the ratio is over 1%. If the aggregation item is **Devices detected as unregistered devices**, then this means more than one unregistered device has been detected.
All 15 Case(s), 14 Case(s) Corresponding.	Number of PCs/devices/contracts that fall into each aggregation item in the aggregation target section. If the aggregation item is **Devices detected as unregistered devices**, only the number of unregistered devices is displayed. Click the link of the corresponding number and only the list of PCs/devices/contracts that is corresponding to this aggregation item will be displayed.

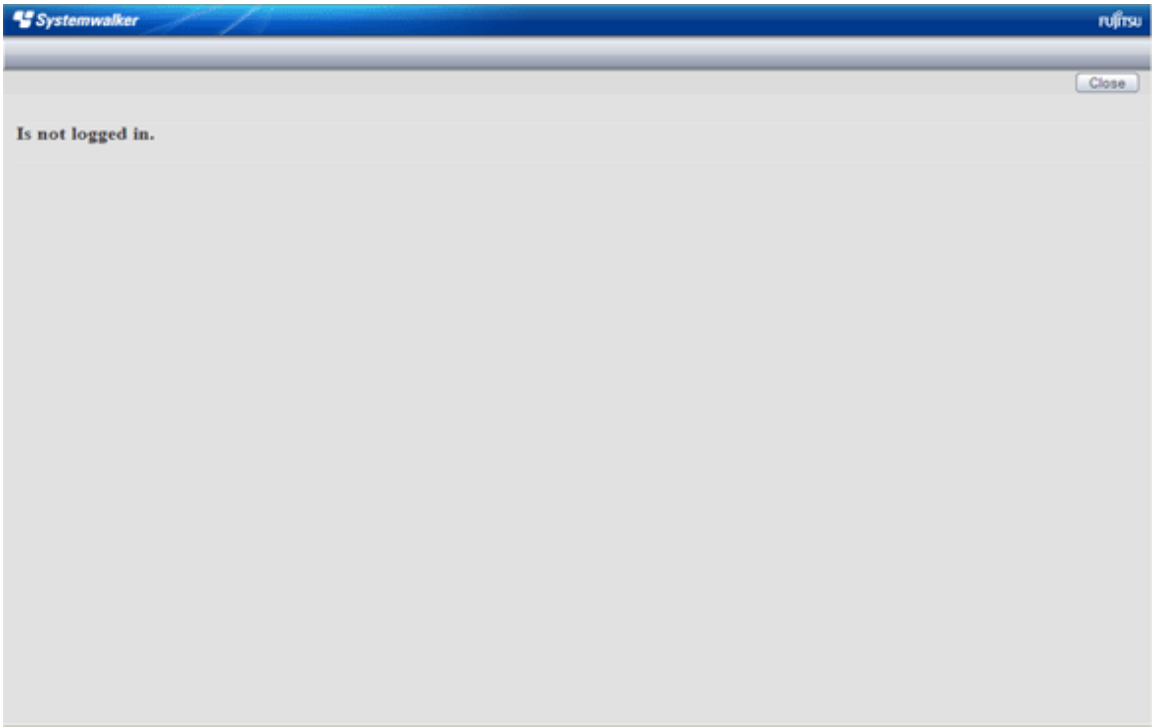
Item	Content
	Proportion of PCs/devices/contracts corresponding to each aggregation item against all PCs/devices/contracts of the section to be aggregated in bar graph. If the aggregation item is **Devices detected as unregistered devices**, this will not be displayed because it is not the percentage. When the proportion is less than 50%, the first decimal place will be rounded up. When it is over 50%, the first decimal place will be rounded down and only the integer part will be displayed.
	To view the details of each aggregation item, click the **Show Details** button. This button cannot be clicked if no PC/device/contract that falls into the aggregation item exists. To close the details window, click the **Hide Details** button.

Note

- When logout from the status window at the time when the asset management window is displayed

  Since the asset management window has already been displayed in another window, even if logging out from the status window, the asset management window will still be displayed sometimes.

  At this time, after operating the asset management window, it will become the window as follows which is unable to operate.



3.2.11.2 View the Display of Aggregation Items

It describes the displayed content of the aggregation items displayed on the status window.

Note

If **Connection Server** set in the **Server** tab of the **Environment Setup** window on CT is changed from the host name specified when CS or DS is built, the server may be deemed non-target for auditing and may not be aggregated.

PCs for which inventory information has not been collected

View **PCs for which inventory information has not been collected** at the time when confirming how many PCs that does not collect and notify inventory information normally.

It can be viewed according to the following items.

- The proportion of number of PCs for which inventory information has not been collected over the specified period against the number of all PCs (%)
- Proportion and number of PC according to section (%)

The information of **PCs for which inventory information has not been collected** is aggregated according to the content set in "3.1.5 Perform Settings Related to Operation Status", and the aggregation result will be displayed in the status window.

Click the **Show Details** button and the information corresponding to this item will be displayed according to the section of PC.

For information on how to view displayed content, refer to "3.2.11.3 View Details According to Aggregation Items".

Click the link of the number of PCs, the list of corresponding PCs will be displayed. Process as needed.

PCs on which security patches have not been installed

View **PCs on which security patches have not been installed** at the time when confirming the PCs on which security patches have not been installed that is supported in software dictionary.

It can be viewed according to the following items.

- The proportion of number of PCs on which security patches have not been installed against the number of all PCs (%)
- Proportion and number of PC according to section (%)

The information of **PCs on which security patches have not been installed** is aggregated according to the content set in "3.1.5 Perform Settings Related to Operation Status", and the aggregation result will be displayed in the status window.

Click the **Show Details** button and the information corresponding to this item will be displayed according to the section of PC.

For information on how to view displayed content, refer to "3.2.11.3 View Details According to Aggregation Items".

Click the link of the number of PCs, the list of corresponding PCs will be displayed. Process as needed.

In **PC Details** > **Unapplied Patch Information**, the security patches to be installed will be displayed.

PCs violating security policy

View **PCs violating security policy** at the time when confirming the PC that violates the assigned security policy.

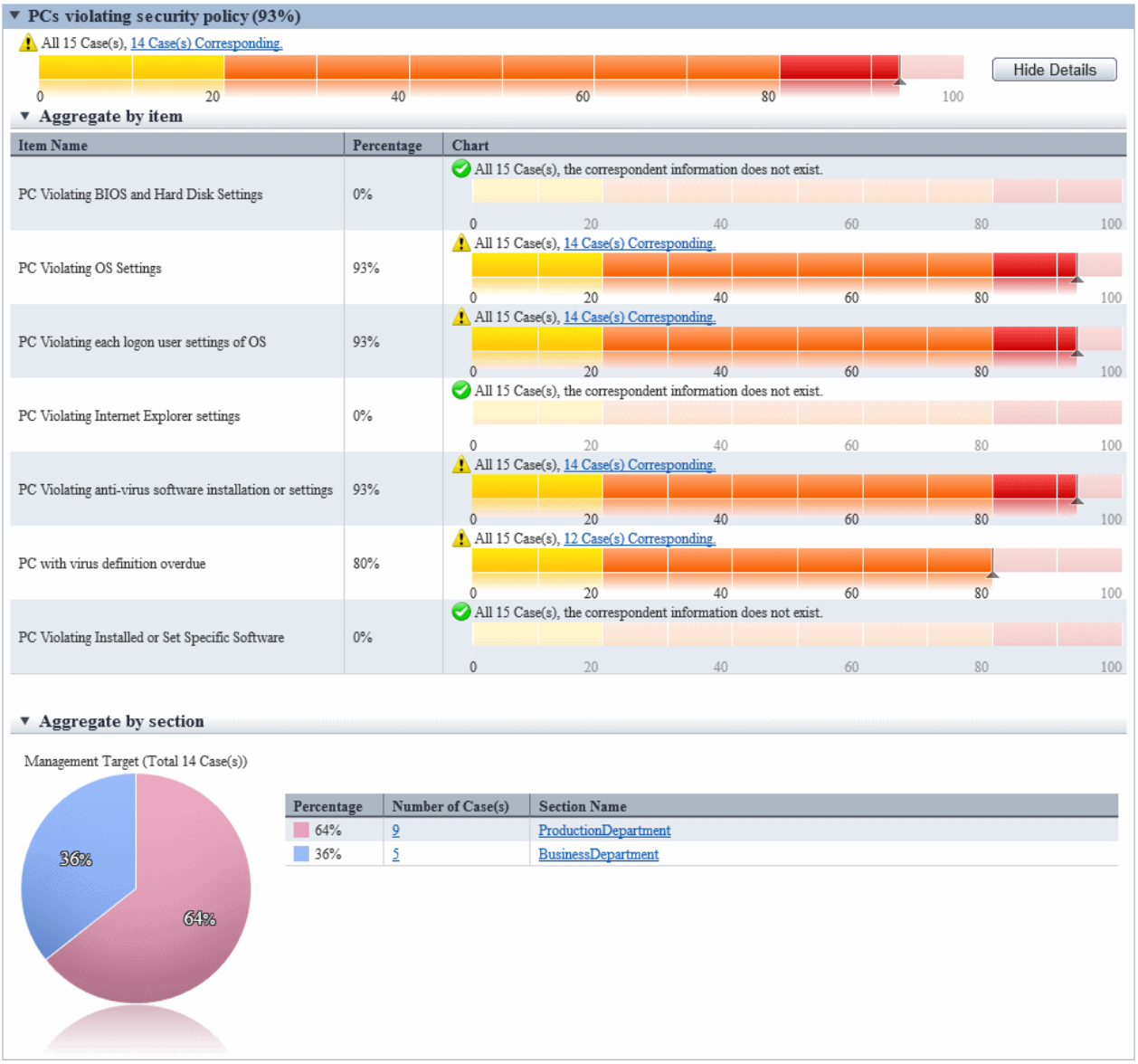
It can be viewed according to the following items.

- Proportion of the number of PCs violating security policy against the number of all PCs (%)
- Proportion and number of PC according to section (%)
- Proportion and number of PC according to item (%)

The information of **PCs violating security policy** is aggregated according to the content set in "3.1.5 Perform Settings Related to Operation Status", and the aggregation result will be displayed in the status window.

Click the **Show Details** button and the information corresponding to this item will be displayed according to the section of PC.

The example of display is shown below.



For information on how to view displayed content, refer to "3.2.11.3 View Details According to Aggregation Items".

Click the link of the number of PCs, the list of corresponding PCs will be displayed. Process as needed.

Information of each violation can be confirmed in **PC Details** > **Security Information** and the **Unapplied Patch Information** window. The description of each item is shown in the following table.

Item Category		Description
PCs violating security policy		It is the number of PCs that violates security policy. After selection, **Aggregate by section** and **Aggregate by item** are displayed in **Show Details**
Aggregate by section		It is the details of list item according to section.
Aggregate by item	PC Violating BIOS and Hard Disk Settings	For auditing content, refer to "Table 3.1 PC Violating BIOS and Hard Disk Settings".
	PC Violating OS Settings	For auditing content, refer to "Table 3.2 PC Violating OS Settings".
	PC Violating each logon user settings of OS	For auditing content, refer to "Table 3.3 PC Violating each logon user settings of OS".

Item Category		Description
	PC Violating Internet Explorer settings	For auditing content, refer to "Table 3.4 PC Violating Internet Explorer Settings"
	PC Violating anti-virus software installation or settings	For auditing content, refer to "Table 3.5 PC Violating anti-virus software installation or settings".
	PC with virus definition overdue	For auditing content, refer to "Table 3.6 PC with virus definition overdue".
	PC Violating Installed or Set Specific Software	For auditing content, refer to "Table 3.7 PC Violating Installed or Set Specific Software".

* When multiple exceptions exist in one item, they will be counted as exceptions of one PC without counting the total.

The detail of judgment standard is as follows.

The PC with **Judgment Result** as * will be counted as **PCs violating security policy**.

Table 3.1 PC Violating BIOS and Hard Disk Settings

Item	Auditing Settings	Setting Status	Judgment Result
BIOS Startup Password	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		Has been set	
		Correct diagnosis result (*1)	
	Audit laptop PC only	**Unable to collect**	
		Not set	*(*2)
		Has been set	
		Correct diagnosis result (*1)	
BIOS Settings Password	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		Has been set	
		Correct diagnosis result (*1)	
	Audit laptop PC only	**Unable to collect**	
		Not set	*(*2)
		Has been set	
		Correct diagnosis result (*1)	
BIOS Settings **Hard disk Password**	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*(*3)
		Has been set	
		Correct diagnosis result (*1)	
	Audit laptop PC only	**Unable to collect**	
		Not set	*(*2)(*3)
		Has been set	

Item	Auditing Settings	Setting Status	Judgment Result
		Correct diagnosis result (*1)	

*1: When the security diagnosis result is corrected to **Auditing OK** manually on CT

*2: Only the laptop PC will be judged

*3: PCs for which the hard disk password cannot be set will be judged as having the password **Not set**

Table 3.2 PC Violating OS Settings

Item	Auditing Settings	Setting Status	Judgment Result
Supporting status of OS	**Do not audit** **Do not display**	-	
	Audit	**Unable to collect**	
		Inappropriate (OS/SP is old)	*
		Appropriate	
		Correct diagnosis result (*1)	
Automatic logon	**Do not audit**	-	
	Audit	**Unable to collect**	
		Automatic logon	*
		Not automatic logon	
Welcome	**Do not audit**	-	
	Audit	**Unable to collect**	
		Display	*
		Do not display	
Last user name	**Do not audit**	-	
	Audit	**Unable to collect**	
		Display	*
		Do not display	
Security of Guest account	**Do not audit**	-	
	Audit	**Unable to collect**	
		Password is not set	*
		Password and user name are matched	*
		Password has been set	
		Not to be collected	
		Account is OFF	
		Account is disabled	
Existence of complex password	**Do not audit**	-	
	Audit	**Unable to collect**	
		Disabled	*
		Enabled	

Item	Auditing Settings	Setting Status	Judgment Result
Settings of automatic update	**Do not audit**	-	
	Audit	**Unable to collect**	
		Disabled	*
		Enabled (Details is unknown)	
		Enabled (Manual installation)	
		Enabled (Automatic)	
		Enabled (Notify update only)	
User account control (UAC)	**Do not audit**	-	
	Audit	**Unable to collect**	
		Disabled	*
		Enabled	
Unsafe shared folder	**Do not audit**	-	
	Audit	**Unable to collect**	
	OK when all of access authorizes are not possessed	**No shared folder**	
		With shared folder	*
	OK when only reading is allowed	**No shared folder that requires writing authority**	
		There is a shared folder that requires writing authority	*
Enter password when restoring from standby	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		Has been set	

*1) When the security diagnosis result is corrected to **Auditing OK** manually on CT

Table 3.3 PC Violating each logon user settings of OS

Item	Auditing Settings	Setting Status	Judgment Result
Screensaver	**Do not audit**	-	
	Audit	**Unable to collect**	
		Do not start	*(*3)
		Start	
Screensaver password	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*(*3)
		Has been set	
Password of logon user	**Do not audit**	-	
	Audit	**Unable to collect**	
		Password not set	*(*3)

Item	Auditing Settings	Setting Status	Judgment Result
		Password and user name are matched	*(*3)
		Has been set	
		Not to be collected	

*3) Even if one of the Windows logon user of the target PC violates the security policy, the security item will be considered as violation.

Table 3.4 PC Violating Internet Explorer Settings

Item	Auditing Settings	Setting Status	Judgment Result
Internet zone	**Do not audit**	-	
	Set "Medium-Low" or above as OK	**Lower than "Medium-Low"**	*
		Higher than "Medium-Low"	
	Set "Medium" or above as OK	**Lower than "Medium"**	*
		Higher than "Medium"	
	Set "Medium-High" or above as OK	**Lower than "Medium-High"**	*
		Higher than "Medium-High"	
	Set "High" or above as OK	**Lower than "High"**	*
		Higher than "High"	
	Set "Custom" as OK	**"Custom"**	
	Set "Custom" as Failed	**"Custom"**	*

Table 3.5 PC Violating anti-virus software installation or settings

Item	Auditing Settings	Setting Status	Judgment Result
Installation status of anti-virus software	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not installed	*
		Has been installed	
		Correct diagnosis result (*1)	
Real-time search of anti-virus software	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		1 has been set	
		2 or more have been set	
		Correct diagnosis result (*1)	
Scheduled scan of anti-virus software	**Do not audit**	-	
	Audit	**Unable to collect**	
		Setting is insufficient	*
		Has been set (The scanning execution date is old)	*
		Has been set	

Item	Auditing Settings	Setting Status	Judgment Result
		Correct diagnosis result (*1)	
Target scanning range of anti-virus software	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		Has been set	
		Correct diagnosis result (*1)	

*1) When the security diagnosis result is corrected to **Auditing OK** manually on CT

Table 3.6 PC with virus definition overdue

Item	Auditing Settings	Setting Status	Judgment Result
Virus pattern status of anti-virus software	**Do not audit**	-	
	1~10 Generation number that is set as OK (Audit)	**Unable to collect**	
		Newer than the set policy	
		Older than the set policy	*
		Older than 10 generations	*
		Anti-Virus software is not installed	*
		Correct diagnosis result (*1)	

*1) When the security diagnosis result is corrected to **Auditing OK** manually on CT

Table 3.7 PC Violating Installed or Set Specific Software

Item	Auditing Settings	Setting Status	Judgment Result
Firewall	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not set	*
		1 has been set	
		2 or more have been set	
Installation status of encryption software	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not installed	*
		Has been installed	
		Correct diagnosis result (*1)	
Google Desktop "Data Search on Multiple Computers"	**Do not audit**	-	
	Audit	**Unable to collect**	
		Not installed	
		Enabled	*
		Disabled	
Detection status of prohibition software	**Do not audit**	-	
	Audit	**Unable to collect**	

Item	Auditing Settings	Setting Status	Judgment Result
		Has prohibited software	*
		No prohibited software	

*1) When the security diagnosis result is corrected to **Auditing OK** manually on CT

PCs violating power saving policy

View **PCs violating power saving policy** at the time when confirming the PC that violates the assigned power saving policy.

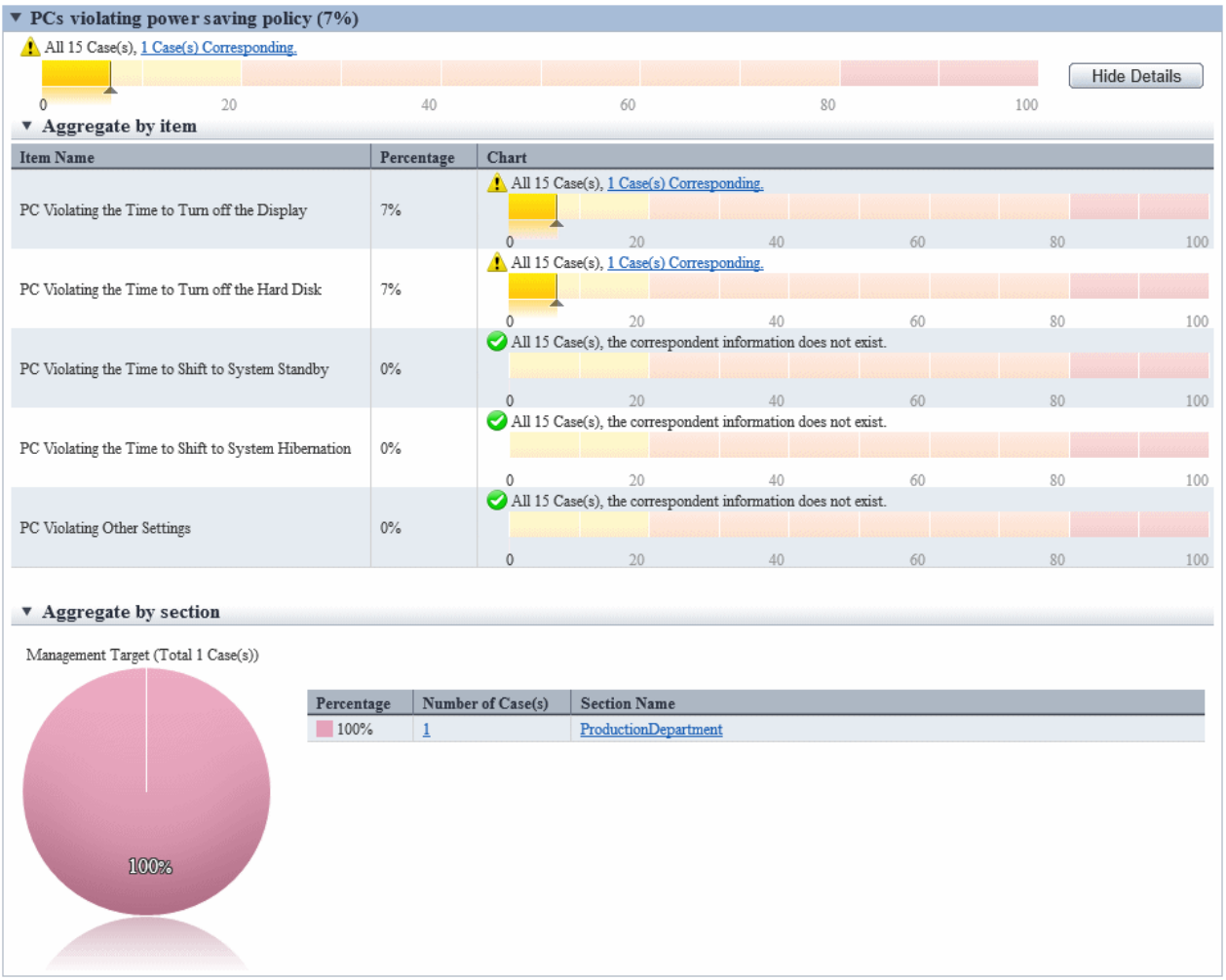
It can be viewed according to the following items.

- Proportion of the number of PCs violating power saving policy against the number of all PCs (%)
- Proportion and number of PC according to section (%)
- Proportion and number of PC according to item (%)

The information of **PCs violating power saving policy** is aggregated according to the content set in "3.1.5 Perform Settings Related to Operation Status", and the aggregation result will be displayed in the status window.

Click the **Show Details** button and the information corresponding to this item will be displayed according to the section of PC.

The example of display is shown below.



For information on how to view displayed content, refer to "3.2.11.3 View Details According to Aggregation Items".

Click the link of the number of PCs, the list of corresponding PCs will be displayed. Process as needed.

Information of each PC Violating Power Saving Policy can be confirmed in **PC Details** > **Security Information** and the **Unapplied Patch Information** window. The description of each item is shown in the following table.

Item		Description
PCs violating power saving policy		Number of PCs that violates power saving policy. After selected, **Aggregate by section** and **Aggregate by item** will be displayed in **Show Details**.
Aggregate by section		It is the details of list item according to section.
Aggregate by item	**PC Violating the Time to Turn off the Display**	For auditing content, refer to the item of **Time to turn off the power of monitor** of "Table 3.8 Auditing Item Content".
	PC Violating the Time to Turn off the Hard Disk	For auditing content, refer to the item of **Time to turn off the power of hard disk** of "Table 3.8 Auditing Item Content".
	PC Violating the Time to Shift to System Standby	For auditing content, refer to the item of **Time to shift to system standby** of "Table 3.8 Auditing Item Content".
	PC Violating the Time to Shift to System Hibernation	For auditing content, refer to the item of **Time to shift to system sleep** of "Table 3.8 Auditing Item Content".
	PC Violating other Settings	For auditing content, refer to the item of **Other settings** of "Table 3.8 Auditing Item Content".

* When PC is laptop, violation will be judged from settings both at connection to power and use of battery.

* When multiple exceptions exist in one item, they will be counted as exceptions of one PC without counting the total.

* When the number of PC with exception is 0, this item will not be displayed.

The detail of judgment standard is as follows.

The PC with **Judgment Result** as ***** will be counted as **PCs violating power saving policy**.

Table 3.8 Auditing Item Content

Item	Auditing Settings	Setting Status	Judgment Result
Time to turn off the power of monitor	**Do not audit**	-	
	None is OK	-	
	OK within *n*	**Unable to collect**	
		Within *n*	
		Larger than *n*	*
Time to turn off the power of hard disk	**Do not audit**	-	
	None is OK	-	
	OK within *n*	**Unable to collect**	
		Within n	
		Larger than n	*
Time to shift to system standby	**Do not audit**	-	
	None is OK	-	
	OK within *n*	**Unable to collect**	
		Within *n*	
		Larger than *n*	*

Item		Auditing Settings	Setting Status	Judgment Result
Time to shift to system sleep		**Do not audit**	-	
		None is OK	-	
		OK within *n*	**Unable to collect**	
			Within *n*	
			Larger than *n*	*
Other settings (*1)	**Operation of Hybrid Sleep**	**Do not audit**	-	
		ON is OK	**Unable to collect**	
			OFF	*
			ON	
	Operation of Processor	**Do not audit**	-	
		Set emphasis on balance /emphasis on power saving as OK	**Unable to collect**	
			The set value of **Status of Smallest Processor** is lower than 5%	
			The set value of **Status of Smallest Processor** is higher than 5%	*
		Set emphasis on power saving as OK	**Unable to collect**	
			The set value of **Status of Smallest Processor** is 0%	
			The set value of **Status of Smallest Processor** is not 0%	*
	Settings of selective suspension of USB	**Do not audit**	-	
		Enabled is OK	**Unable to collect**	
			The set value of **Settings of Selective Suspension of USB** is **Disabled** (*2)	*
			The set value of **Settings of Selective Suspension of USB** is **Enabled** (*2)	
	Brightness settings of monitor	**Do not audit**	-	
		OK when the brightness of dark ~ normal	**Unable to collect**	
			Lower than 70%	
			Higher than 70%	*
		Dark setting is OK	**Unable to collect**	
			Lower than 40%	
			Higher than 40%	*

* In case of laptop PC, if violation exists in one of the settings of **Connect to Power** and **Use Batter**, it will be counted as PC with violation.

*1) It is for OS later than Windows Vista only. In OS prior to that, **Unable to collect** will be displayed.

*2) In Windows(R) 7 or later and Windows Server(R) 2008 R2 or later, the setting name will become **Settings of Selective Suspension of USB**.

PCs on which unlicensed software is installed

To check how many PCs in which the software is installed but license is not assigned exist, view **PCs on which unlicensed software is installed**.

The following items can be viewed:

- Number of PCs in which the software is installed but license is not assigned, and its percentage in overall number of PCs (%)
- Number of the appropriate PCs and percentage per section (%)

Clicking **Details Display** displays information about the PCs that fall into this aggregation item, grouped by section.

Clicking the number of PCs display the list of the corresponding PCs. Take the required actions, such as assigning license to the PCs.

Refer to "5.3.4.2 Processing at Confirmation of License Violation PC" for details on how to take actions.

Expired contracts

To check how many expired contracts exist, view **Expired contracts**.

The following items can be viewed:

- Number of contracts that have expired, and its percentage in overall number of contracts (%)
- Number of the appropriate contracts and percentage per section (%)

Clicking **Details Display** displays information about the contracts that fall into this aggregation item, grouped by section.

Clicking the number of contracts displays the list of corresponding contracts. Take the required actions, such as deleting contract information or extending contracts. Note that even if a contract is extended, it will still be an aggregation target as long as old contract information remains. If you do not want it to be included as an aggregation target, delete the old contract information.

Refer to "11.4.1 Confirm Contract Information" for details on deleting contract information.

Refer to "11.4.5 Extend Contract" for details on contract extension.

Contracts about to expire

To check how many contracts are about to expire, view **Contracts about to expire**.

The following items can be viewed:

- Number of contracts for which the days until expiry is less than the days before the notice of contract expiry is sent, and its percentage in overall number of contracts (%)
- Number of the appropriate contracts and percentage per section (%)

Note that "days before the notice of contract expiry is sent" is the value specified in **Management Ledger Settings** > **Set Contract Expiration Notification** > **XX Days Ago, Notify Prior Notice of Contract Expiration** (where "XX" ca be 30, 60, 90, or 180).

Clicking **Details Display** displays information about the contracts that fall into this aggregation item, grouped by section.

Clicking the number of contracts displays the list of corresponding contracts. Take the required actions, such as deleting contract information or extending contracts.

Refer to "11.4.1 Confirm Contract Information" for details on deleting contract information.

Refer to "11.4.5 Extend Contract" for details on contract extension.

Devices for which stocktaking is not yet complete

To check how many devices for which stocktaking is not yet complete exist, view **Devices for which stocktaking is not yet complete**.

The following items can be viewed, which are hidden by default. Display and use them if required during stocktaking.

- Number of devices for which stocktaking is not yet complete, and its percentage in overall number of devices (%)
- Number of the appropriate devices and percentage per section (%)

Clicking **Details Display** displays information about the devices that fall into this aggregation item, grouped by section.

Clicking the number of devices displays the list of corresponding devices. Take the required stocktaking actions to complete stocktaking.

Refer to "11.5 Stocktaking Support" for details on stocktaking tasks.

Devices detected as unregistered devices

To check the number of devices for which registration is not yet completed, view **Devices detected as unregistered devices**.

Note that "unregistered devices" are the devices that have not been registered in the asset ledger after the collection information for devices connected with the network and the asset ledger are compared.

The following items can be viewed:

- Number of the appropriate devices per installation location

Clicking **Details Display** displays information about the devices that fall into this aggregation item, grouped by installation location.Clicking the number of devices displays the list of corresponding devices. Take the required actions.

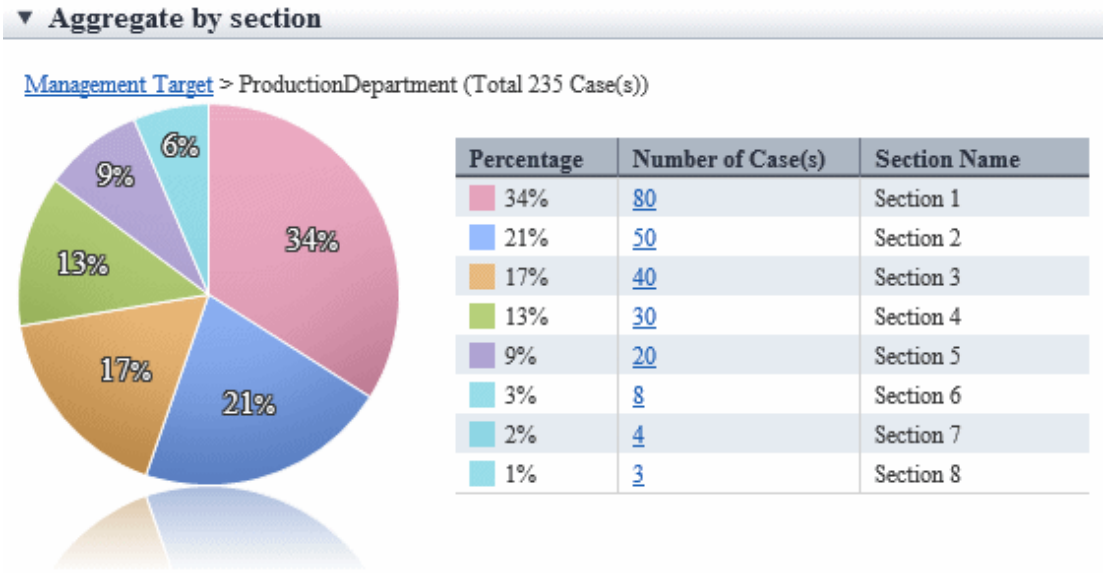
Refer to "11.2.3.2 Display/Register Unregistered Device" for details on how to take actions.

3.2.11.3 View Details According to Aggregation Items

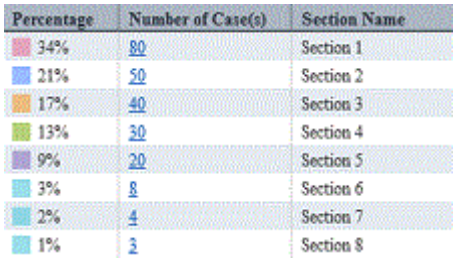
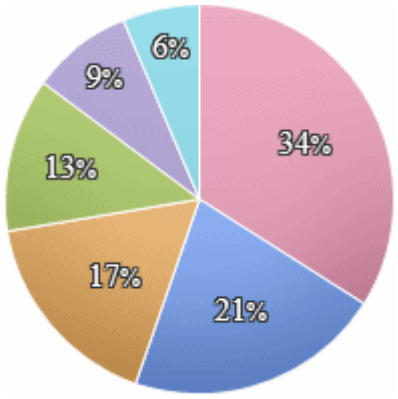
This section describes the format of details displayed after clicking the **Show Details** button in the displayed aggregation item information.

Details "Aggregate by section"

In this window, the PCs corresponding to each aggregation item is displayed according to section.



Item	Content
Management Target > ProductionDepartment (Total 235 Case(s))	It shows the sections represented by the pie chart. Section name without a link: the section being displayed currently Section name with a link: Higher section Click the link and you can switch to the details related to the clicked section. (*1) The number of PCs corresponding to the aggregation item in the section is displayed in the () after section name.

Item	Content
 Percentage / Number of Case(s) / Section Name 34% 80 Section 1 21% 50 Section 2 17% 40 Section 3 13% 30 Section 4 9% 20 Section 5 3% 8 Section 6 2% 4 Section 7 1% 3 Section 8	It shows the PCs corresponding to the aggregation item according to section. Display in order from the section with most number of PCs. The meaning of each item is as follow. **Proportion** In the section displayed currently, it shows the proportion of PCs corresponding to the aggregation item occupied in the section. In the proportion, the first decimal place will be rounded off and only the integer part will be displayed. Therefore, the total value will not be 100% sometimes. **Number of PCs** It shows the number of PCs corresponding to the aggregation item. By clicking the link, the PC list of the clicked section can be displayed. **Section Name** Display the section name. By clicking the link, the details of the clicked section can be switched. (*1) If the section displayed in the pie chart is the section itself, it will be displayed as "-". In addition, it cannot be clicked in following cases. The bottom level department Without configuration It is the section displayed in pie chart
 	It shows the proportion occupied by each ranking in pie chart. (*2) In the proportion, the first decimal place will be rounded off and only the integer part will be displayed. Therefore, the total value will not be 100% sometimes.

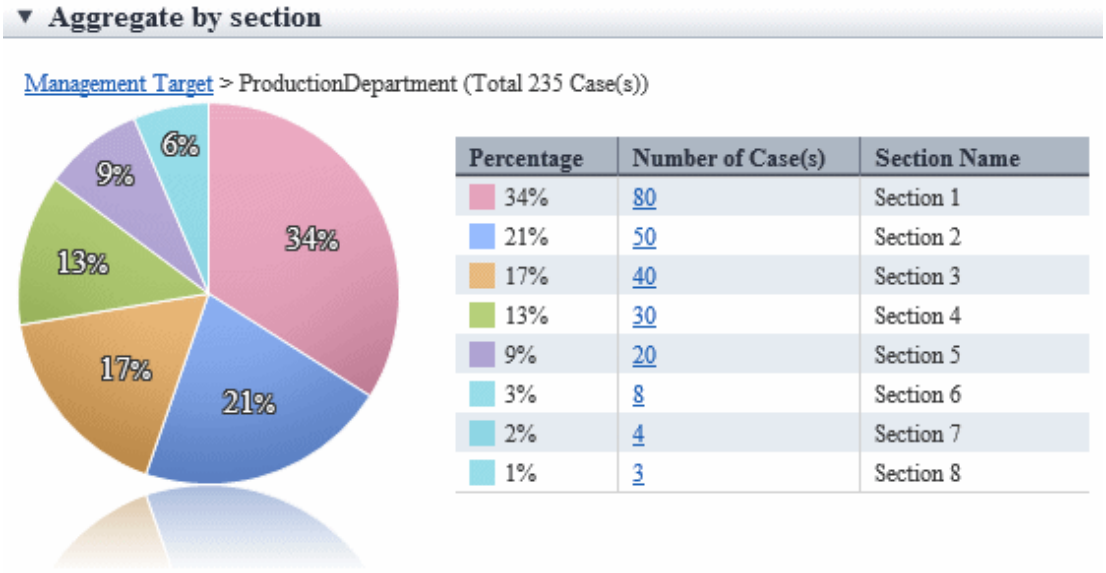
*1: When the structure of section contains multiple levels, it can be output according to level.

*2: The pie chart is displayed in different colors according to the number of PCs from more to less, and the number after the sixth will be displayed in the same color.

The example of pie chart is shown as follows.

- Example of display when the number of PCs in all sections is different.

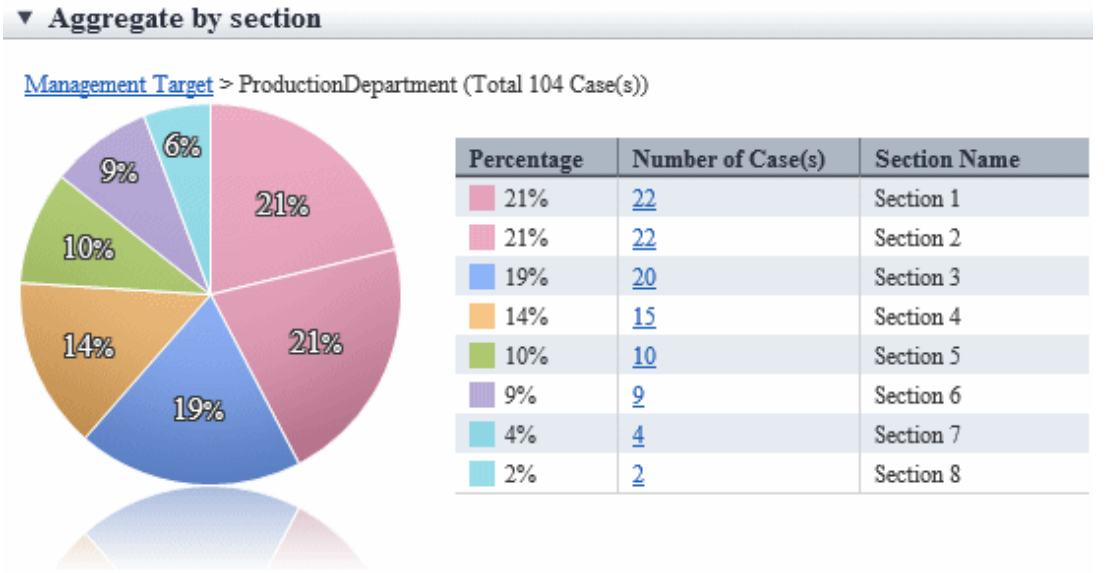
  When the number of PCs of all sections is different from section 1 to section 8. For the section after the sixth, that is, from section 6 to section 8, the number will be shown in the same color.



Percentage	Number of Case(s)	Section Name
34%	80	Section 1
21%	50	Section 2
17%	40	Section 3
13%	30	Section 4
9%	20	Section 5
3%	8	Section 6
2%	4	Section 7
1%	3	Section 8

- Example of display when the same number of PCs exists up to the fifth section

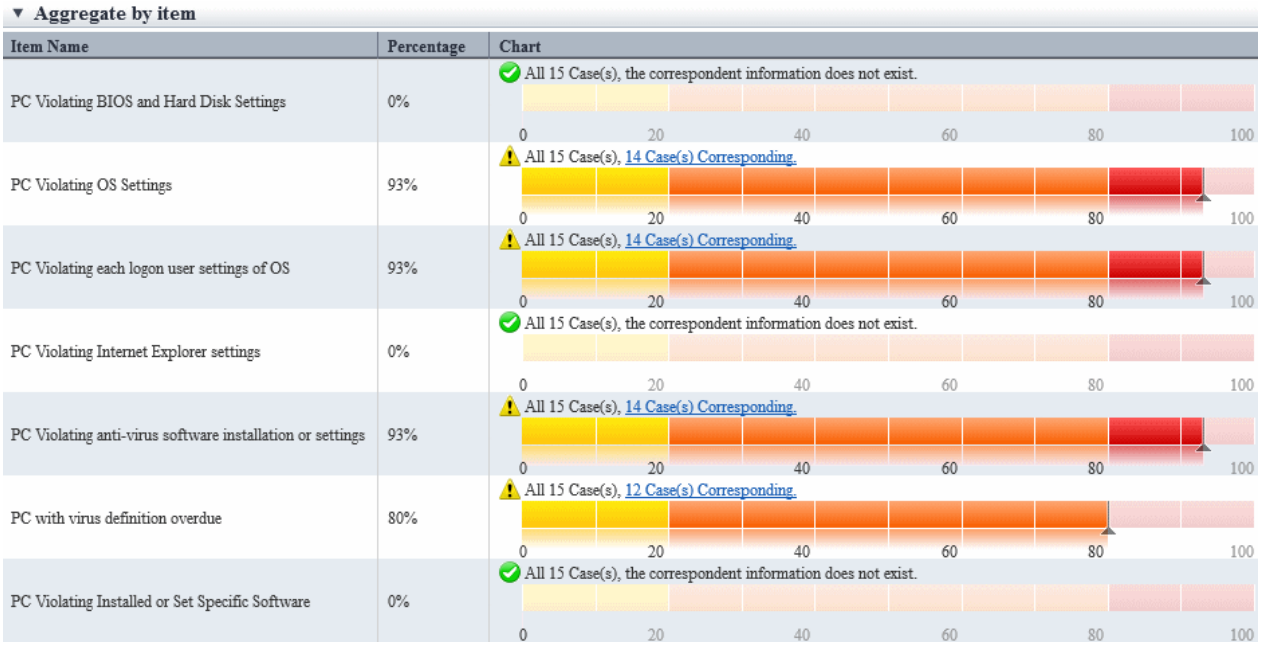
  Up to the fifth section, the number of PCs of section 1 and section 2 is the same, so section 1 and section 2 are displayed in same color.



Percentage	Number of Case(s)	Section Name
21%	22	Section 1
21%	22	Section 2
19%	20	Section 3
14%	15	Section 4
10%	10	Section 5
9%	9	Section 6
4%	4	Section 7
2%	2	Section 8

Details "Aggregate by item"

In this window, the PCs corresponding to each aggregation item is displayed according to item of policy. It takes **PCs violating security policy** as example for description.



Item	Content
Item Name	Display the item name of security policy or power saving policy. By clicking the link, you can switch to the clicked item, which is the details of PC with violation.
Percentage	It is the proportion of PC with violations against each item in the PC with assigned policy.
	It means the ratio is 0%.
	It means the ratio is over 1%.
All 15 Case(s), 14 Case(s) Corresponding.	It shows the number of PCs corresponding to each aggregation item against all PCs of the section to be aggregated. Click the link of this number, only the list of PCs corresponding the aggregation item will be displayed.
Chart	The proportion will be displayed in graphs visually.

3.2.11.4 View Corresponding PC according to Aggregation Item

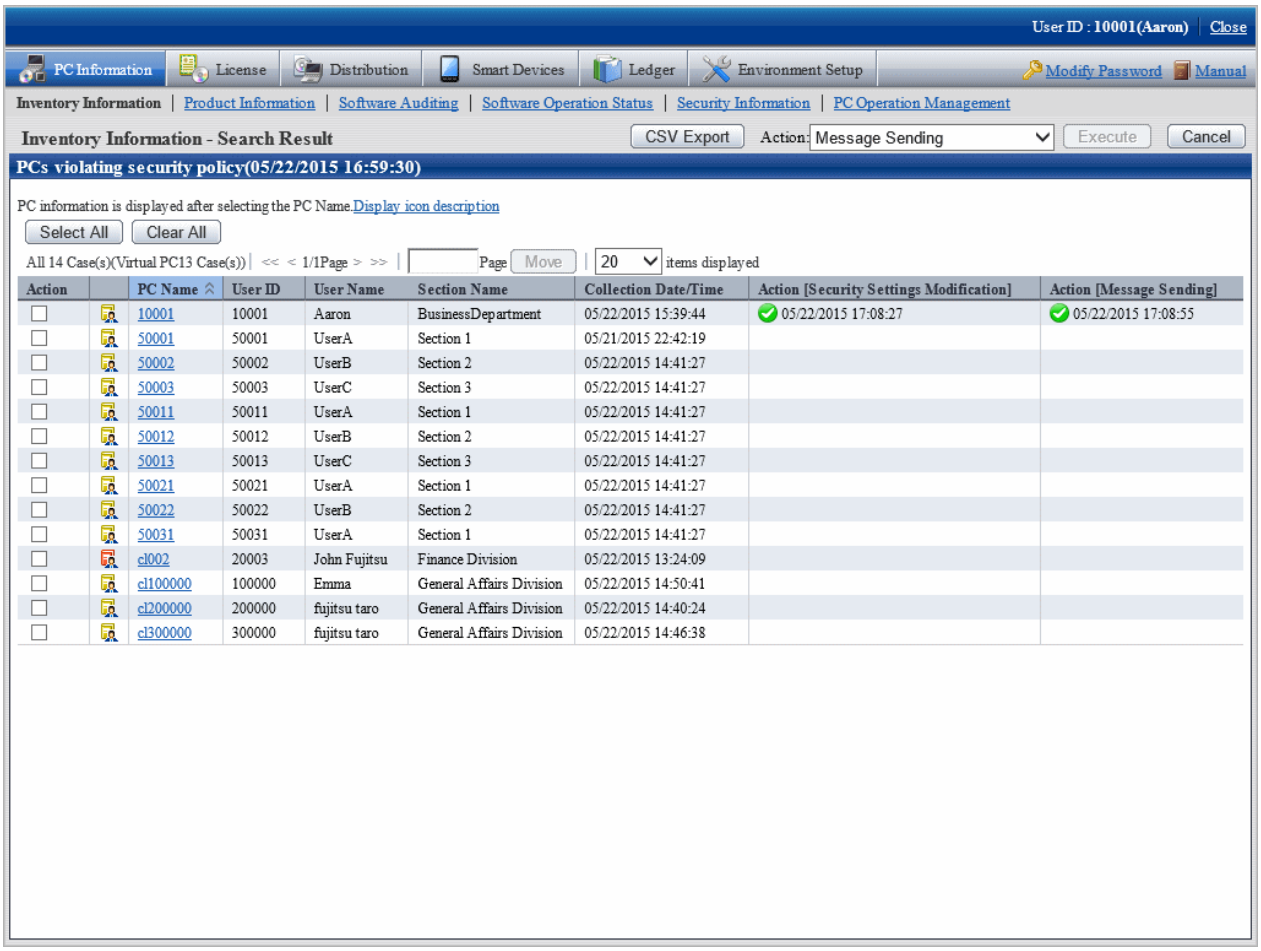
Click the link of corresponding number in the status window and only the PC corresponding to the aggregation item can be viewed as PC list.

This window is displayed in a window other than the status window.

Note

Display the PC corresponding to aggregation item based on the inventory information of displayed time point.

Therefore, it may be different from the number of corresponding PC displayed in the status window.



The item of this window is displayed according to the item set in **Inventory Information** > **Displayed Item Settings**.

By clicking the **Cancel** button, you can return to the initial window of inventory information.

Operation action

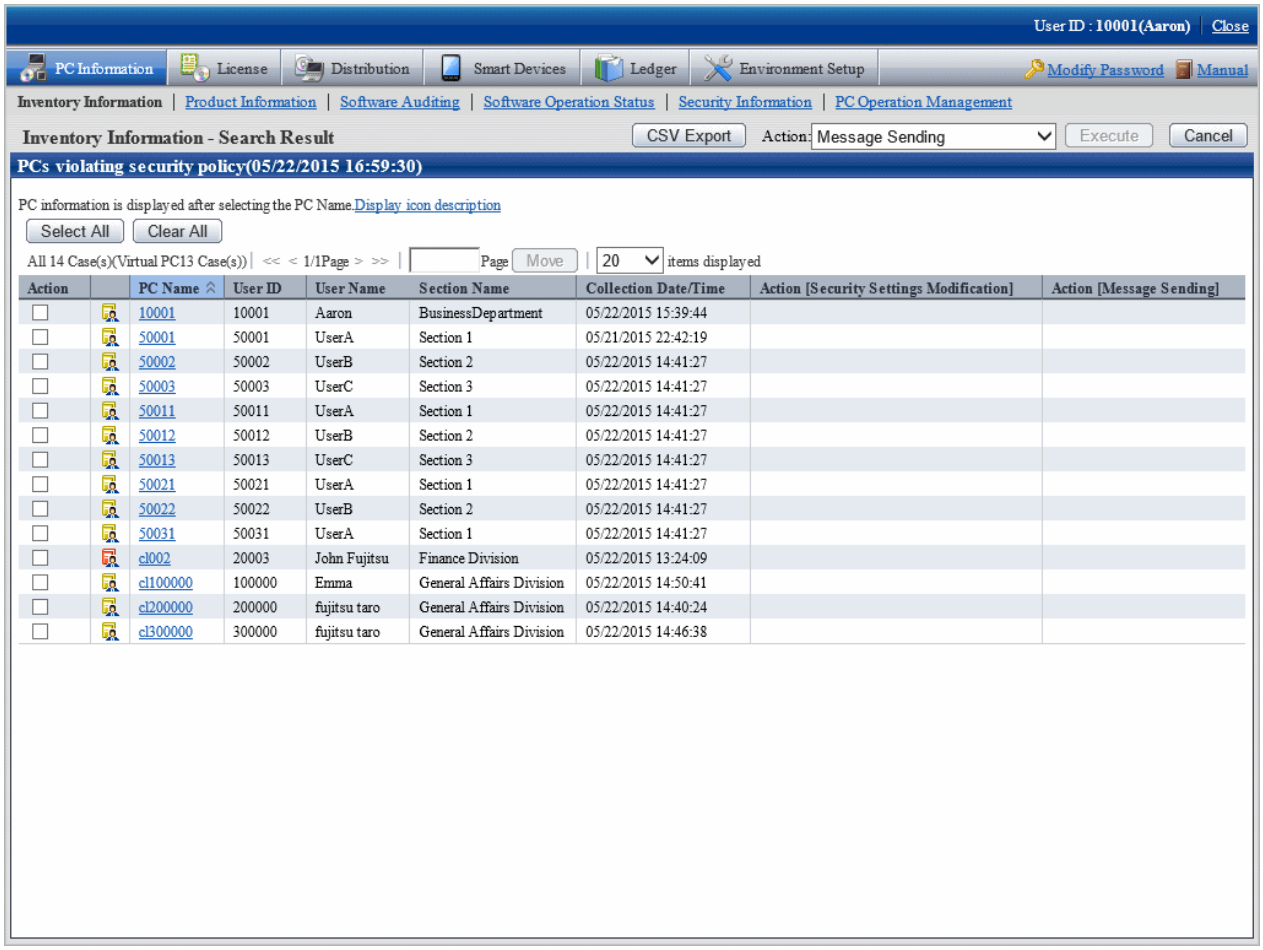
Note

The information after operation action will be reflected at next time of inventory collection. The display of status window is not instant, which will be reflected at the next aggregation timing.

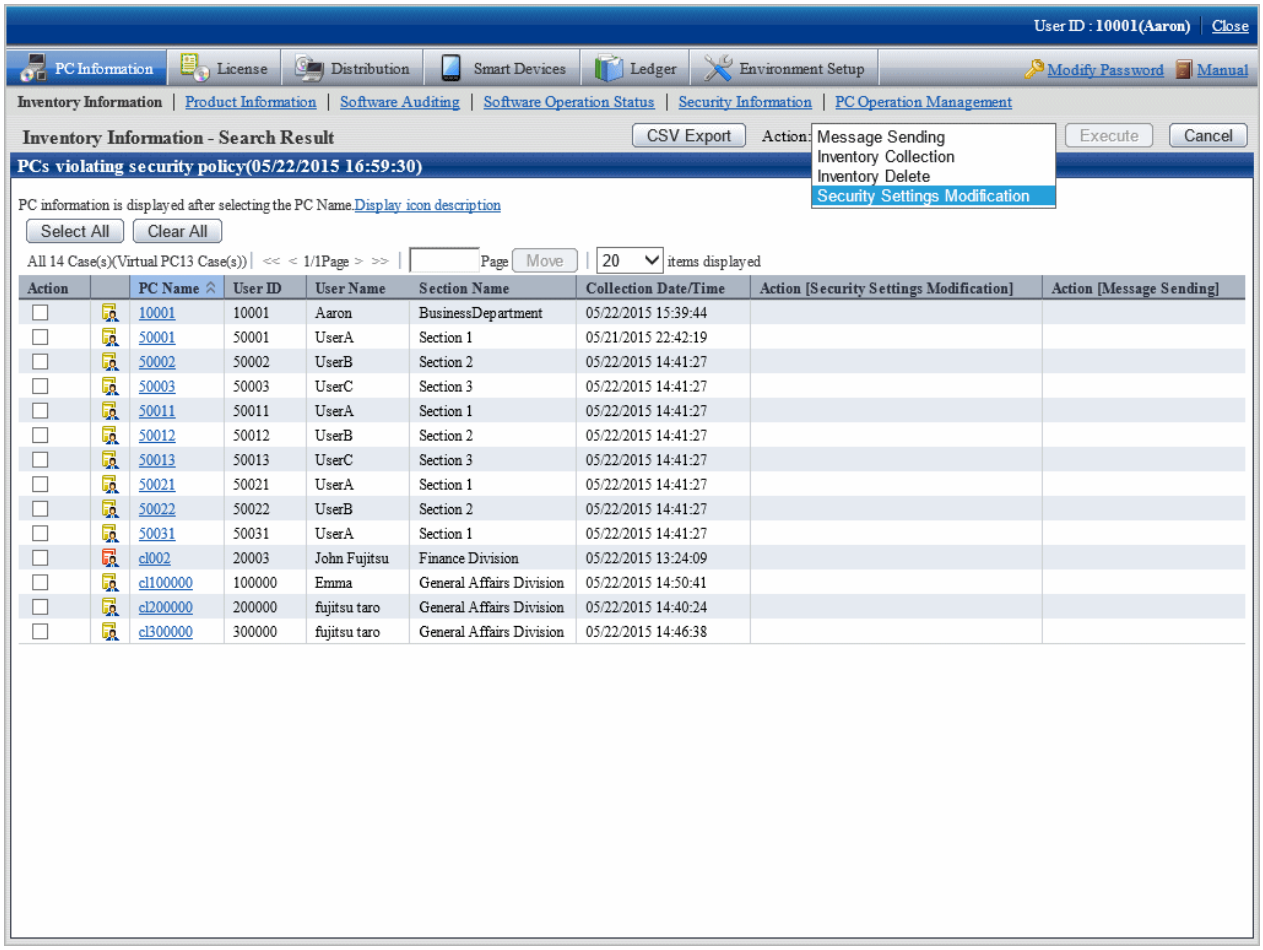
Check the corresponding PCs and perform operation action as needed.

The procedure when performing processing in this window is as follows.

1. Select the PC to be processed.

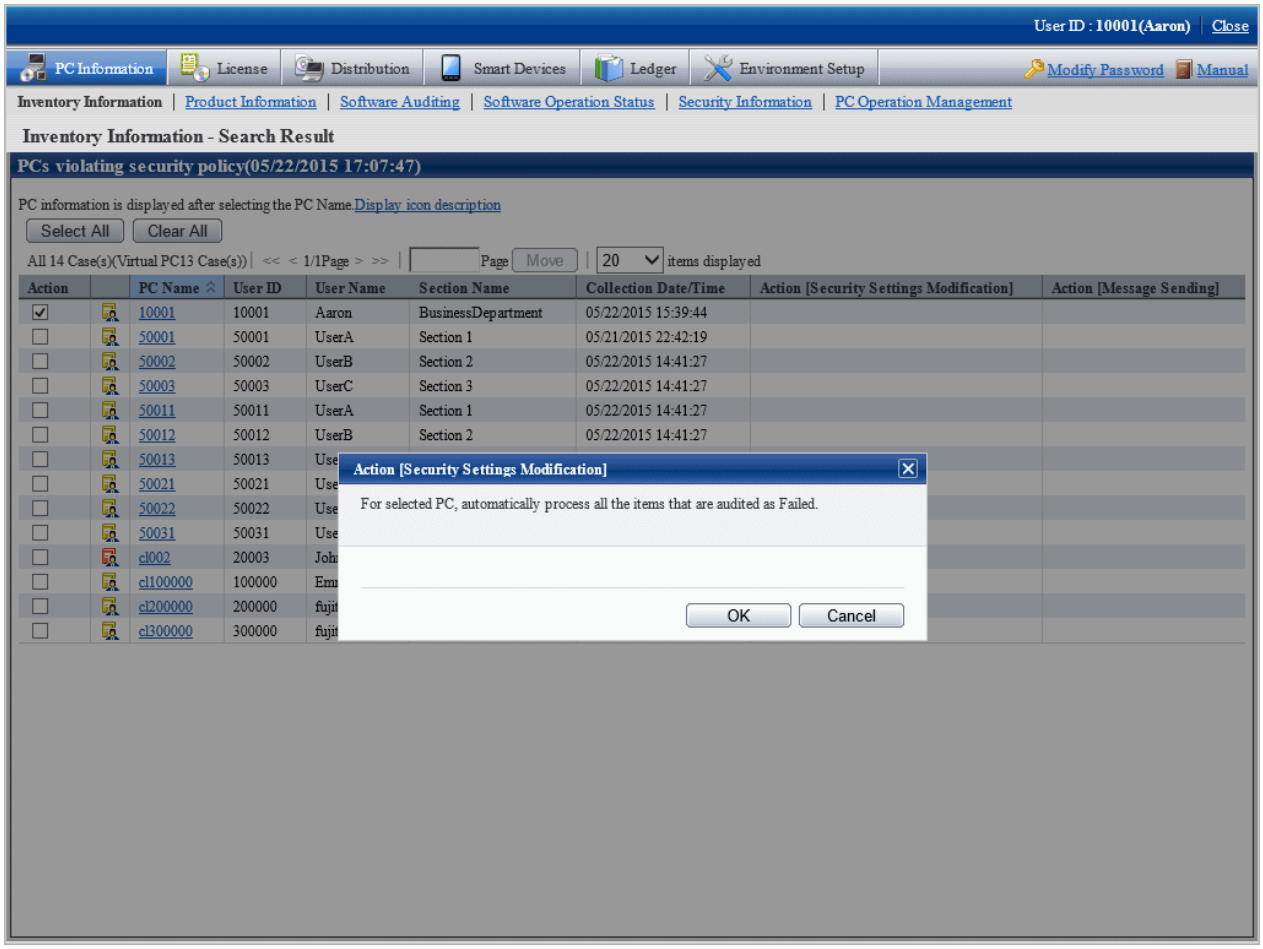


2. Select the content to be processed from the pull-down menu of **Action**, and click the **Execute** button.



3. After the window for confirming the processing content is displayed, check the content and click the **OK** button.

   The PC selected in Item No. 1 will be processed.

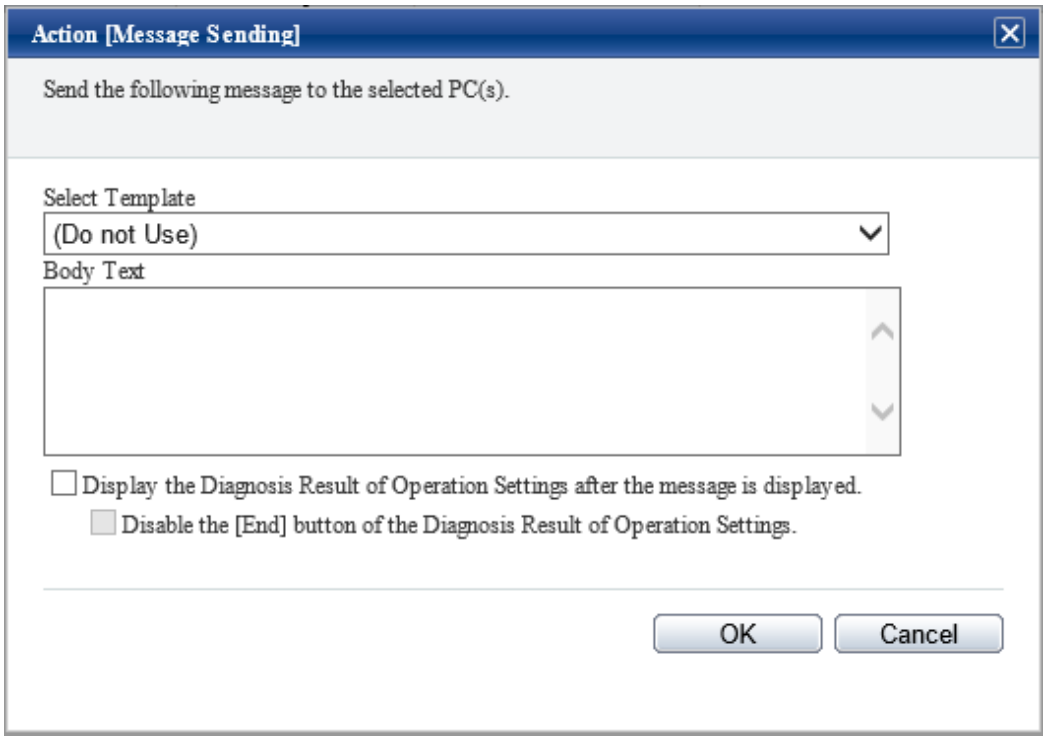


About the content of selection item of Action

The following describes the content of selection item of **Action**.

Message Sending

The following processing content will be displayed.



- **Select Template**

  Select the appropriate template from the templates prepared again. You can also create content again based on the content of selected template.
  For the settings of template, refer to "Template using for Action Message Sending Confirmation Session".

- **Body text**

  Specify the message body when displaying a message using up to 1024 fullwidth or 2048 halfwidth characters.

- **Display the Diagnosis Result of Operation Settings after the message is displayed**

  After this check box is selected, **Disable the [End] button of the Diagnosis Result of Operation Settings** can be selected.

  In addition, the **Diagnosis** button of the message window displayed in CT will be enabled. Click the **Diagnose** button, the diagnosis result window of operation settings will be displayed.

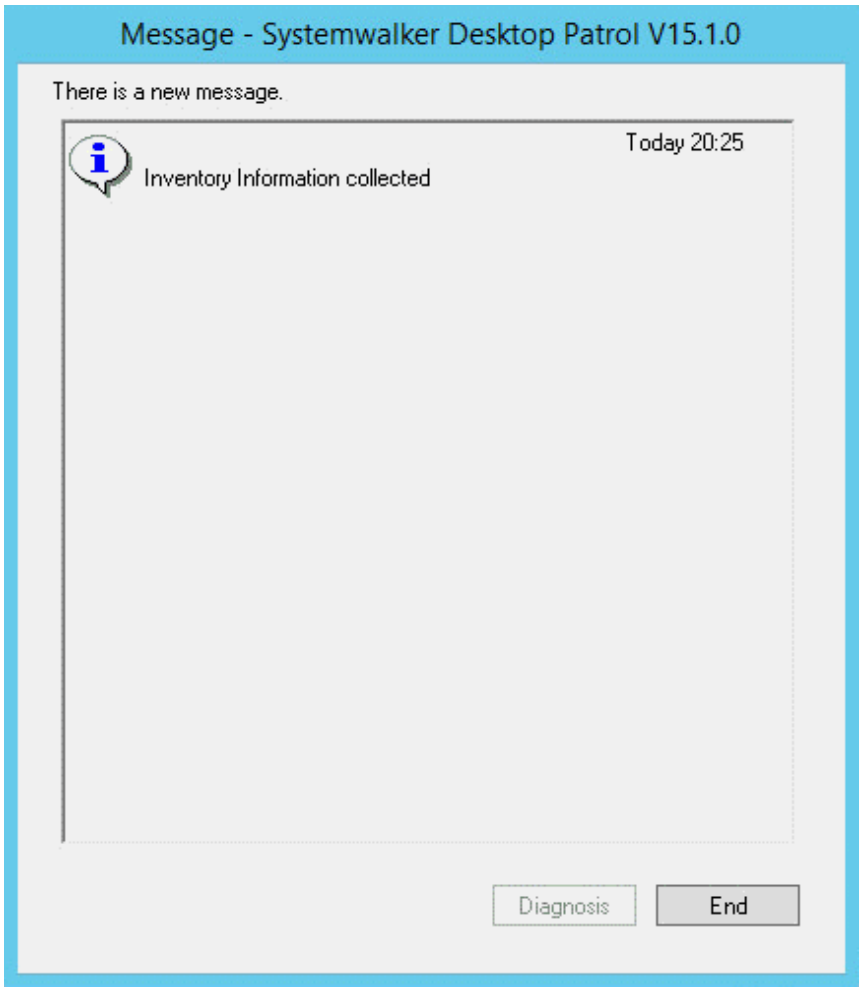
- **OK** button

  After it is clicked, message can be sent to the selected PC.

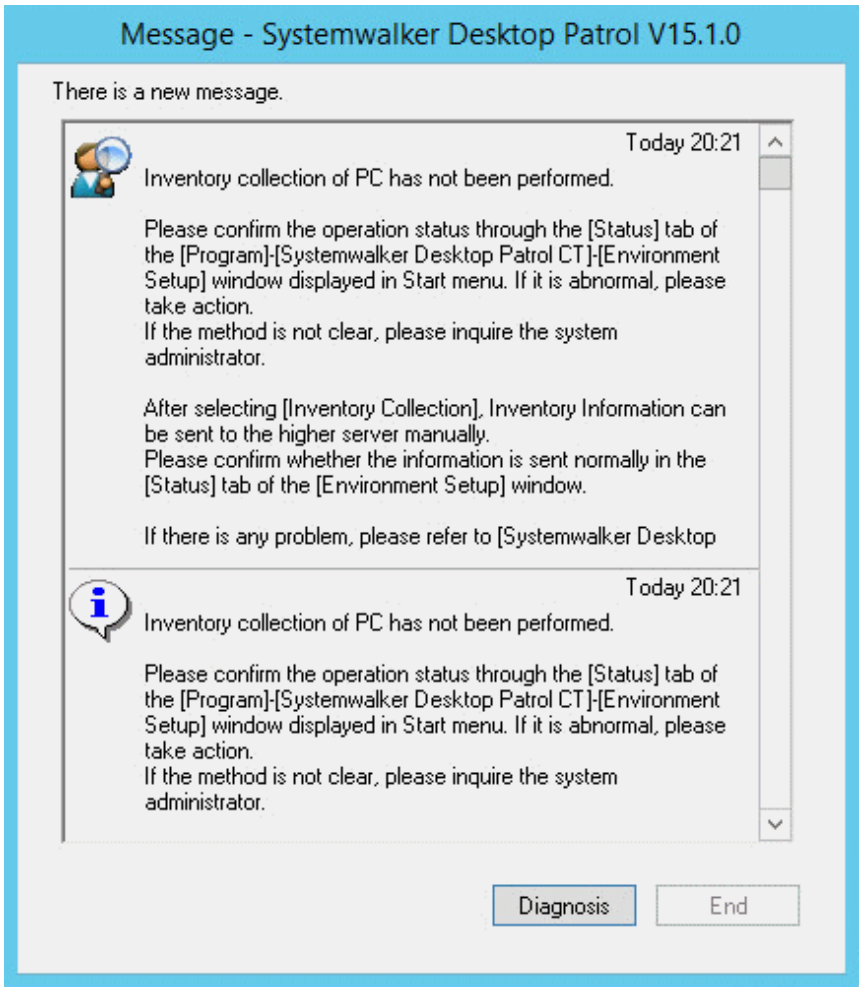
Note

Even if the body text is modified, it will not be reflected to the template. In addition, the body text of last time will be displayed at next time of processing.

After the message has been sent, the following message will be displayed on CT.



When the CT receives multiple messages at a time, it will be displayed as follows in CT.



- After the message of **Display the Diagnosis Result of Operation Settings after the message is displayed** is selected

  The **Diagnosis** button will be enabled, and the **Exit** button will be disabled.
  At this time, after the **Diagnosis** button is clicked, the diagnosis result window of operation settings will be displayed and the **End** button will be enabled.

  The CT in which the message is displayed is the Ct with one of the following policy settings only.

  - Select **Policy Groups**> **Power Saving Policy** > **Display Diagnosis Result Window of Operation Settings**.
  - Select **Policy Groups**> **Security Policy** > **Display Diagnosis Result Window of Operation Settings**.

  CT with these policy settings is the CT on which the diagnosis result window of operation settings can be started from selecting **Start** > **All Programs** > **Systemwalker Desktop Patrol CT**, or **Apps** > **Systemwalker Desktop Patrol CT**.

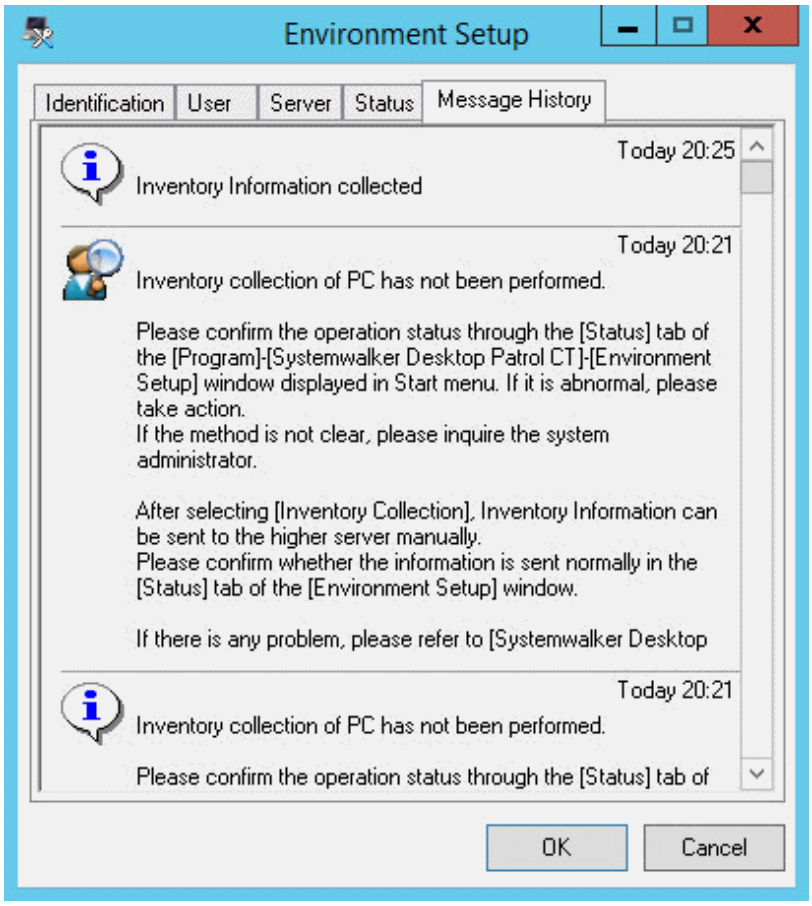
  On the CT of the policy setting without any of the above item being selected, the diagnosis result window of operation settings cannot be displayed, and message cannot be displayed.

- When **Disable the [End] button of the Diagnosis Result of Operation Settings** is selected

  The exit button of the diagnosis result window of operation settings will be disabled and cannot be clicked.
  After all processing has been done for the part that requires processing, the **End** button will be enabled and processing can be finished.

In addition, after selecting the range, the message can be copied. Even if information such as URL and contact address of administrator is contained in the message, it can be paste to another application through copy and paste.

The information received by CT in the past can be confirmed as follows in environment setup. For details, refer to "Message Sending and Message History" of *Systemwalker Desktop Patrol Operation Guide: for Clients*.

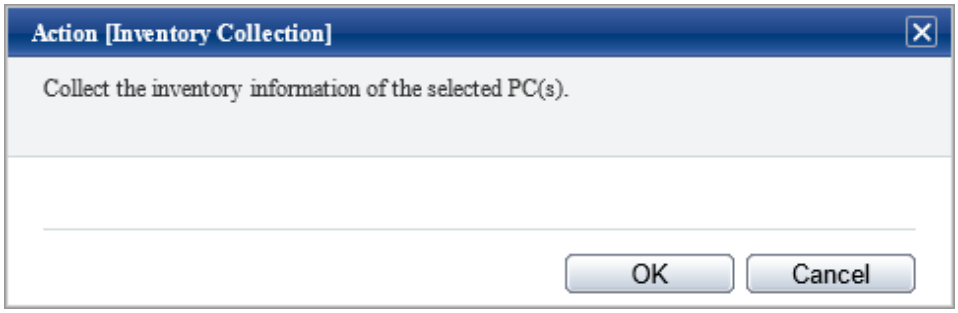


The number of items displayed is the latest 20 items.

The date displayed is the date when system administrator sends the processing instruction on the server.

Inventory Collection

The following processing content will be displayed.

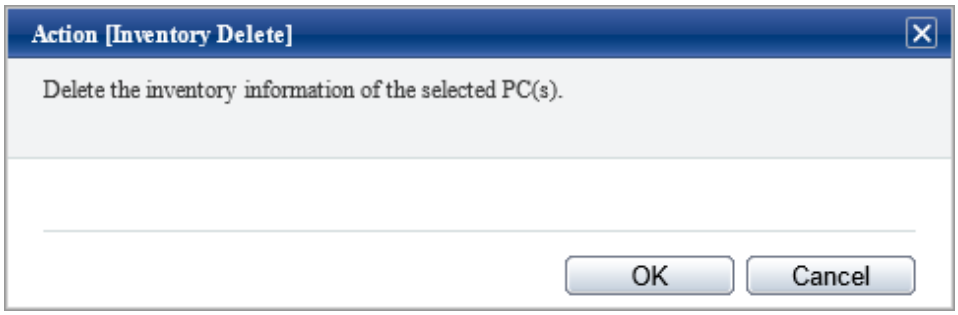


Click the **OK** button to collect the inventory information of the selected PC.

Nothing will be displayed on CT and inventory information will be collected automatically.

Inventory Delete

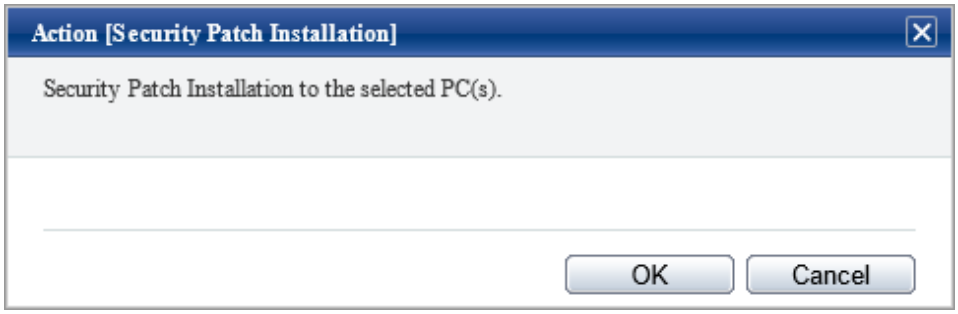
The following processing content will be displayed.



Click the **OK** button to delete the inventory information of the selected PC.

Security Patch Installation

The following processing content will be displayed.



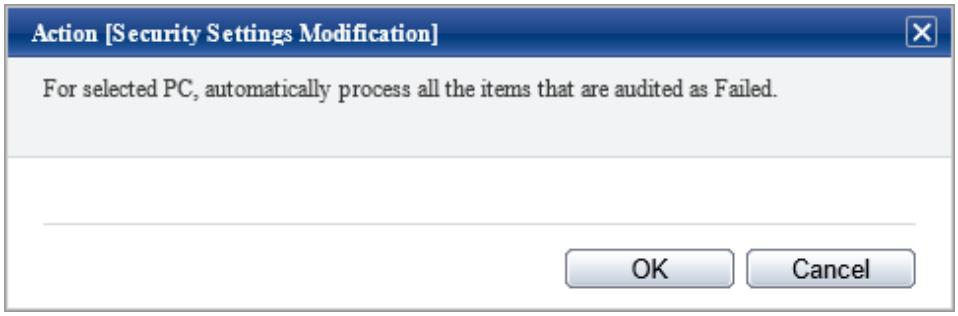
Click the **OK** button, and security patches can be installed to the selected PC.

Nothing will be displayed on CT and security patches will be installed automatically.

Do not restart or perform inventory collection after patch installation. Inventory collection will run according to schedule.

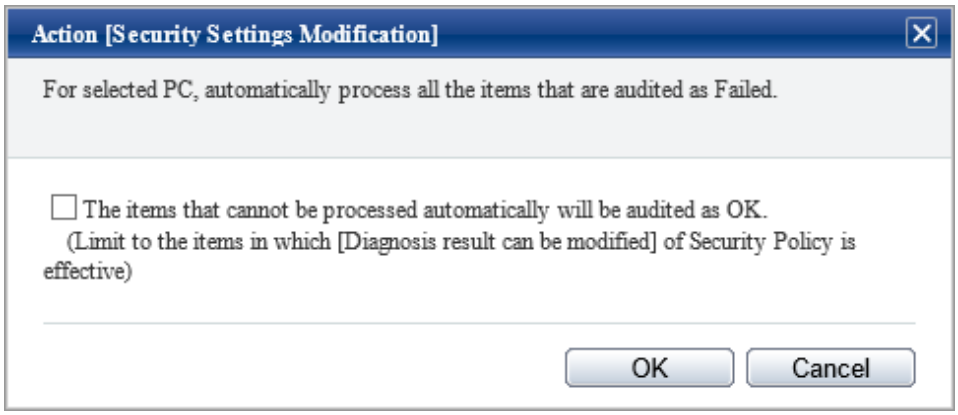
Security Settings Modification

The following processing content will be displayed.



Regardless of the aggregation item **PCs violating security policy** or **Aggregate by item** in display of details, all items that are audited as failed will be processed. The range that can be processed is limited to the items that allow auto-processing.

However, in **Option** > **Settings of Status** > **Action [Security Settings Modification], when "Display the setting of "Set the items that do not allow auto-processing to be audited as OK** is selected, the following window will be displayed.

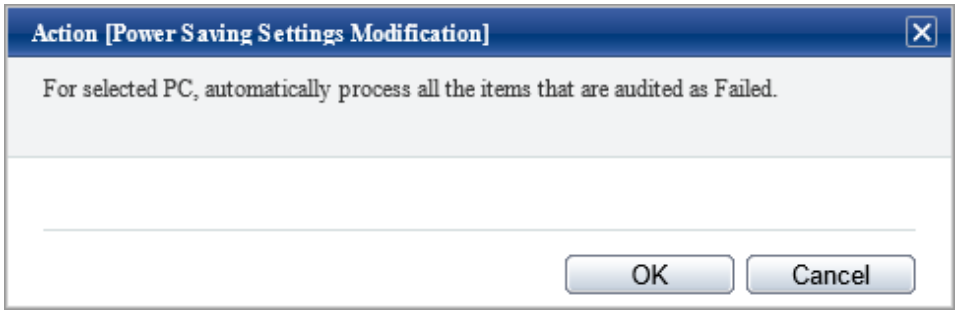


When processing the items that do not allow auto-processing, it is required to set **Set the diagnosis result to be correctable** in the policy settings again and then select **Correct the diagnosis result to "Auditing OK" for the items that can be corrected** in the above processing dialog.
For information on how to set **Set the diagnosis result to be correctable**, refer to the item descriptions of the **Auditing Settings of System Security** tab and the **Auditing Settings of User Security** tab of the **Policy Groups - Security Policy** window of "4.2.2.1 Set the Auditing Items of Security Settings".

The following processing will be performed on CT.
Nothing will be displayed on the window, the items of security settings that has been set as **Audit** in policy settings will be processed.
If the **Correct the diagnosis result to "Auditing OK" for the items that can be corrected** check box is not selected, correct the items set in **Set the diagnosis result to be correctable** in the policy settings.

Power Saving Settings Modification

The following processing content will be displayed.

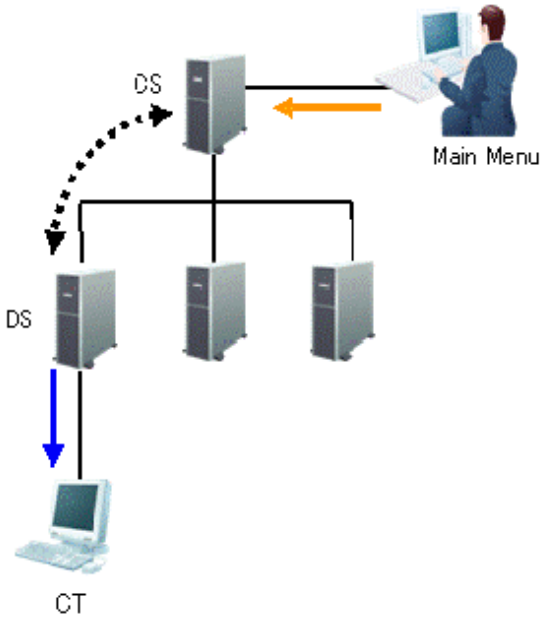


Regardless of the aggregation item **PCs violating power saving policy** or **Aggregate by item** in display of details, all items that are audited as failed will be processed.

The following processing will be performed on CT.
Nothing will be displayed on the window, the items of power saving settings that has been set as **Audit** in policy settings will be processed.

Timing when information flows

When **Message Sending**, **Inventory Collection**, **Security Patch Installation**, **Security Settings Modification** and **Power Saving Settings Modification** in the selection items of **Processing** are selected, information will flow to CT according to the following timing.



The information required in **Processing** and the timing when the information flows (initial value) is shown in the following table.

Line Type	Action	Opportunity of Action
←	Settings of processing	Any time Execute the processing from the main menu
◄····►	Synchronization of processing	Confirm in an interval of 5 minutes Setting can be performed in the **Environment Setup** > **Settings and Operation Status of CS/DS - Settings of DS** window of the main menu
←	Execution of processing	Confirm in an interval of 10 minutes Setting can be performed through the CustomPolicy.exe command

Confirm the processing result

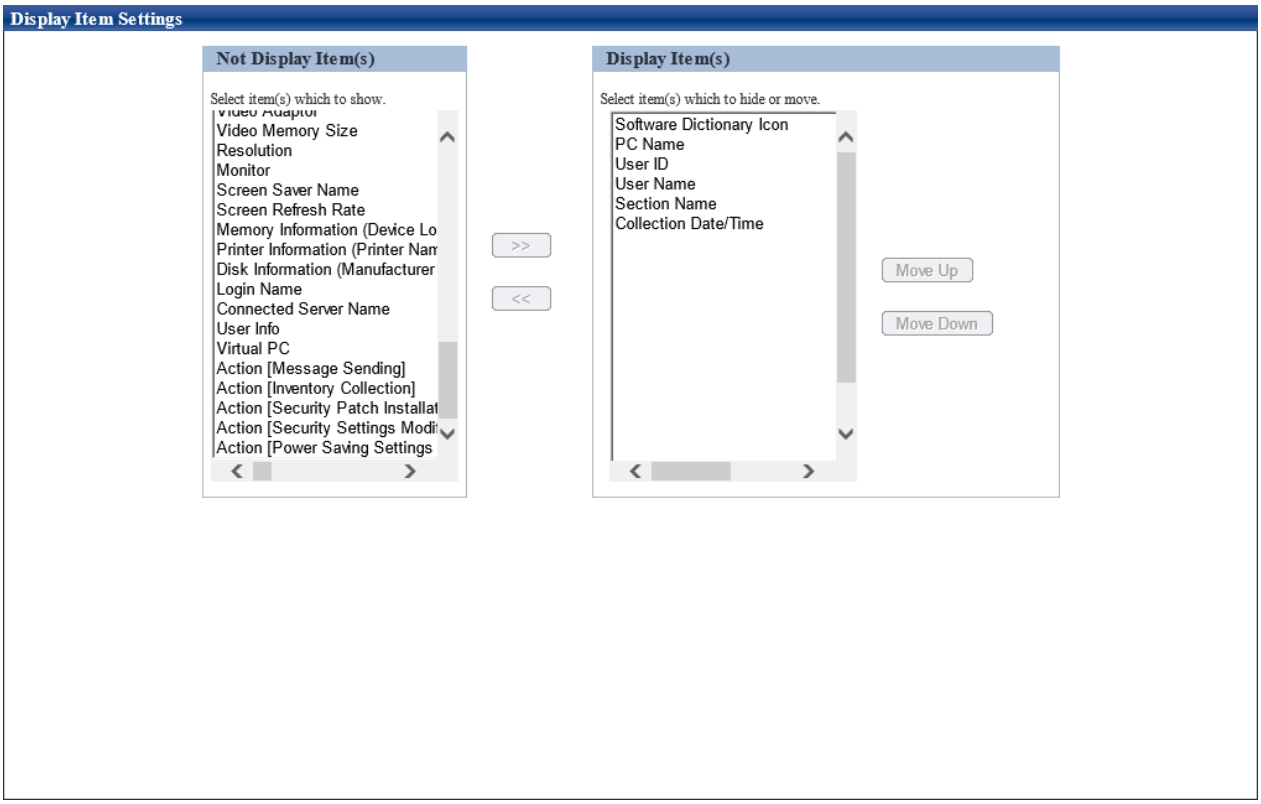
The processing result can be confirmed in the window for viewing PCs corresponding to aggregation item (PC list).

Displayed Item

The processing result can be confirmed in processing unit.

In the displayed window, select the processing content to be displayed as a list in **Displayed Item Settings**.

For information on how to set **Displayed Item Settings**, refer to "How to modify the items displayed in the PC list".

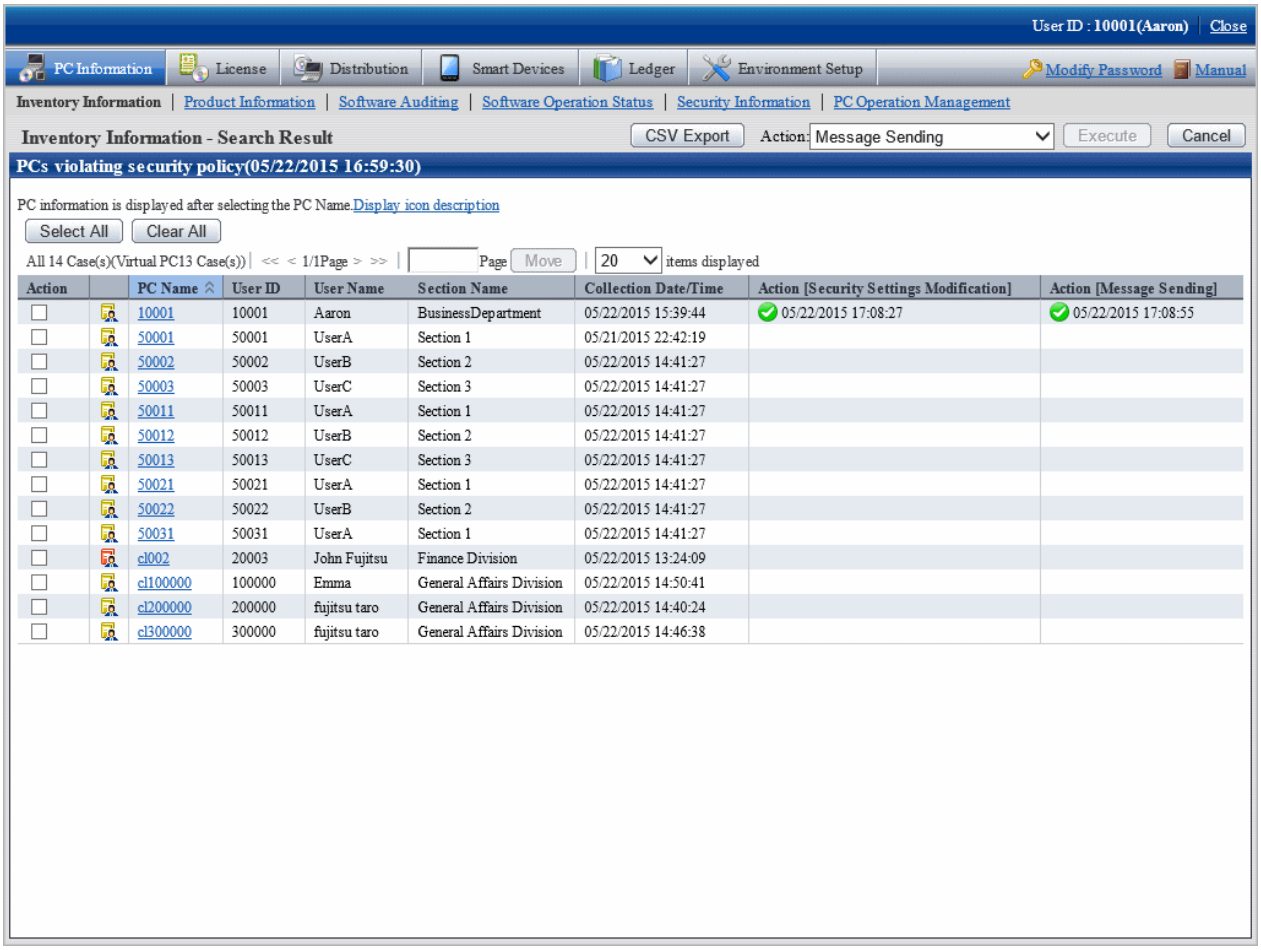


The following items are contained in processing. Modify the item to be displayed from hidden item to displayed item.

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

The time of processing last time and result of processing can be known through the items displayed in the window.

Therefore, even if processing has been done at last time in aggregation result, it is still easy to process the PC that has been detected again.



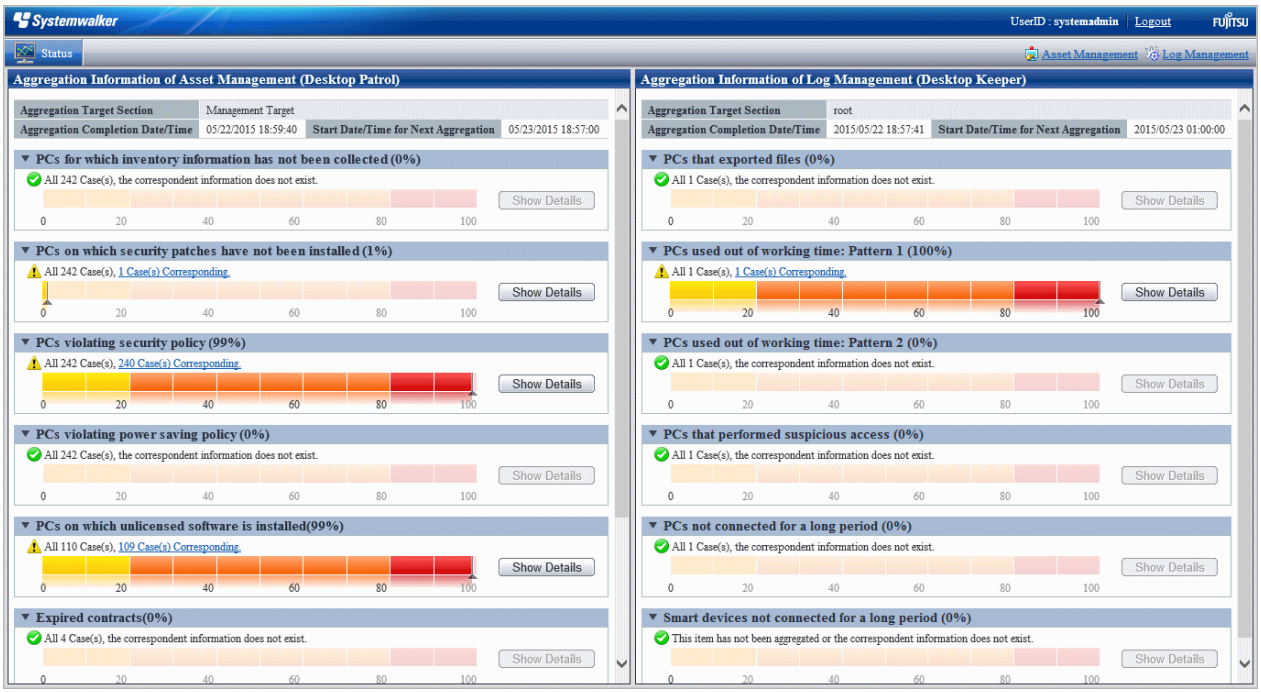
The content of items displayed as the result of processing result is as follows.

Item	Content	
Status	The status of processing is displayed by the following icons.	
		Processing has finished normally.
		Process has been failed.
		Unable to instruct a processing.
		Processing is being instructed.
Time of processing instruction	Display the time when processing is instructed.	
Error content	When warning or exception occurs, output the error content.	

3.2.11.5 View Status of Systemwalker Desktop Keeper

When Systemwalker Desktop Keeper has been installed, the asset management information of Systemwalker Desktop Patrol and log management information of Systemwalker Desktop Keeper will be displayed in the status window.

The status window when Systemwalker Desktop Keeper is installed is shown below.



Click the link of **Log Management** of Global Navigation, or lick the link of each aggregation items displayed in the aggregation information of Log Management (Desktop Keeper), the window of Systemwalker Desktop Keeper can be displayed in another window.

No matter whether relevant specification exists in **URL of Desktop Keeper** of **Environment Setup** > **Option** > **Settings of Status**, consider the following causes when the aggregation information of Log Management (Desktop Keeper) is not displayed.

- The URL specified in **URL of Desktop Keeper** of **Environment Setup** > **Option** > **Settings of Status** is incorrect

  Specify a correct URL.

- Even if the URL specified in **URL of Desktop Keeper** is correct, it cannot be accessed in the environment that uses browser

  Check the setting of browser. If there is no problem in the setting of proxy server .etc, register the site (URL) of Desktop Keeper to **Site** of the zone of **Local Intranet** or **Trusted Site**.

- The user ID or password used for login is not set for Systemwalker Desktop Keeper

  Set the user ID and password of Systemwalker Desktop Keeper.

- The user ID or password used for login is incorrect

  Check the user ID and password registered in Systemwalker Desktop Keeper.

In addition, click **Log Management** of the Global Navigation, the above events will be output as message.

Note

At the time when displaying the status of Systemwalker Desktop Keeper or the window of Log Management, warning dialogs relating to security protection of Internet Explorer may be displayed sometimes, select to display even without protected items.

Automatic authentication of login ID (SSO)

On each product of Systemwalker Desktop Patrol and Systemwalker Desktop Keeper, management of user ID and password is required. When the user ID and password managed in each product are consistent, the status of each product can be displayed.

In addition, the login ID on Systemwalker Desktop Patrol is case-sensitive, but not on Systemwalker Desktop Keeper.

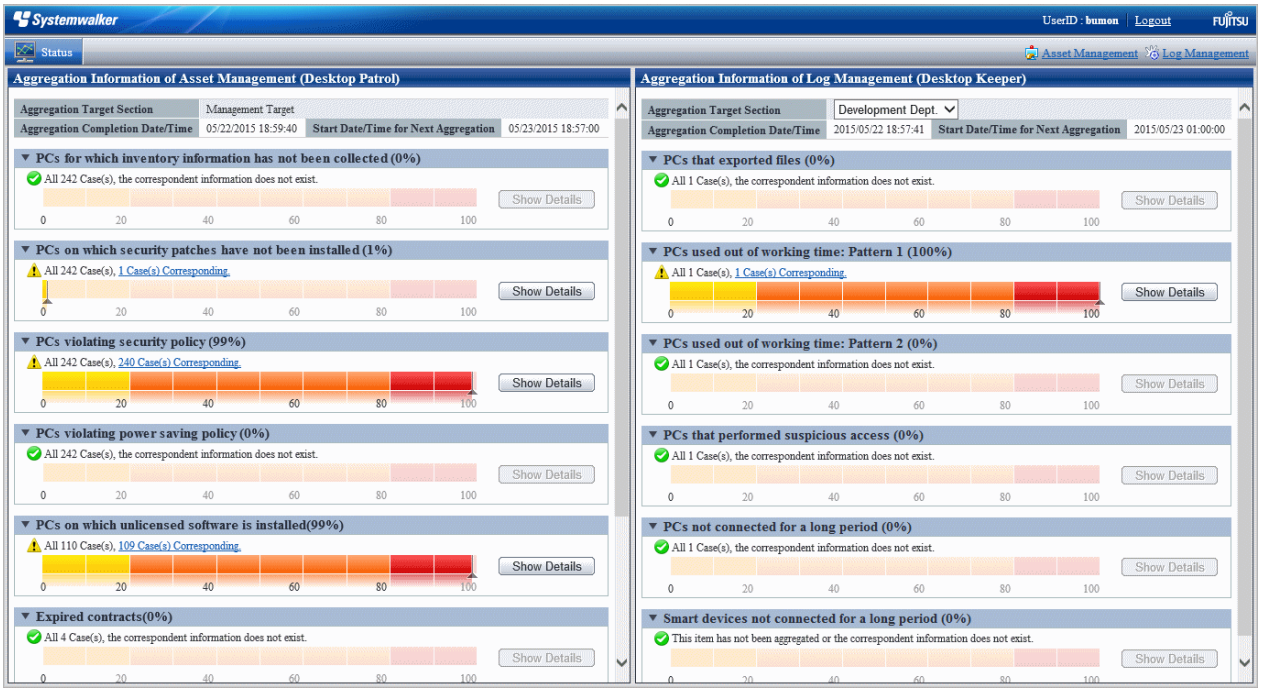
When logging in from Systemwalker Desktop Keeper, log in with the user ID of Systemwalker Desktop Patrol intentionally (case-sensitive). When the uppercase and lowercase are incorrect, the status of Systemwalker Desktop Patrol will not be displayed.

When the authorities of login ID on Systemwalker Desktop Patrol and Systemwalker Desktop Keeper are different

When performing the management of user ID and password in each product of Systemwalker Desktop Patrol and Systemwalker Desktop Keeper, different authority may be set for different products by mistake sometimes.

At this time, information will be displayed according to different authorities.

Example) When it is system administrator on Systemwalker Desktop Patrol, and section administrator on Systemwalker Desktop Keeper



However, when the authority at Systemwalker Desktop Patrol side is "General User", the status window will not be displayed, and only the informant of product logged in will be displayed.

No	Login Side	Automatic Authentication Side	Displayed Content
1	"General User" of Systemwalker Desktop Patrol	Same IDs exist in Systemwalker Desktop Keeper	Only the information of Systemwalker Desktop Patrol will be displayed
2	Systemwalker Desktop Keeper	The same IDs exist as "General User" of Systemwalker Desktop Patrol	Only the information of Systemwalker Desktop Keeper will be displayed

3.2.12 Check the Operation Status of CT

This section describes how to confirm whether the CT run according to the policy set in the main menu.

The operation status on CS or CT can be confirmed.

When using in the following timing, the operation status of CT can be confirmed.

- When operation is started or modified

  During the installation of Systemwalker Desktop Patrol or when settings are modified, use it to confirm whether the policy set in the main menu is correct or not.

  For example, use in the following timing.

  - When Systemwalker Desktop Patrol is installed for the first time
  - When version update of Systemwalker Desktop Patrol is performed
  - When the structure of system is modified
  - When the setting of policy is modified
- When trouble occurs

  Use it when trouble occurs on CT or to confirm whether trouble has occurred.
  - Security patch is not installed
  - Inventory information is not notified to server (CS/DS)
  - The software reserved for distribution is not distributed

3.2.12.1 Check the Operation Status of CT on CT

When checking the operation status on CT, use one of the following methods.

- Execute the logcheck.exe (check CT operation status) command
- Start from the logget.exe (log collection tool) command

Execute the logcheck.exe (check CT operation status) command

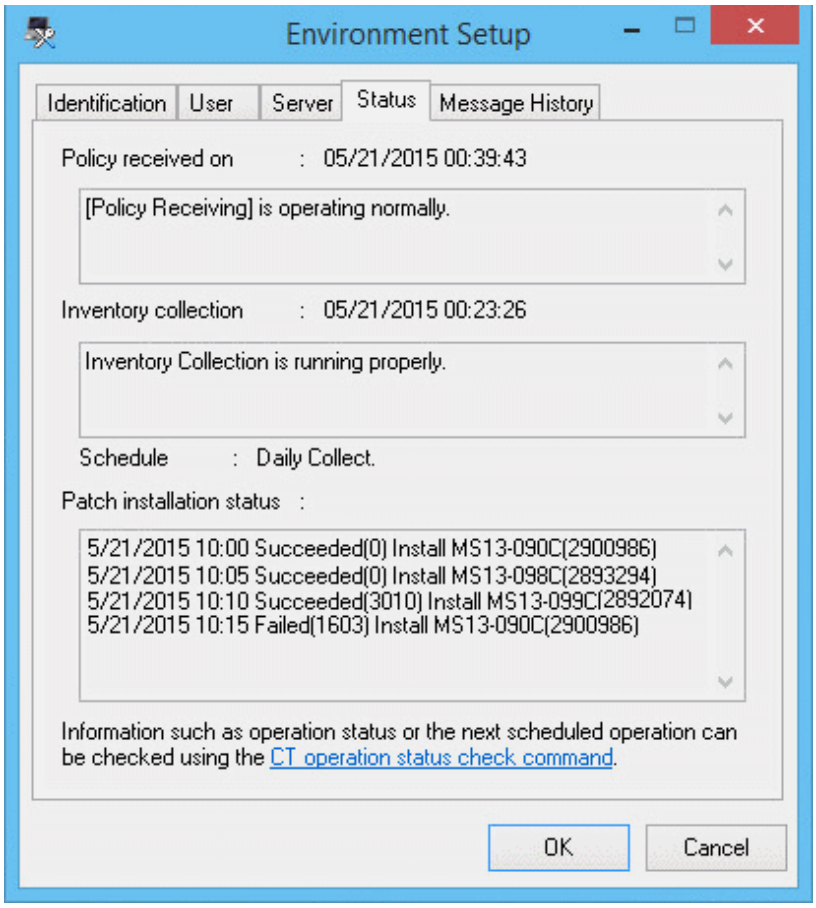
1. Execute the following command.

Installation directory of CT\FJSVsbtrsc\bin\logcheck.exe

   For details of the logcheck.exe (check CT operation status) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

   Point

   logcheck.exe (check CT operating status on CS) can also be executed by clicking the link in **CT operation status check command** in the **Status** tab in the **Environment Setup** window.


Environment Setup
Identification
User
Server
Status
Message History
Policy received on : 05/21/2015 00:39:43
[Policy Receiving] is operating normally.
Inventory collection : 05/21/2015 00:23:26
Inventory Collection is running properly.
Schedule : Daily Collect.
Patch installation status :
5/21/2015 10:00 Succeeded(0) Install MS13-090C(2900986)
5/21/2015 10:05 Succeeded(0) Install MS13-098C(2893294)
5/21/2015 10:10 Succeeded(3010) Install MS13-099C(2892074)
5/21/2015 10:15 Failed(1603) Install MS13-090C(2900986)
Information such as operation status or the next scheduled operation can be checked using the CT operation status check command.
OK
Cancel

2. Start Web browser, the operation status of CT will be displayed.

```
------------------------------------------------------------------------
 Basic Information
------------------------------------------------------------------------
PC Name
        000000
User ID
        000000
Connection server
        cs.example.com
CTID
        1234567890+1234567890ABCDEF1234567890ABCDEF
Version
        V15.1.0-SN1551

------------------------------------------------------------------------
 at the next time of operation
------------------------------------------------------------------------
Policy Receiving and Update Application Reservation
         5/20/2015 18:54
Inventory Collection Reservation
         5/21/2015 0:00 -  5/22/2015 0:00
Diagnosis result display reservation of operation settings
        nothing
Time to access system standby
        nothing

------------------------------------------------------------------------
 at the last time of operation
------------------------------------------------------------------------
Policy Receiving Time
         5/20/2015 18:24
Policy Receiving Result
        Succeeded
Inventory Collection Time
         5/20/2015 15:24
Inventory Collection Result
        Succeeded

------------------------------------------------------------------------
 Settings status of policy
------------------------------------------------------------------------
Confirm the interval of policy
        180min
Specify Inventory Collection Date
        Everyday
Specify the time frame for Inventory collection
        Do not
Automatical Installation of Security Patches
        Apply Regularly at Logon
Download target software automatically
        Download at Windows Logon
Group Name
        Policy-GRP1
Software Dictionary Update Time
         5/20/2015 15:13

------------------------------------------------------------------------
```

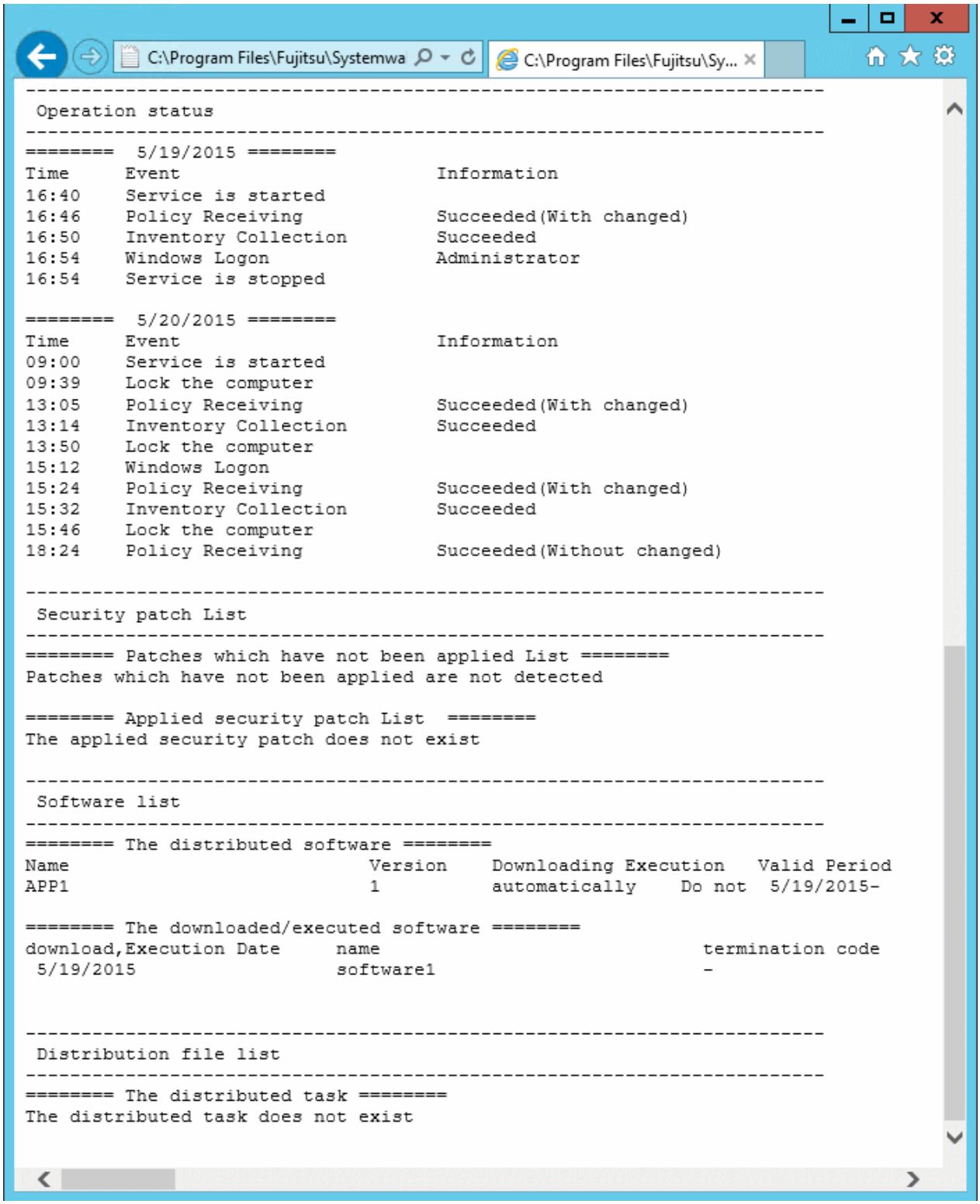


Table 3.9 [Displayed Items can be Confirmed in the Window]

Category	Item	Description	Displayed Content	
			logcheck	logcheckcs
Basic Information	**Collection Time**	Display the time when inventory is collected.		Y
	PC Name	Display the value set in environment setup.	Y	Y
	User ID		Y	Y

Category	Item	Description	Displayed Content	
			logcheck	logcheckcs
	Collection Server		Y	Y
	CTID	Display CTID. This information is the value obtained in internal processing at CT installation.	Y	Y
	Version	Display the version of CT. Example: V14.1.0-R1.0-SN950 Example: Version prior to V12	Y	Y
at the next time of operation	**Policy Receiving and Update Application Reservation**	Display the time of next policy receiving or updater application.	Y	
	Inventory Collection Reservation	Display the time to perform next inventory collection.	Y	
	Diagnosis result display reservation of operation settings	Display the time when the diagnosis result of operation setting is displayed next time.	Y	
	Time to access system standby	Display the time when shifting to system standby next time.	Y	
at the last time of operation	**Policy Receiving Time**	Display the time when policy has been received last time.	Y	
	Policy Receiving Result	Display the result after last policy receiving.	Y	
	Inventory Collection Time	Display the time when inventory collection is performed last time.	Y	
	Inventory Collection Result	Display the result after last inventory collection.	Y	
Settings status of policy	**Confirm the Interval of Policy**	Display the policy information set in **Environment Setup** > **Policy Groups** in the main menu.	Y	Y
	Specify Inventory Collection Date			
	Specify the time frame of Inventory collection			
	Automatical Installation of Security Patches			
	Downloaded target software automatically			
	Group Name			
	Software Dictionary Update Time			
Operation status	**-**	CS: Display the latest operation status of CT of the last two days. CT: Display the latest operation status of CT of the last 7 days.	Y	Y

Category	Item	Description	Displayed Content	
			logcheck	logcheckcs
		(display the part of date number of the date when PC was started) In case of CS, through specifying operation, all operation status kept in CS can be displayed. For displayed item, refer to Table 3.10 [Displayed Item of Operation Status] of the following table		
Security patch List	**Patches which have not been applied List**	Display the list of security patches to be installed to the target CT.	Y	Y
	Applied security patch List	Display the list of security patches that have been installed to the target CT.	Y	
Software list	**The distributed software**	Display the list of software that has been distributed to the target CT.	Y	Y
	The downloaded/ executed software	Display the list of software that has been downloaded and executed in the target CT.	Y	
Distribution file list	**The distributed task**	Display the list of distribution result of distribution task of file distribution.	Y	Y

Y: content will be displayed.

Table 3.10 [Displayed Item of Operation Status]

Item	Details	Description
Shift to System Standby	-	Shifted to standby.
Restore from System Standby	-	Restored from standby.
Windows Logon	<Logon Account of Windows>	user has logged on.
Windows Logoff	<Logon Account of Windows>	user has logged off.
Switch of Users	<Logon Account of Windows>	user has been switched.
Lock of Computer	-	It has been locked.
Connect to Network	-	It is connected to network and communication is enabled.
Cut off Network	-	The network is cut off and communication is disabled.
Start Service	-	ITBudgetMGR(INV) service has been started.
Stop Service	-	ITBudgetMGR(INV) has been stopped.
Policy Receiving	Successful (with change) Successful (without change) Failed (<Error Code> <Description>) Example)	Policy has been received.

Item	Details	Description
	Failed (10051 Unable to connect to the connection server)	
Inventory Collection	Successful Failed (<Error Code> <Description>) Example) Failed (10051 Unable to connect to the connection server)	Inventory has been collected.
Patch Installation	Successful (<Name>, End Code(<n>)) Failed (<Name>, End Code(<n>), <Description>) Example 1) Successful (Install MS09-048 Critical(967723) to WindowsVista/SP1/SP2, End Code(0)) Example 2) Failed (Install MS09-048 Critical(967723) to WindowsVista/SP1/SP2, End Code(-3), Fatal error occurred during installation.)	Patch has been installed. For details of end code of patch, refer to the *Systemwalker Desktop Patrol Reference Manual*.
Software Download	<Name> ver.<n> has been downloaded Failed to download <Name> ver.<n> (<Error Code><Description>) <Name> ver.<n> has been executed, End Code<m> Example 1) Information sending tool ver.2 has been downloaded Example 2) Failed to download information sending tool ver.2 (10051 Unable to connect to the connection server) Example 3) Failed to execute information sending tool ver.2 Failed (-13 authority pretending failed) Example 4) Information sending tool ver.2 has been executed, End Code 0	Software has been downloaded.
Restart Automatically	After patch has been installed, restart has been performed automatically After patch installation, restart has been performed according to user operation.	After patch installation, restart has been performed. This item is displayed when performing patch installation in Systemwalker Desktop Patrol and restart is selected. In usual operation of Windows, it is not displayed when restart is performed.
Start Updater Application	Before application (V15.1-SN2010) and after application (V15.1-SN2035)	Start applying the updater.

Point

Location for saving the files displayed in the window (when executed on CT)

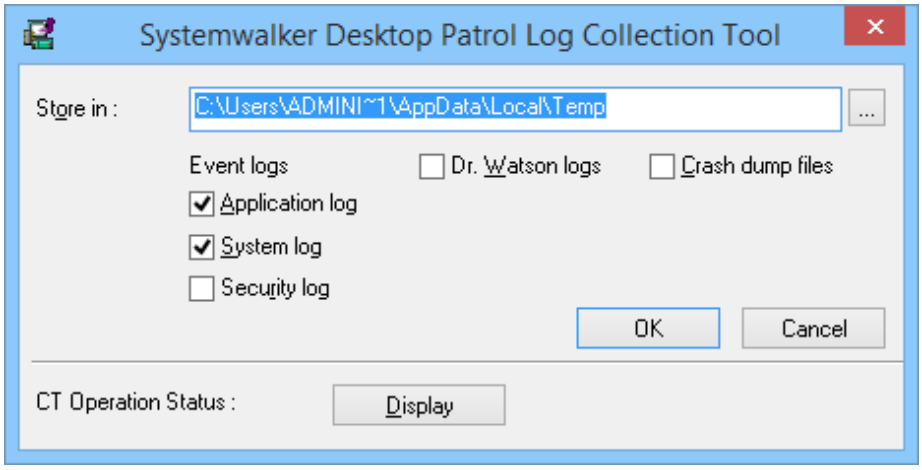
- Folder: Installation Directory of CT\FJSVsbtrsc\data\status

  File: ctstatus.txt (*)

  *: File is output in UTF-8 format.

Start from the logget.exe (log collection tool) command

1. Execute the logget.exe (log collection tool) command, and the **Systemwalker Desktop Patrol Log Collection Tool** dialog will be displayed.



   Click the **Display** button in this dialog.

   For the logget.exe(log collection tool) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

2. Start Web browser, and the operation status of CT will be displayed.

   The displayed window and items are the same as "Execute the logcheck.exe (check CT operation status) command".

3.2.12.2 Check the Operation Status of CT on CS

When checking the operation status of CT on CS, perform through executing the logcheckcs.exe.

For details of logcheckcs.exe (Check the Operation Status of CT on CS), refer to *Systemwalker Desktop Patrol Reference Manual*.

1. Log on to Windows with the user that belongs to the Administrators group.
2. Execute the command operation for the CT to be confirmed. There are following methods to specify the option
   - The method that specifies part of the string of user ID, PC name, connection server as the search condition (partial match)
   - The method that specifies the user ID, PC name, connection server (complete match)

The method that specifies part of the string of user ID, PC name, connection server as the search condition

1. Start the following command.

```
Installation Directory of CS\FJSVsbtrs\bin\logcheckcs.exe <Search string>
```

   For example, when searching the CT that contains "yama", start the following command.

```
Installation Directory of CS\FJSVsbtrs\bin\logcheckcs.exe yama
```

2. The CT whose user ID and PC name and connection server matches with the entered search string in a list.

   When only one target CT exists in the searched result, Web browser will be started after the list has been displayed and the operation status of CT will be displayed.

```
No User ID PC Name Connection Server
------------------------------------------------------------------
1 YamadaTaro tokyo02 ds1.example.com
2 YamamotoHanako tokyo03 ds1.example.com
3 SatoJiro toyama01 ds2.example.com
Please enter the number (end with q):
```

3. Enter the No. of CT to be confirmed, and Web browser will be started and the operation status of CT will be displayed.

   For the displayed window and displayed item, refer to the item marked as "Y" in the "logcheckcs" column of **Displayed Content** of **Displayed Items that can be Confirmed in the Window** recorded in "Execute the logcheck.exe (check CT operation status) command".

The method that specifies the user ID, PC name, connection server

1. When it is difficult to narrow down the CT by string search, and the user ID, PC name and connection server are unknown, execute the following command to specify CT.

```
Installation Directory of CSFJSVsbtrsbinlogcheckcs.exe [-u User ID] [-p PC Name] [-s Connection Server]
```

   Example 1) When user ID is "User", PC name is "PC" and connection server is "ds.example.com", start the following command.

```
Installation Directory of CSFJSVsbtrsbinlogcheckcs.exe -u User -p PC -s ds.example.com
```

   Example 2) When PC name and connection server are omitted, start the following command.

```
Installation Directory of CS\FJSVsbtrs\bin\logcheckcs.exe -u User
```

2. When the CT whose user ID, PC name and connection server are matched with the specified option exists, it will be displayed in the list.

   When there is only 1 CT in the searched result, Web browser will be started after the list has been displayed, and the CT operations status will be displayed.

```
No User ID PC Name Connection Server
------------------------------------------------------------------
1 User PC1 ds.example.com
2 User PC2 ds.example.com
Please enter the number (end with q):
```

3. Enter the No. of CT to be confirmed, and Web browser will be started and the operation status of CT will be displayed.

   For the displayed window and displayed item, refer to the item marked as "Y" in the "logcheckcs" column of **Displayed Content** of **Displayed Items that can be Confirmed in the Window** recorded in "Execute the logcheck.exe (check CT operation status) command".

About displayed information

For displayed message, even if CT is uninstalled, the information before CT uninstallation will be kept on CS. Therefore, when Ct is installed again and the user ID, PC name and connection server that are same as before is set, the information displayed CS is still the information before uninstallation.

Point

About display of operation status

- When there is no particular specification, the operation status of the latest two days will be displayed. However, through specifying the "-a" option, all operation status kept in CS will be displayed.

  Installation Directory of CS\FJSVsbtrs\bin\logcheckcs.exe [-a] <Search string>

  Installation Directory of CS\FJSVsbtrs\bin\logcheckcs.exe [-a] [-u User ID] [-p PC Name] [-s Connection Server]

- Under the environment in which the CT operation status log is not collected, "Operation Status" will not be displayed. By using the CTPolicy.exe (client environment setup) command, collection function of CT operation status log can be enabled/disabled.

Location for saving the files displayed in window (when executed on CS)

- Folder: Installation Directory of CS\FJSVsbtrs\data\ctstatus
- File: <User ID>+<PC Name>+<Connection Server>.txt (*)

  (*) File is output in UTF-8 format.

3.2.13 Checking the Operational Status of CS/DS

This section explains how to check the operational status of the distribution server feature and inventory collection feature of CS/DS.

The operational status of CS/DS can be checked:

- When the operation is started or when it is changed

  Use this feature to check if the policy set on CS during changing the system configuration changes or operation policy settings are distributed as intended when the administrator builds CS or DS for the first time.

  For example, use when:

  - CS or DS is installed for the first time
  - CS or DS version upgrade is performed
  - System configuration is changed
  - Policy settings (such as policy group settings, auditing software settings) are changed

- When a problem occurs

  Use this feature to check when/if a problem has occurred on CS/DS, for example:

  - The installed DS is not displayed in **Environment Setup** > **CS/DS Settings and Status** window.
  - Link for CS or DS is displayed in **Environment Setup** > **CS/DS Settings and Status** window.
  - Icon indicating that CS or DS is not operating is displayed in **Environment Setup** > **CS/DS Settings and Status** window.
  - Software, security patches, updater, or files are not distributed to CT under specific CS or DS.
  - Inventory for CT under specific CS or DS is not updated.

Executing logchecksv.exe (CS/DS operation status check)

Execute the following command:

cs/dsInstallDir\FJSVsbtrs\bin\logchecksv.exe

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on this command.

Table 3.11 [Items that can be checked on command prompt or in file]

Category	Item	Description	Type
Basic Information	**Server Type**	Basic information set in the environment setup window.	CS, DS
	CS/DS Name		CS, DS
	Host Name		CS, DS
	Higher Host Name		DS
	Host name resolution	Whether names can be resolved using the host name or upstream host name. If successful, the IP address will be displayed.	CS, DS
	Upstream host name resolution		DS
	Windows host name	Windows information. If not successful, then it will not be displayed.	CS, DS
	Windows IPv4 address		CS, DS
	Windows IPv6 address		CS, DS
	Version information	Version information for CS/DS. Example: V15.1.0-R1.1-SN1501	CS, DS
Communication setting	**Connection interval with the support center**	Content of the communication settings set in the **Settings of CS** window, **Settings of DS** window, or set using CustomPolicy.exe.	CS
	Connection interval with upstream CS/DS		DS
	Time frame for communicating with the support center		CS
	Time frame for receiving the distributed software		DS
	The maximum number of concurrent connections from a downstream DS or CT		CS, DS
	Polling Interval		CS, DS
Policy information	**Datetime of software dictionary creation**	Datetime when the software dictionary on CS/DS was created.	CS, DS
	Datetime of software dictionary update	Datetime when the software dictionary on CS/DS was updated.	CS, DS
	Datetime of CS setting update	Datetime when the **Settings of CS** window was updated.	CS
	Datetime of DS setting update	Datetime when the **Settings of DS** window was updated.	DS
	Datetime of policy group update	Update datetime and error information for each policy group.	CS, DS
	Datetime of unapplied patch detection information update	Datetime of unapplied patch detection information update and error.	CS, DS
	Datetime of next unapplied patch detection operation	Next scheduled operation time for the unapplied patch detection schedule.	CS
	Datetime of next connection to upstream servers	Next communication time for communication with an upstream server.	CS, DS

Category	Item	Description	Type
Distribution server feature status	**Distribution server feature status**	Status of the distribution server feature.	CS, DS
	Heap memory size of distribution server (MB)		CS, DS
	nsufficient memory status		CS, DS
	Datetime of overflow of maximum concurrent connections from a downstream DS or CT		CS, DS
	Status of connection to upstream servers		CS, DS
Inventory collection server feature status	**Inventory collection server feature status**	Status of the inventory collection server feature.	CS, DS
	Heap memory size of inventory collection server (MB)		CS, DS
	Insufficient memory status		CS, DS
	Datetime of overflow of maximum concurrent connections from a downstream DS or CT		CS, DS
Software or file distribution status	**Software distributed successfully to CS**	Number of software distributed successfully. Example: 15	CS
	Updaters distributed successfully to CS	Number of updaters distributed successfully. Example: 5	CS
	Security patches distributed successfully to CS	Number of software distributed successfully. Example: 300	CS
	Files distributed successfully to CS	Number of software distributed successfully. Example: 10	CS
	Software distributed successfully to DS	Number of software distributed successfully. Example: 15	DS
	Updaters distributed successfully to DS	Number of updater distributed successfully. Example: 5	DS
	Security patches distributed successfully to DS	Number of software distributed successfully. Example: 300	DS
	Files distributed successfully to DS	Number of software distributed successfully. Example: 10	DS
	Software or file being prepared for distribution	Number of software or file being prepared for distribution. Example: 10	DS
	Distribution error information	Information about error during software or file distribution. Example: Insufficient available capacity in software directory	DS

Category	Item	Description	Type
	Software directory path name	Name of the software directory path.	CS, DS
	Software directory size (set value/usage amount/ available capacity)	Information about the software directory. Example: 300MB/150.015MB/1010.938MB	CS, DS
	Software directory path name for extension	Name of the software directory path for extension.	CS, DS
	Software directory size for extension (set value/ usage amount/available capacity)	Information about the software directory for extension. Example: No setting/150.343MB/55023.023MB	CS, DS
	Installation path	Name of the installation directory path to compare with the software directory.	CS, DS

Table 3.12 Content displayed in Distribution server feature status and Inventory collection server feature status

Item	Details	Description
Server feature status	**Running (Start datetime: 2014/09/18 10:10:30)**	The server feature is running. The datetime indicates the start time for the server feature.
	Restarting	Automatic restart is being performed.
	Not running (Services are not running)	Server feature has been stopped due to the services stopped.
	Not running (Port number 2922 being used)	Sever feature has been stopped due to the port number 2922 being used by another application.
	Not running (Port number 2856 being used)	Sever feature has been stopped due to the port number 2856 being used by another application.
	Not running (Other errors)	Sever feature has been stopped due other errors.
Insufficient memory status	**None**	Memory insufficiency has not occurred.
	2014/09/17 15:15:40	Datetime when memory insufficiency occurred. Displays the datetime of the 5 most recent occurrences.
Datetime of overflow of maximum concurrent connections from a downstream DS or CT	**None**	Overflow of maximum concurrent connections has not occurred.
	2014/09/17 17:30:15	Datetime when overflow of maximum concurrent connections occurred. Displays the datetime of the 5 most recent occurrences.
Status of connection to upstream servers	**Completed**	Connection to the upstream server has completed successfully.
	None	Connection to the upstream server has not been performed.
	Connecting	Connection to the upstream server is being performed.

Display example for command prompt

```
------------------------------------------------------------
Basic Information
------------------------------------------------------------
Server Type: DS
CS/DS Name: dsServer1
```

```
Host Name: ds1.exmaple.com
Higher Host Name: cs.example.com
Host name resolution: Successful (192.0.2.0)
Upstream host name resolution: Successful (198.51.100.0)
Windows host name: ds1.example.com
Windows IPv4 address: 192.0.2.0
Windows IPv6 address: 2001:db8::%10
Version information: V15.0.0-R1.0-SN1400

------------------------------------------------------------
Communication setting
------------------------------------------------------------
Connection interval with upstream CS/DS: 5 minutes
Time frame for receiving the distributed software: 08:00 - 17:00
The maximum number of concurrent connections from a downstream DS or CT: 30
Polling Interval: 5 minutes

------------------------------------------------------------
Policy information
------------------------------------------------------------
Datetime of software dictionary creation at the support center: 2014/09/09 10:52:24
Datetime of software dictionary u
```
update
```
: 2014/09/09 10:52:34
Datetime of DS setting update: 2014/09/09 10:52:24
Datetime of unapplied patch detection information update: 2014/09/09 11:02:11
Datetime of next connection to upstream servers: 2014/09/09 11:02
========Policy Group========
Status   Group Name    Update Date/Time
OK   CS (2014/09/10 15:40)
OK   DS1 (2014/09/10 16:45)
OK   DS2 (2014/09/09 10:20)
Failed   policyGroup1 (2014/09/10 11:10)
OK   policyGroup2 (2014/09/10 11:10)
Error information: policyGroup2 (GrpPolicy.5) Failed to write to files

------------------------------------------------------------
Distribution server feature status
------------------------------------------------------------
Running Status: Running (Start datetime: 2014/09/18 15:20:25)
Heap memory size: 256MB
Insufficient memory status:
2014/09/15 13:20:45
2014/09/16 10:10:35
2014/09/16 13:34:10
2014/09/16 16:05:04
2014/09/17 09:30:25
Datetime of overflow of maximum concurrent connections from a downstream DS or CT: None
Status of connection to upstream servers: Completed

------------------------------------------------------------
Inventory collection server feature status
------------------------------------------------------------
Running Status: Running (Start datetime: 2014/09/18 15:22:10)
Heap memory size: 128MB
Insufficient memory status: None
Datetime of overflow of maximum concurrent connections from a downstream DS or CT:
2014/09/15 13:20:45
2014/09/16 10:10:35
2014/09/16 13:34:10
2014/09/16 16:05:04
2014/09/17 09:30:25

------------------------------------------------------------
Software or file distribution status
```

```
------------------------------------------------------------
Software distributed successfully to DS: 10
Updaters distributed successfully to DS: 3
Security patches distributed successfully to DS: 150
Files distributed successfully to DS: 20
Software or file being prepared for distribution to DS: 10
Distribution error information: Insufficient available capacity in software directory
Software dictionary: D:\DesktopPatrol\swc
Software directory size (set value/usage amount/available capacity): 300MB/150.015MB/1010.938MB
Software directory for extension: No setting
Software directory size for extension (set value/usage amount/available capacity): No setting/
150.343MB/55023.023MB
Installation path: C:\Program Files\Fujitsu\Systemwalker Desktop Patrol
```

3.2.14 Collect Simple Operation Log File

It describes how to collect the simple operation logfile of CT.

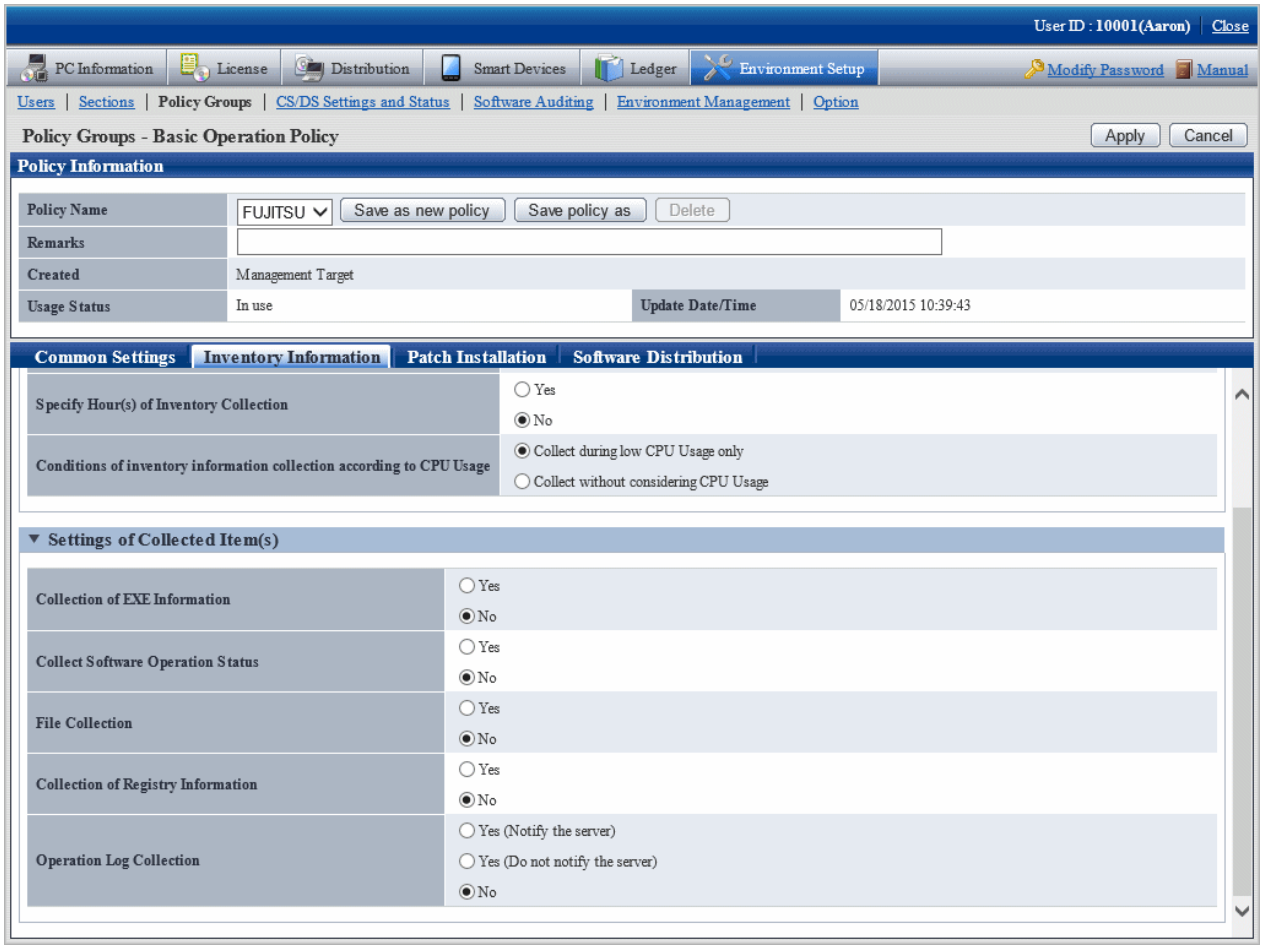
Note

It is required to use this function in agent mode CT.

This function cannot be used under command mode CT.

Modify settings of policy

1. After logging in to the main menu, modify the **Collect simple operation log** in **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** > **Inventory Information** and **Settings of Collected Item(s)** to one of the following.



Item	Description	
Operation Log Collection	Specify whether to collect the simple operation log of each PC.	
	Yes (Notify the server)	After selecting, simple operation log information will be recorded on CT, and its information will be notified to server at the time of inventory collection. When notifying to server, even if the required disk capacity of CS will be increased, collective management of logs can be achieved on CS.
	Yes (Do not notify the server)	After selecting, simple operation log information will be recorded on CT, but it will not be notified to server as inventory. Since it will be notify to server, the required capacity of CS will not be increased. However, when confirming the recorded log information, it is required to confirm on CT.
	No	After selecting, simple operation log information will not be collected When this item is selected, the simple operation log that has been saved on CS or CT will not be deleted. The initial value is **No**.

Note

When installing the current version of CS to the CS of V13.0.0 or earlier

The collection condition of simple operation log file will be set as the following.

- When the metering function is used on the old version (prior to V13.0.0):
  - Collection of Software Operation Status
  - **Yes**
  - Collection of simple operation log
    Yes (Notify the server) (when file collection is not performed for operation logs), or
    Yes (Do not notify the server) (when file collection is performed for operation logs)
  - File Collection
    The specified simple operation log file cannot be modified.
- When the metering function is not used on the old version (prior to V13.0.0):
  - Collection of Software Operation Status
    No
  - Collection of simple operation log
    No

When performing mixed operation with the CT prior to V13.0.0

After installation of the current version of CS when collecting the operation logs for the CT prior to V13.0.0, execute the following procedure.

1. Set **Collect Software Operation Status** to **Yes**.
2. Set to collect the following files in the file collection function. <DTPDIR> is macro definition, enter directly.
   - <DTPDIR>\invcl\inv\meter\opelog\UserOperation.00.wdt
   - <DTPDIR>\invcl\inv\meter\opelog\UserOperation.01.wdt
   - <DTPDIR>\invcl\inv\meter\opelog\UserOperation.02.wdt
   - <DTPDIR>\invcl\inv\meter\opelog\UserOperation.03.wdt

   For information on how to set the file collection function, refer to "3.1.1 Perform Operation Settings of Client".

2. Confirm the settings, click the **Apply** button, and modify policy.

   On CT, this function is enabled from the user logged on after the modified policy has been received.

View simple operation log file

The created simple operation log file is saved under the following directory of CT.

Installation Directory of CT\invcl\inv\meter\opelog

In addition, when notified to CS, it is saved under the Directory for saving collected file on CS.

When viewing, view the content directly under the directory.

The simple operation log file is saved for maximum 4 months. The meaning of each created file is as follows.

UserOperation.00.wdu: Simple operation log file of current month

UserOperation.01.wdu: Simple operation log file of last month

UserOperation.02.wdu: Simple operation log file of two months before

UserOperation.03.wdu: Simple operation log file of three month before

For the format of each file, refer to the *Systemwalker Desktop Patrol Reference Manual*.

Chapter 4 Audit/Control PC Operational Configuration

This chapter describes how to audit and control the operational configuration of PC (power saving settings, and security settings).

4.1 Operation Procedure

The operation procedure of auditing and controlling PC operational configuration (power saving settings and security settings) is as follows.

Overview of operation

The audit/control of PC operational configuration is performed according to the following flow.

1. Auditing Plan

   Perform the planning of power saving auditing and security auditing on the operation system.

2. Audit and Collect

   Collect the information of PC setting status (power saving settings and security settings).

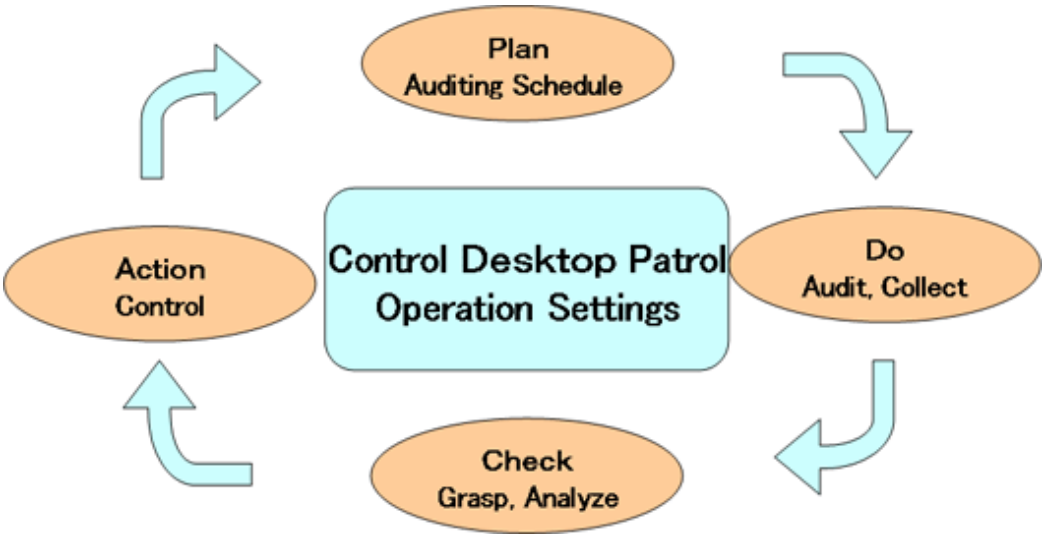
3. Know and Analyze

   Confirm and analyze the PC setting status (power saving settings and security settings).

4. Control

   For PC that requires analysis result and countermeasure, modify settings by force and execute operation guide.

The flow of auditing/controlling PC operational configuration is shown below.



Flow of operation

This section describes the flow of operation when auditing/controlling the PC operational configuration.

To confirm the current status of power saving and security settings of PC

Through installing Systemwalker Desktop Patrol and collecting information, the current power saving/security status can be known.

Set the item to be audited in policy and the set status can be confirmed through regularly check the status window or report result.

Note

When CT is running on virtual PC

When CT is judged to be running on a virtual PC, perform the following processing for power saving and security auditing.

- Power Saving auditing

  The virtual PC runs as the guest OS on virtual server, and it is not the status of physical PC. Therefore, since the setting value related to the power saving of PC (time to access standby) has no meaning, power saving audit will not be performed.
  In addition, the **Power Saving** tab of the Diagnosis result window of operation settings cannot be displayed.

- Security auditing

  The virtual PC runs as the guest OS on virtual server, so it is no need to set the BIOS/HDD password.

  Therefore, BIOS/HDD password will not be audited.

To merge the power saving and security settings of PC into corporate policy

Set the period of the following two stages and perform proper information collection and customization. Confirm the effects of control from knowing the current status to the power saving and security settings.

1. Audit/Control period

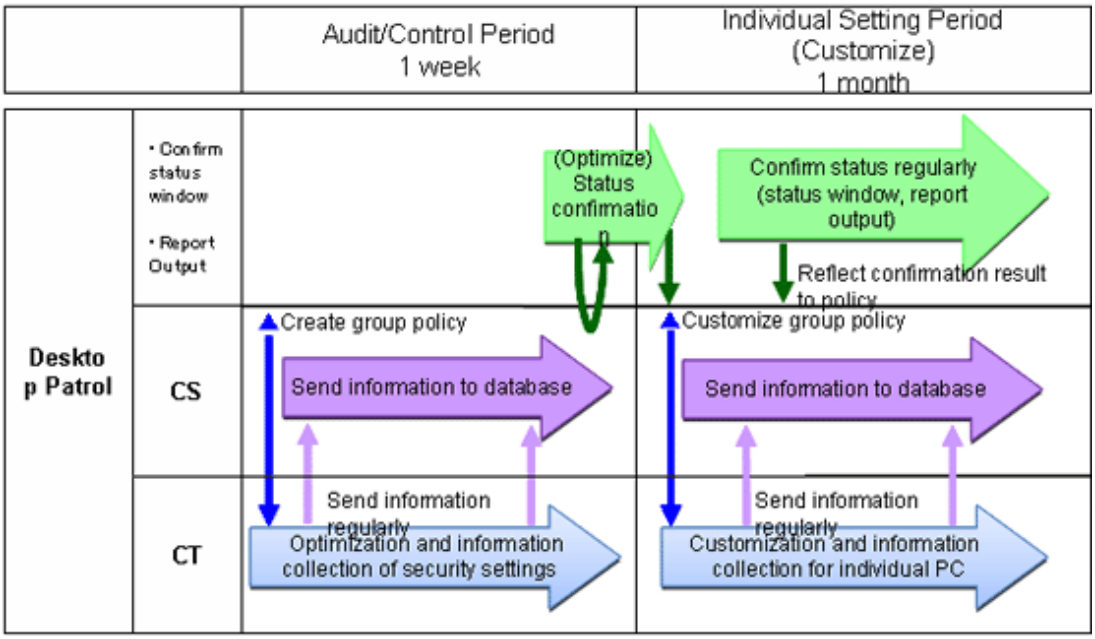
   In order to know the period of power saving and security settings, the control operation of power saving and security settings is performed here.

   In this period, check the status window or report result to confirm the status of power saving and security settings.

2. Customized period

   After the power saving and security settings are known, it will become the period for compulsory change and customization for individual PC.

   Check the status window or report result regularly to confirm the status of power saving and security settings. If customization is needed, further change of policy is required.



4.2 Settings

In order to audit and manage PC settings, the following settings should be performed.

- Setting for auditing power saving settings
- Settings for auditing security settings

4.2.1 Settings for Auditing Power Saving Settings

To audit power saving settings, the following settings are required.

- Settings of power consumption
- Settings of auditing items of power saving settings

Set power consumption

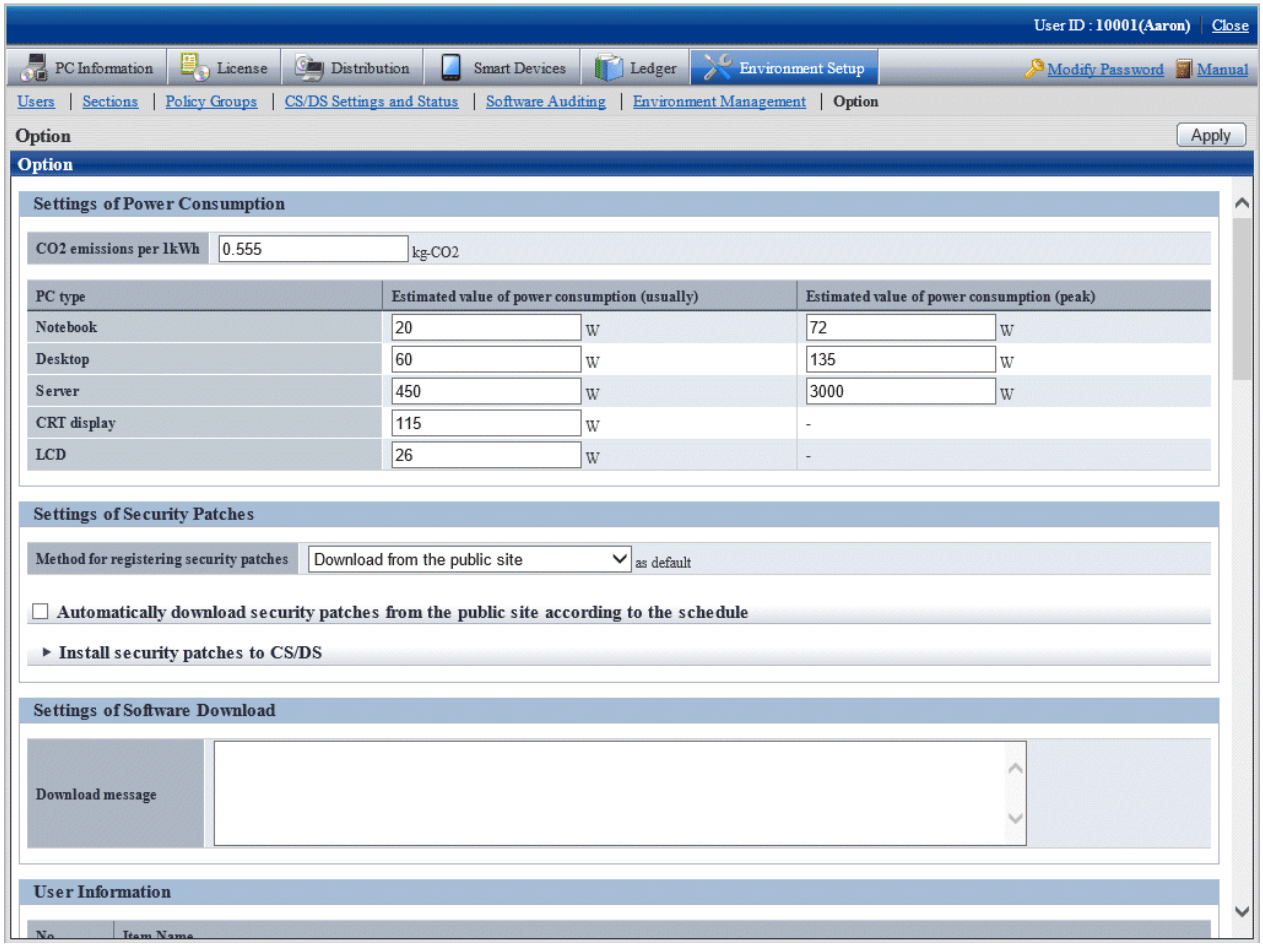
Perform settings related to the calculation of power consumption volume.

1. Log in to the main menu, and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Option**.

   The following window will be displayed.



3. Set the following items.

   Based on the value set here, calculate the value of the following items.

   - Value of **Settings of Power Consumption** of the diagnosis result window (power saving) of operation settings

Item	Description
CO2 emissions per 1kWh	Set the CO2 emission equivalent to 1kWh with a value within 0.000~9.999. Default value (0.555 Kg-CO2) is the standard value by Ministry of the Environment Government of Japan.
PC type	Set the estimated value of power consumption volume. The default value of power consumption is described according to the average value of power consumption of Server, Desktop PC and Notebook PC of Fujitsu products in the past 3 years. The power consumption volume of PC varies depending on the PC model, CPU type, size of display and other accessories. If these values are greatly different from the actual operation, modify the value. - **Notebook** Set the power consumption volume of notebook with a value within 0.00~99999.99. - **Desktop** Set the power consumption volume of desktop with a value within 0.00~99999.99. - **Server** Set the power consumption volume of server with a value within 0.00~99999.99. - **CRT display** Set the power consumption volume of CRT display with a value within 0.00~999.99. - **LCD** Set the power consumption volume of LCD with a value within 0.00~999.99.

4. Click the **Apply** button.

Set auditing items of power saving settings

The setting items of power saving to be audited is set in **Environment Setup** > **Policy Groups** of the main menu.

For details, refer to "4.2.1.1 Set the Auditing Items of Power-Saving Settings".

4.2.1.1 Set the Auditing Items of Power-Saving Settings

Set the auditing items of power saving settings.

The procedure is as follows.

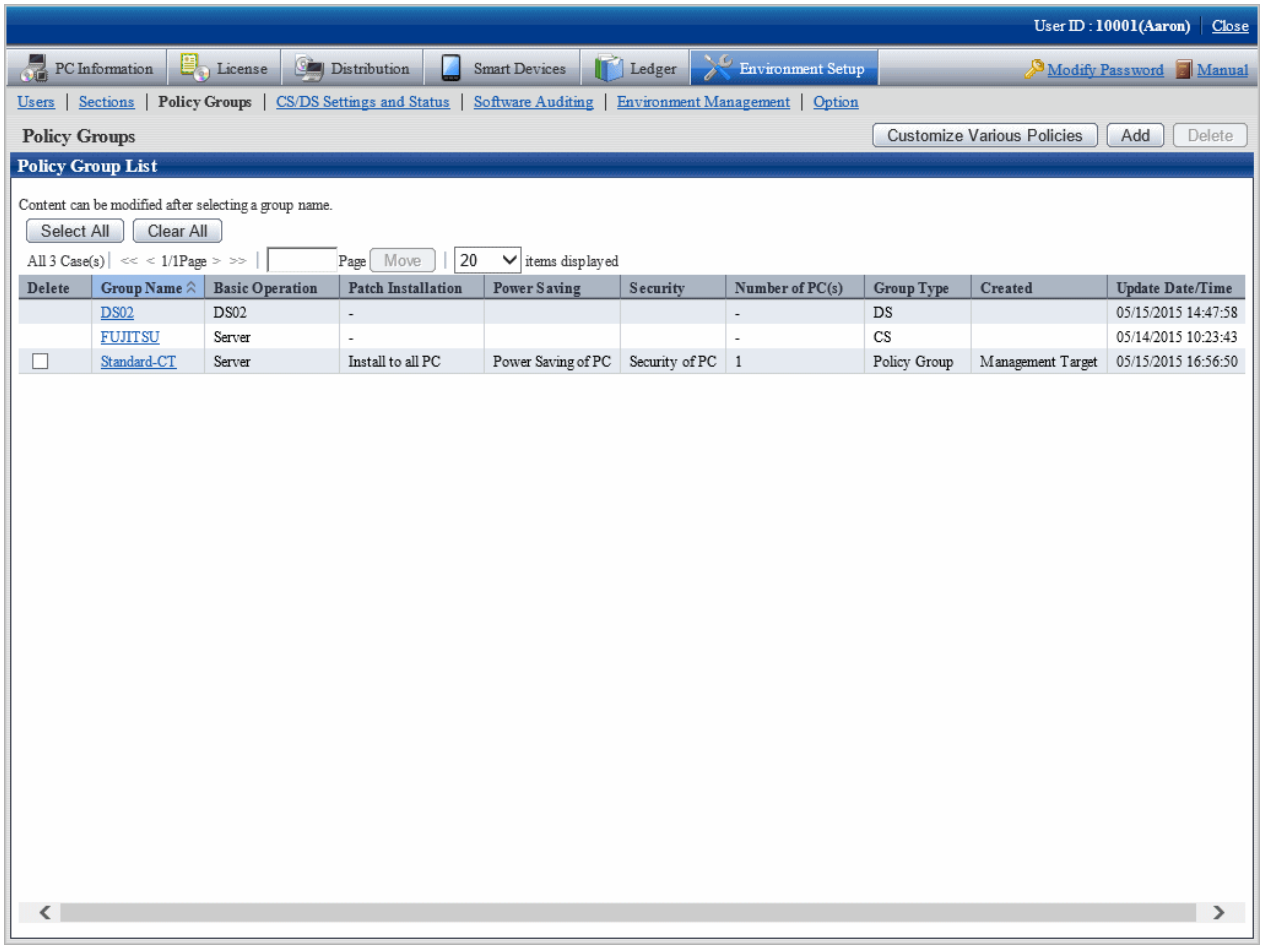
In addition, the setting of auditing items is also effective for command mode CT. When it is set to display the window, the Diagnosis result window of operation settings will be displayed.

1. Log in to the main menu, and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

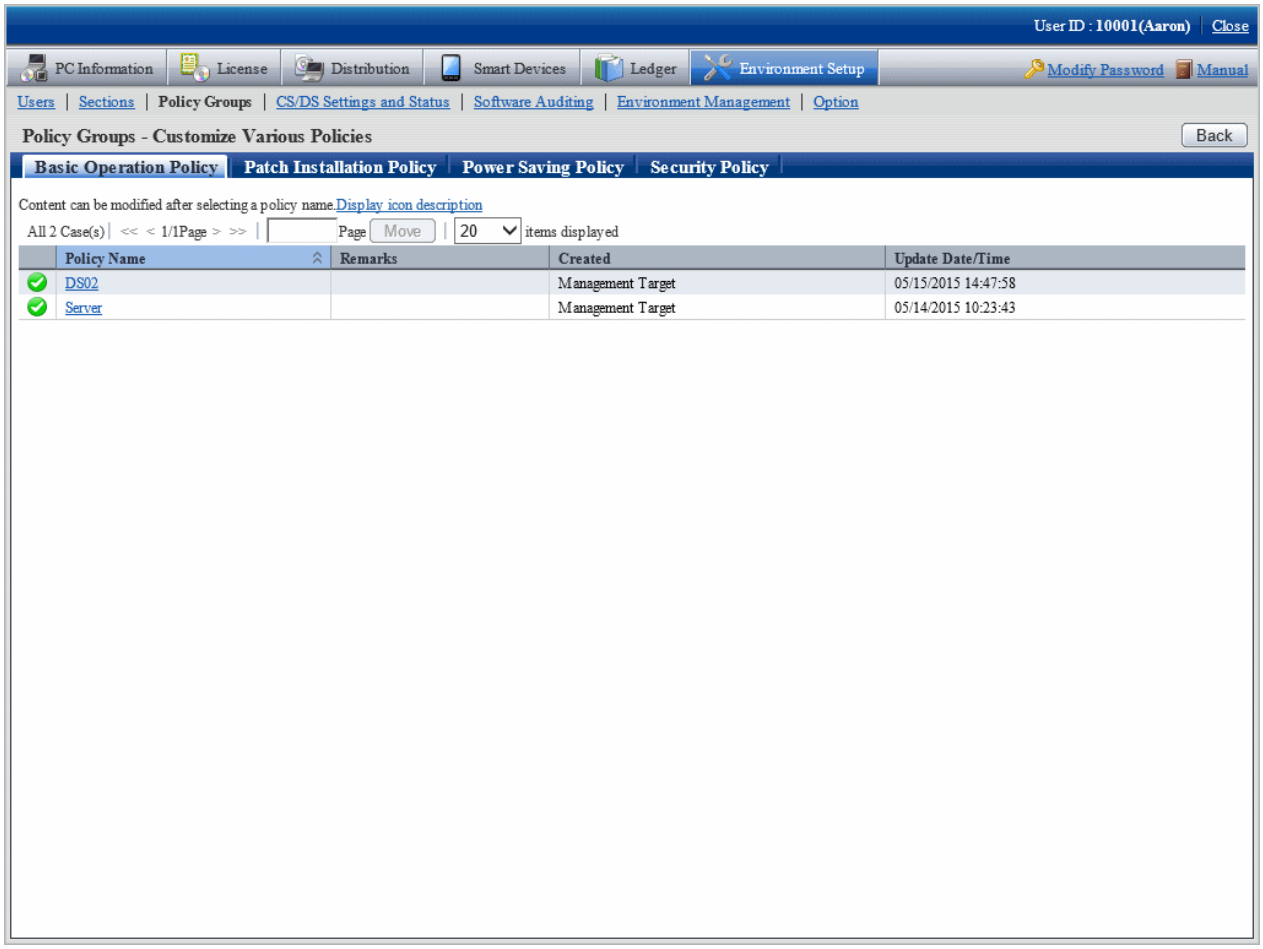
2. Click **Policy Groups**.

   The following window will be displayed.



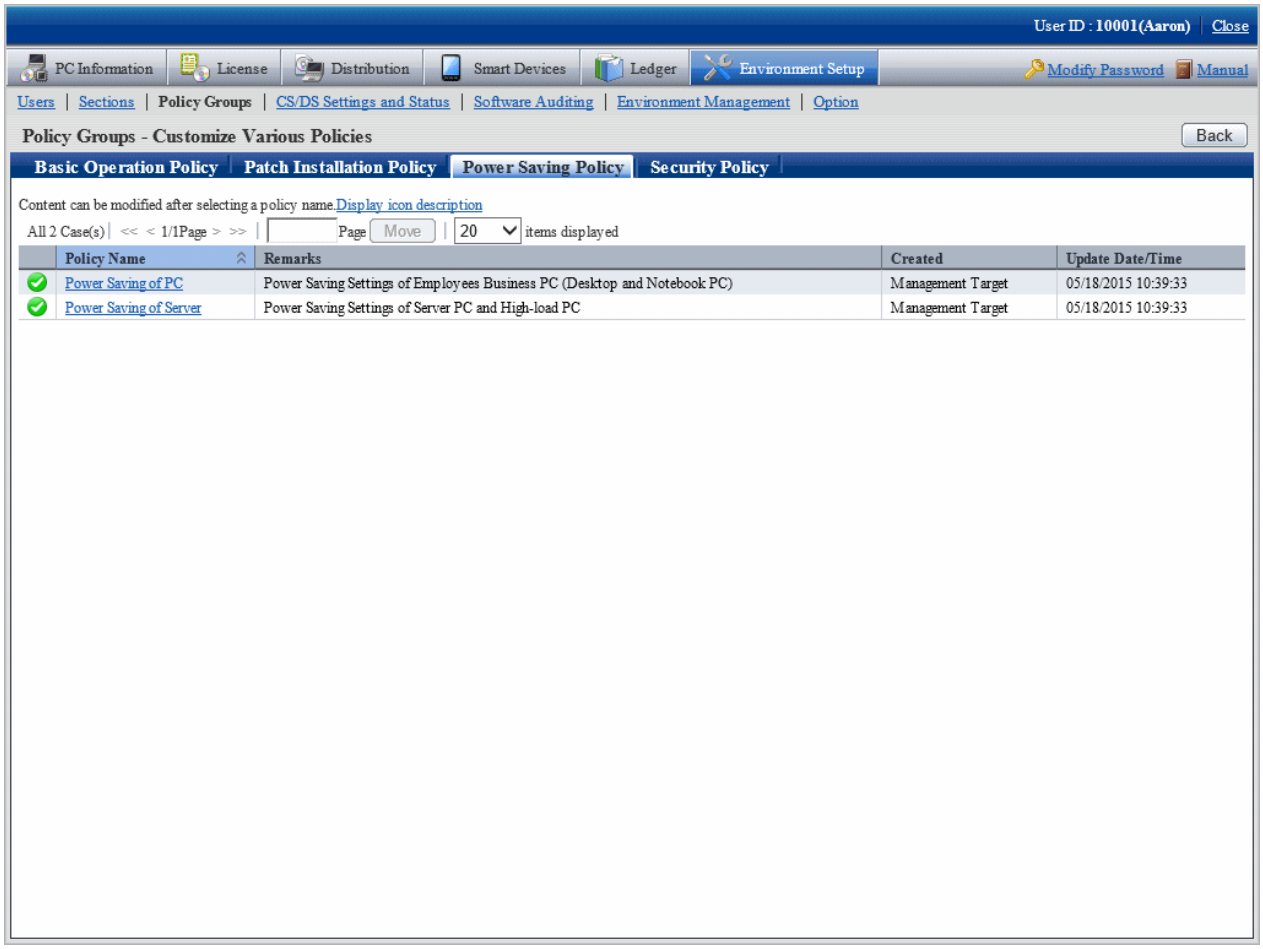
3. Click the **Customize various policies** button.

   The following window will be displayed.



4. Click the **Power saving policy** tab.

   The following window will be displayed.



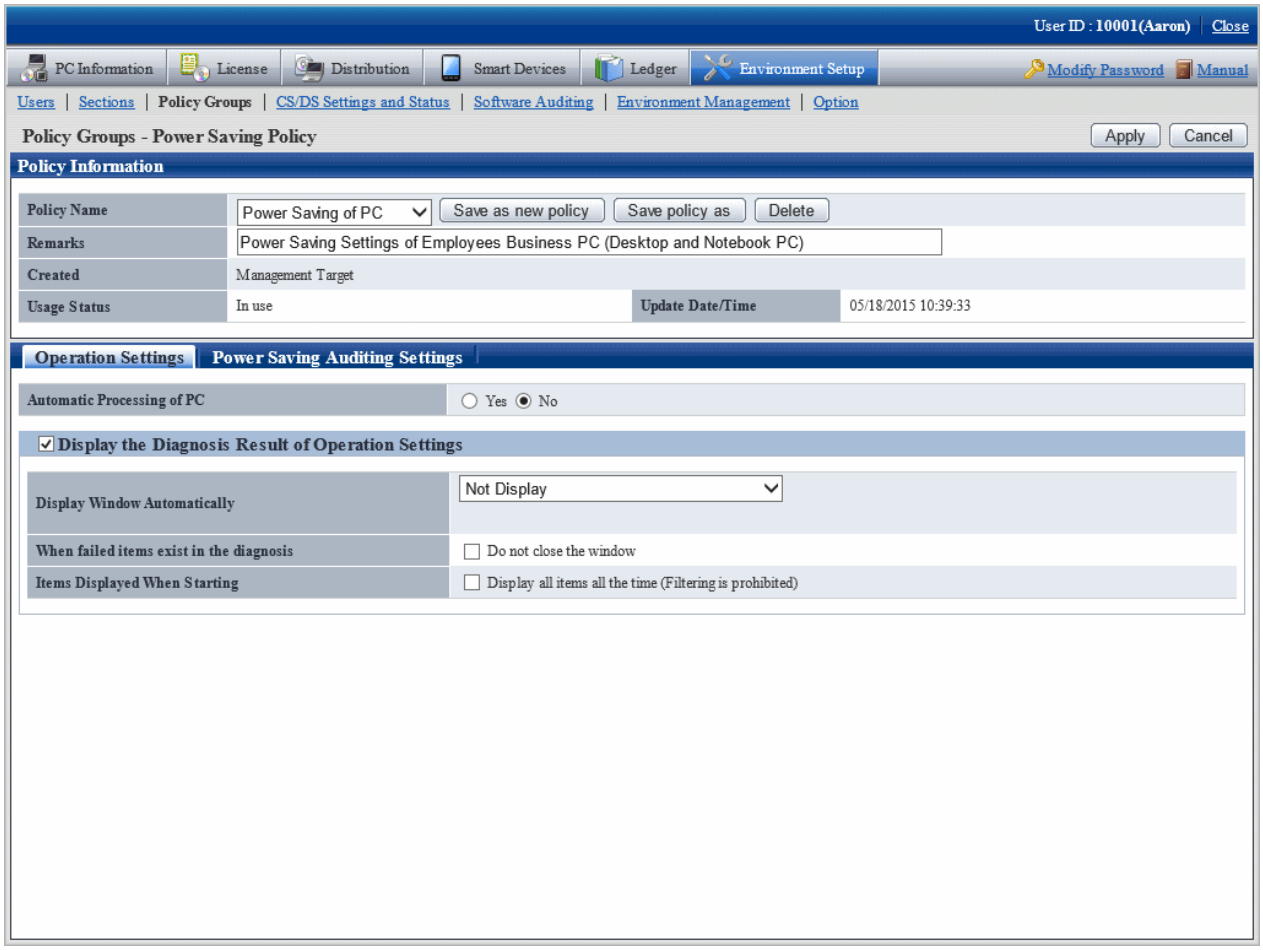
5. Select the one of the following setting patterns based on purpose and click the link of policy name.

   The recommended detailed settings have been set in each policy. The customization can be performed based on this setting.

Purpose	Auditing Contents
Power Saving of PC	It is the power saving auditing policy for business PC (desktop PC, notebook PC) used by general employees. Audit the all the power saving auditing items.
Power Saving of Server	It is the power saving auditing settings for server PC and PC with high load. Audit the power settings of monitor only.

6. Perform the operation settings of Diagnosis result window of operation settings.

   Click the **Operation Settings** tab, and the following window will be displayed.



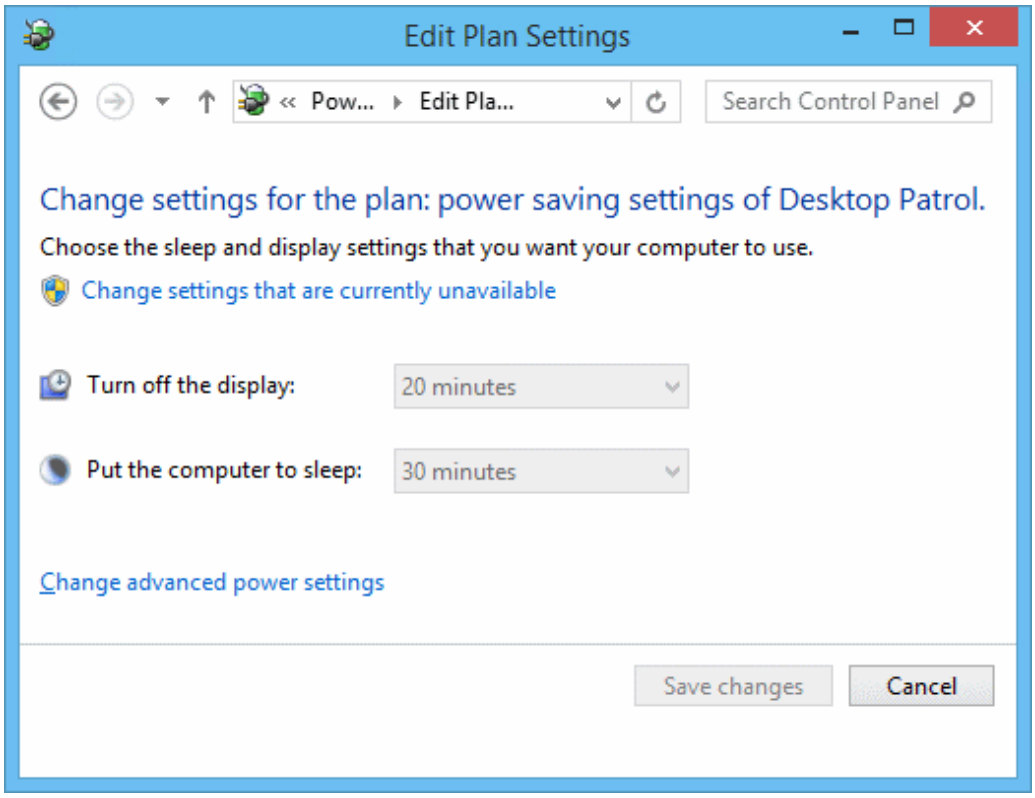
   Set the following items.

Item	Description		Initial Value
Automatic Processing of PC (Note 1)	Set whether each auditing item will change settings automatically according to Systemwalker Desktop Patrol.		**No**
Display the Diagnosis Result of Operation Settings (Note 2)	Set whether to display the Diagnosis result window of operation settings. When it is selected, the following items can be set.		Selected
	Display Window Automatically	The timing of automatically displaying the diagnosis result window is selected from the following. - **Not Display** - **Display During Logon** When **Display at Logon** is selected, display in the following timing. - At Windows logon	**Not Display**

Item	Description		Initial Value
		- The PC is standby on the previous day and restore from the standby on the next day - **Display During Logon and Specified Time** When **Display During Logon and Specified Time** is selected, specify the time. The default is 1pm.	
		- **Perform Inventory collection when displaying** Select when performing inventory collection after the diagnosis result window is displayed. When it is not selected, the result of last inventory collection will be displayed.	
	When failed items exist in the diagnosis	If failed items exist, it is selected when users are not allowed to close the Diagnosis result window of operation settings.	Not selected
	Items Displayed When Starting	When the auditing window is started, select it to display all items constantly.	Not selected

Note 1)

When **Yes** is selected for **Automatic Processing of PC**, **power saving settings of Desktop Patrol** will be added in the properties of PC power options.



Note 2)

The setting that is different from the power saving policy and security policy can be set for this item.

The operation of performing different settings in each policy is as follows.

Setting Item		Power Saving Policy	Security Policy	Operation
Display the Diagnosis Result of Operation Settings	-	Selected/Not selected	Selected/Not selected	The selected tab will be displayed. If none of them is selected, window will not be displayed.
	Display Window Automatically	Not Display	Not Display	Window will not be displayed automatically.
		Not Display	Display During Logon	Window will be displayed automatically at logon.
		Not Display	Display During Logon and Specified time	Window will be displayed automatically at logon and at specified time.
		Display During Logon	Not Display	Window will be displayed automatically at logon.
		Display During Logon	Display During Logon	Window will be displayed automatically at logon.
		Display During Logon	Display During Logon and Specified time	Window will be displayed automatically at logon and at specified time.
		Display During Logon and Specified time	Not Display	Window will be displayed automatically at logon and at specified time.
		Display During Logon and Specified time	Display During Logon	Window will be displayed automatically at logon and at specified time.
		Display at logon and specified time	Display at logon and specified time	Window will be displayed automatically at logon and at specified time.(*1)
	Perform Inventory collection when displaying	Selected/Not selected	Selected/Not selected	After it is selected, inventory collection will be performed at the timing specified in **Display Window Automatically**. Operation can be set according to each policy.
	When failed items exist in the diagnosis	Selected/Not selected	Selected/Not selected	When failed items exist in the selected tab, the window cannot be closed.
	Items Displayed When Starting	Selected/Not selected	Selected/Not selected	The narrowing function of the selected tab will be disabled.

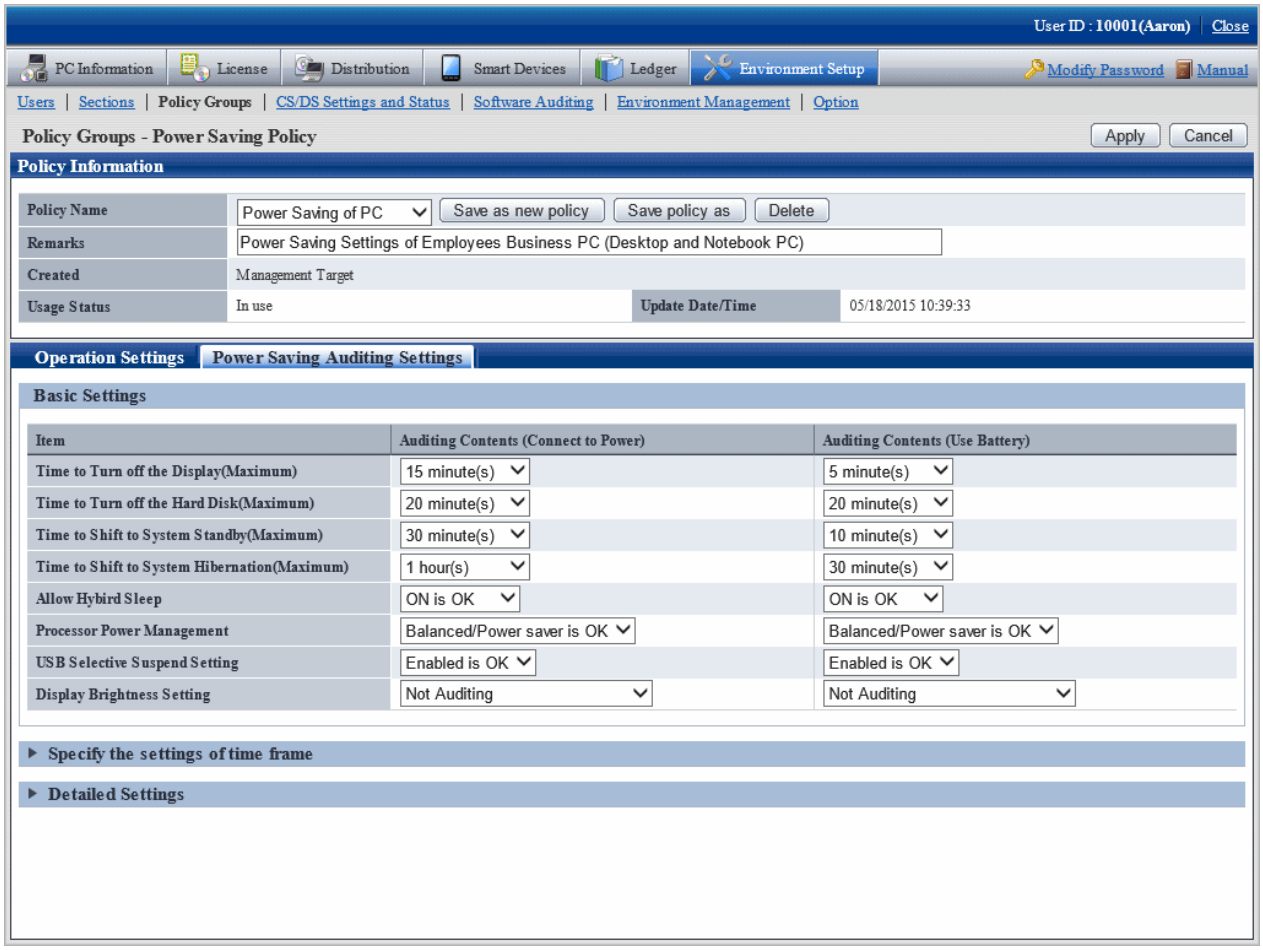
*1)In power saving policy and security policy, when the time that is different from the specified time is specified, the window will be displayed automatically in the following 3 timings.

- At logon
- Specified time set in power saving policy

- Specified time set in security policy

7. Set the auditing items of power saving.

   Click the **Power Saving Auditing Settings** tab and the following window will be displayed.



   Set the following auditing items.

Item	Description	Value set at auto-processing	Initial Value			
			Power Saving of PC		Power Saving of Server	
			Connect to power	Use battery	Connect to power	Use battery
Time to Turn off the Display(Maximum) (Note 1)	When there is no operation on the PC, audit whether it is set to cut off power of monitor at proper time. Select from the following. - ***n* minutes (*n* hours)** - **Not set is OK** - **Not Auditing** *The selectable range is within 1 minute ~ 5 hours.	Brightness Settings of Display	15 minutes	5 minutes	15 minutes	5 minutes

Item	Description	Value set at auto-processing	Initial Value			
			Power Saving of PC		Power Saving of Server	
			Connect to power	Use battery	Connect to power	Use battery
Time to Turn off the Hard Disk(Maximum) (Note 1) (Note 4)	When there is no operation on the PC, audit whether it is set to cut off the power of hard disk at proper time. Select from the following. - ***n* minutes (*n* hours)** - **Not set is OK** - **Not Auditing** *The selectable range is within 3 minutes ~ 5 hours.	Brightness Settings of Display	20 minutes	20 minutes	Not Auditing	Not Auditing
Time to Shift to System Standby(Maximum) (Note 1) (Note 4)	When there is no operation on the PC, audit whether it is set to shift to system standby at proper time. Select from the following. - ***n* minutes (*n* hours)** - **Not set is OK** - **Not Auditing** *The selectable range is within 1 minute ~ 5 hours.	Brightness Settings of Display	30 minutes	10 minutes	Not Auditing	Not Auditing
Time to Shift to System Hibernation(Maximum) (Note 1) (Note 4) (Note 5)	When there is no operation on the PC, audit whether it is set to shift to system sleep at proper time. Select from the following. - ***n* minutes (*n* hours)** - **Not set is OK** - **Not Auditing** *The selectable range is within 1 minute ~ 6 hours.	Brightness Settings of Display	1 hour	30 minutes	Not Auditing	Not Auditing
Allow Hybrid Sleep (Note 2)	Audit the setting items of Hyper sleep. Select from the following. - **ON is OK** - **Not Auditing**	Set to ON	Set to ON is OK	Set to ON is OK	Not Auditing	Not Auditing
Processor Power Management (Note 2) (Note 3) (Note 4)	When there is no operation on the PC, audit whether it is set to reduce the CPU clock speed. Select the minimum value of CPU clock speed from the following. - **Power saver is OK** **Plugged in**: 0% for **Minimum**	Display Brightness Setting	Balanced/Power saver is OK	Balanced/ Power saver is OK	Not Auditing	Not Auditing

Item	Description	Value set at auto-processing	Initial Value			
			Power Saving of PC		Power Saving of Server	
			Connect to power	Use battery	Connect to power	Use battery
	processor state and 0% - 100% for **Maximum processor state** are deemed acceptable. **On battery**: 0% for **Minimum processor state** and 0% - 50% for **Maximum processor state** are deemed acceptable. - **Balanced/Power saver is OK** **Plugged in**: 0% - 5% for **Minimum processor state** and 0% - 100% for **Maximum processor state** are deemed acceptable. **On battery**: 0% - 5% for **Minimum processor state** and 0% - 100% for **Maximum processor state** are deemed acceptable. - **Not Auditing**					
USB Selective Suspend Setting (Note 2)	Audit the settings of selective suspension of USB. Select from the following. - **Valid is OK** - **Not Auditing**	Set to Valid	Valid is OK	Valid is OK	Not Auditing	Not Auditing
Display Brightness Setting (Note 2)	Audit the brightness of display. Select from the following. - **Darkness settings is OK** 0% - 40% is deemed acceptable. - **Dark-General Brightness is OK** 0% - 70% is deemed acceptable. - **Not Auditing**	Display Brightness Setting	Not Auditing	Not Auditing	Not Auditing	Not Auditing

Note 1)

Select the time of various items from the following.

Item	Selection
Time to Turn off the Display(Maximum)	1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes, 25 minutes, 30 minutes, 45 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, None

Item	Selection
Time to Shift to System Standby(Maximum)	
Time to Shift to System Hibernation(Maximum)	1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes, 25 minutes, 30 minutes, 45 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hours, None
Time to Turn off the Hard Disk	3 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes, 25 minutes, 30 minutes, 45 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, None

Note 2)

This item is only effective in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

Note 3)

The set value can be modified by force only on the PC with power saving technology of processor.

- Made by Intel: Extended edition of Intel SpeedStep(R) Technology(EIST), Demand & Base & Switching (DBS)
- Made by AMD: PowerNow!, Cool'n'Quiet

Note 4)

The motherboard/BIOS may not be supported. At this time, no item can be displayed in the diagnosis result.

Note 5)

Power management settings (settings to transition to hibernation) cannot be configured on PCs that have Rapid Start Technology installed.

None will be displayed for the settings value on the operating system. For this reason, **Time to Shift to System Hibernation** will not be handled automatically on the PCs in question.

Example: Power management settings (settings to transition to hibernation) on Windows 8

1. Click **Control Panel** > **Power Options**, and for the selected plan click **Change plan settings**.
2. Click **Change advanced power setting**s.
3. In **Sleep** > **Hibernate after**, set the following items:

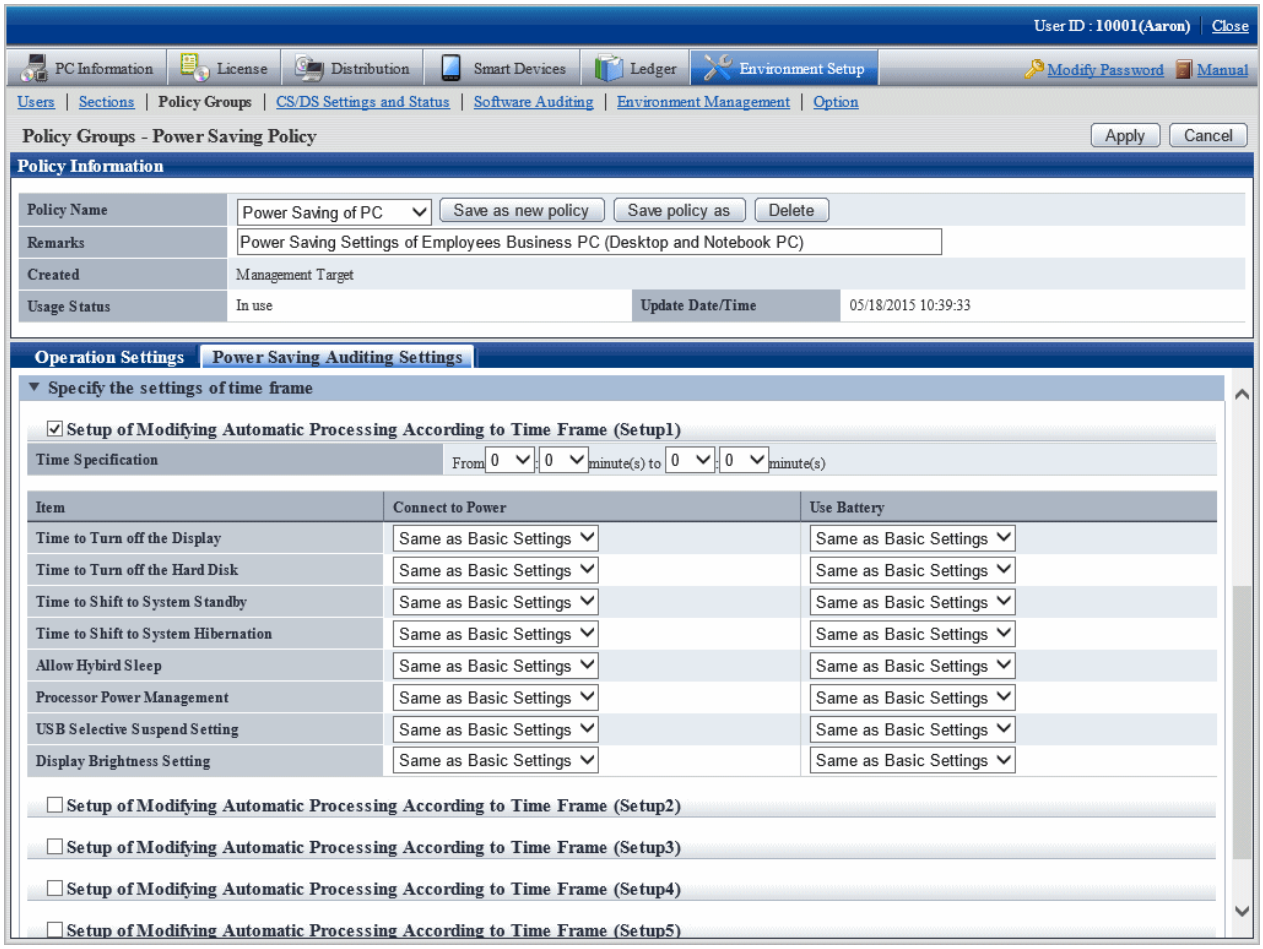
- **On battery**
- **Plugged in**

About auto-processing

In the Active Directory environment, the setting of Windows group policy is effective, so it may not be able to process automatically sometimes. Modify the setting of Windows group policy to not audit for the items set in Windows group policy.

8. To modify the setting of auto-processing according to time frame, click **Specify the settings of time frame**.

   The following window will be displayed.



In the **Operation Settings** tab, select **Yes** for **Automatic Processing of PC**, and the operation of auto-processing that is different from the specified time frame can be set.

Up to 5 items can be created for the setting of operation that specified time frame.

Item	Description		Value set at auto-processing	Initial Value			
				Power Saving of PC		Power Saving of server	
				Connect to power	Use battery	Connect to power	Use battery
Setup of Modifying Automatic Processing According to Time Frame	Select it when modifying the settings of auto-processing at specified time frame. When it is selected, the following items can be set.		-	Not selected	Not selected	Not selected	Not selected
	Time to Turn off the Display	The content that can be set is same as the basic settings.	Same as basic settings	Same as basic settings	Same as basic settings	Same as basic settings	Same as basic settings
	Time to Turn off the Hard Disk						
	Time to Shift to System Standby						

Item	Description		Value set at auto-processing	Initial Value			
				Power Saving of PC		Power Saving of server	
				Connect to power	Use battery	Connect to power	Use battery
	Time to Shift to System Hibernation						
	Allow Hybrid Sleep						
	Processor Power Management						
	USB Selective Suspend Setting						
	Display Brightness Setting						

Point

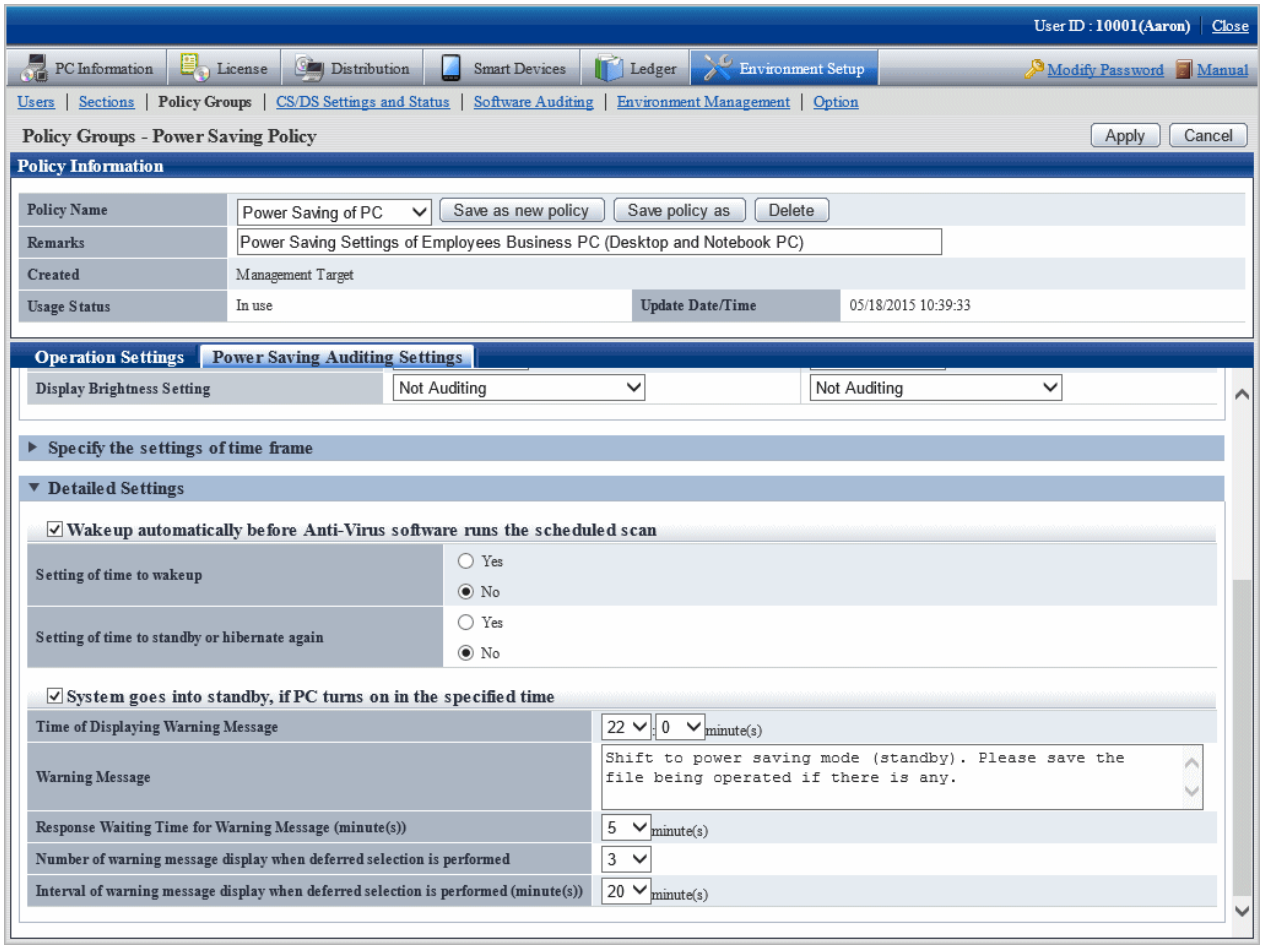
About Security Patch installation at Standby/Suspension Status

Security patches cannot be installed when PC is in standby/sleep status.

When it is expected to install security patches in operation, set to disable the system from shifting into standby/sleep status at the time frame when installation of security patches is performed in "Setting to Specify Time Frame" mentioned above.

9. To perform more detailed settings, click **Detailed Settings**.

   The following window will be displayed.



Set the following items.

Item	Description		Initial Value	
			Power Saving of PC	Power Saving of Server
Wakeup automatically before Anti-virus software runs the scheduled scan	When performing the auditing of security settings, select it when it is expected to restore the system from standby/sleep status. When it is selected, the following items can be set.		Not selected	Not selected
	Setting of time to wakeup (Note 1)	Select whether to specify the time to restore from standby/ sleep. - **No** - **Yes** When **Yes** is selected, time frame should be specified. The default is 12pm.	**No**	**No**

Item	Description		Initial Value	
			Power Saving of PC	Power Saving of Server
	Setting of time to standby or hibernate again	Select whether to specify the time to shift to standby/sleep again after restoring from standby/sleep. - **No** - **Yes** When **Yes** is selected, the time frame should be specified. The default is 30 minutes later.	**No**	**No**
System goes into standby, if PC turns on in the specified time	When PC is started at specified time, select it when shifting to system standby. When it is selected, the following items can be set.		Not selected	Not selected
	Time of Displaying Warning Messages	Set the time to display warning message.	**22:00**	**22:00**
	Warning Message	Set the warning message using up 512 fullwidth characters or 1024 halfwidth characters.	(Note 2)	(Note 2)
	Response Waiting Time for Warning Messages	Set the time to wait when there is no response in warning message with a value within 1~60 minutes.	**5**	**5**
	Number of warning message display when deferred selection is performed	When **Delay** is selected in warning message, set the times to display warning message again within 0~10 times.	**3**	**3**
	Interval of warning message display when deferred selection is performed	When **Delay** is selected in warning message, set the interval to display warning message again with a value within 1~60 minutes.	**20**	**20**

Note 1)

For the anti-virus software of the following vendors, even if **No** is selected in **Setting of time to wakeup**, it can still restore automatically before the scheduled scan.

- Endpoint Protection 12.1 of Symantec Corporation
- VirusScan Enterprise 8.7i/8.8 of McAfee Corporation
- Virusbuster Corporate Edition 10.0/10.5/10.6 of TrendMicro Corporation

When the anti-virus software apart from the above is used, select **Yes** in **Setting of time to wakeup** and specify the time.

Note 2)

For characters that cannot be entered in warning message, refer to "1.2 Main menu".

The initial value of warning message is as follows.

```
Shift to power saving mode (standby). Please save the file being operated.
```

10. Click the **Apply** button and save the settings.

4.2.2 Settings Related to Auditing Security Settings

To audit security settings, the following settings are required.

- Settings of Windows update program to be audited
- Settings of anti-virus software to be audited
- Settings of encryption software to be audited
- Settings of prohibition software to be audited
- Settings of security auditing items

Set the windows update program to be audited

The auditing of **Application Status of Windows Update Program** is to check the security patch to be selected as the auditing target in software dictionary.

Select the security patch to be audited in **Distribution** > **Security Patches Distribution** of the main menu. For selection of security patch, refer to "6.2.4 Select Security Patches".

Set the anti-virus software to be audited

The auditing of **Anti-virus Software** is to check the anti-virus software selected as auditing target in software dictionary.

Select the anti-virus software to be audited in **Environment Setup** > **Software Auditing** of the main menu.

Set the encryption software to be audited

The auditing of **Encryption Software** is to check the encryption software selected as auditing target in software dictionary.

Select the encryption software to be audited in **Environment Setup** > **Software Auditing** of the main menu.

Set the prohibition software to be audited

The auditing of "Prohibition Software" is to check the prohibition software selected as auditing target in software dictionary.

When defining "Prohibition Software" and the prohibition software is detected at client, that software can be deleted automatically.

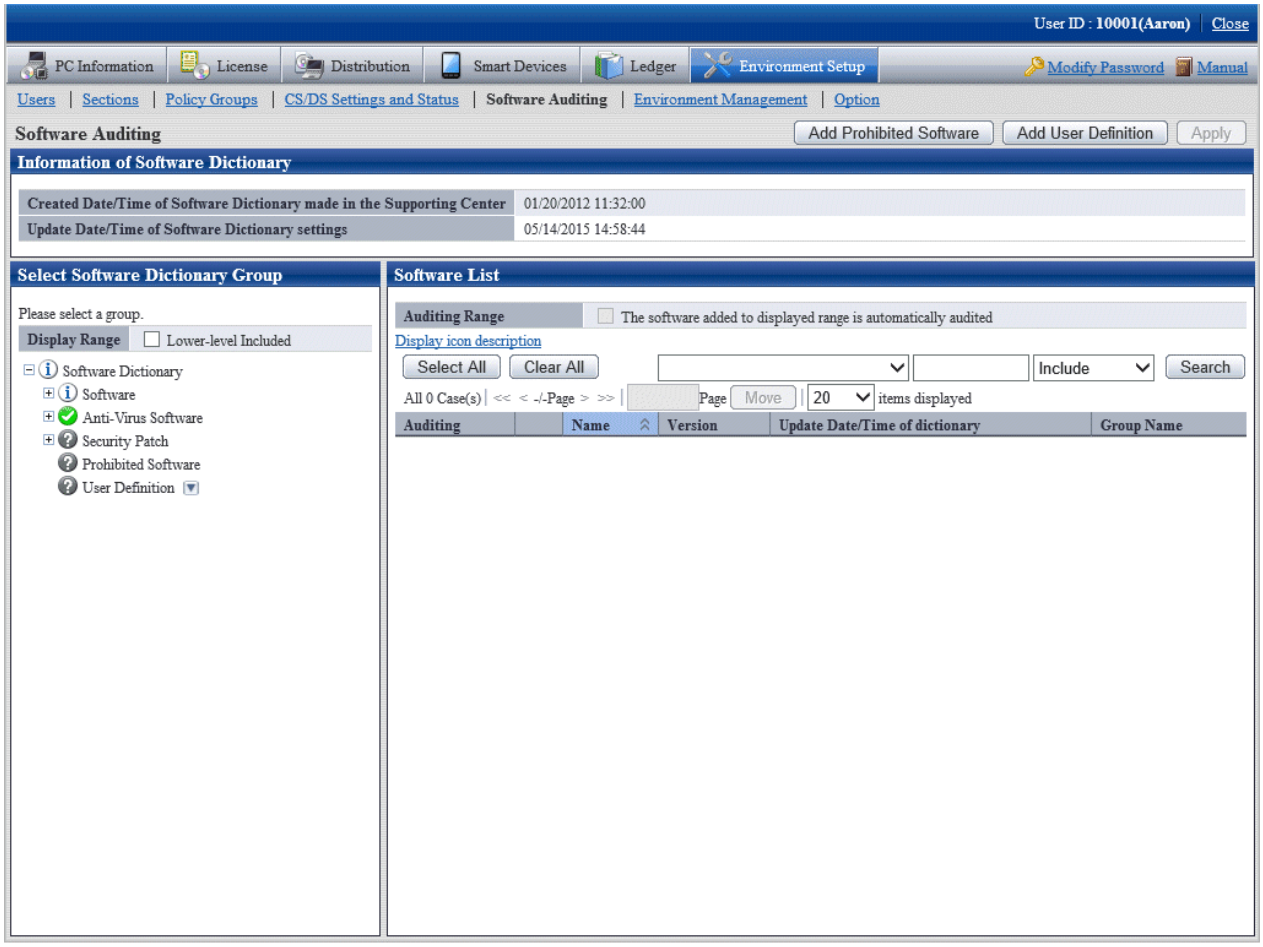
The definition of prohibition software is performed according to the following procedure.

1. Log in to the main menu, and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

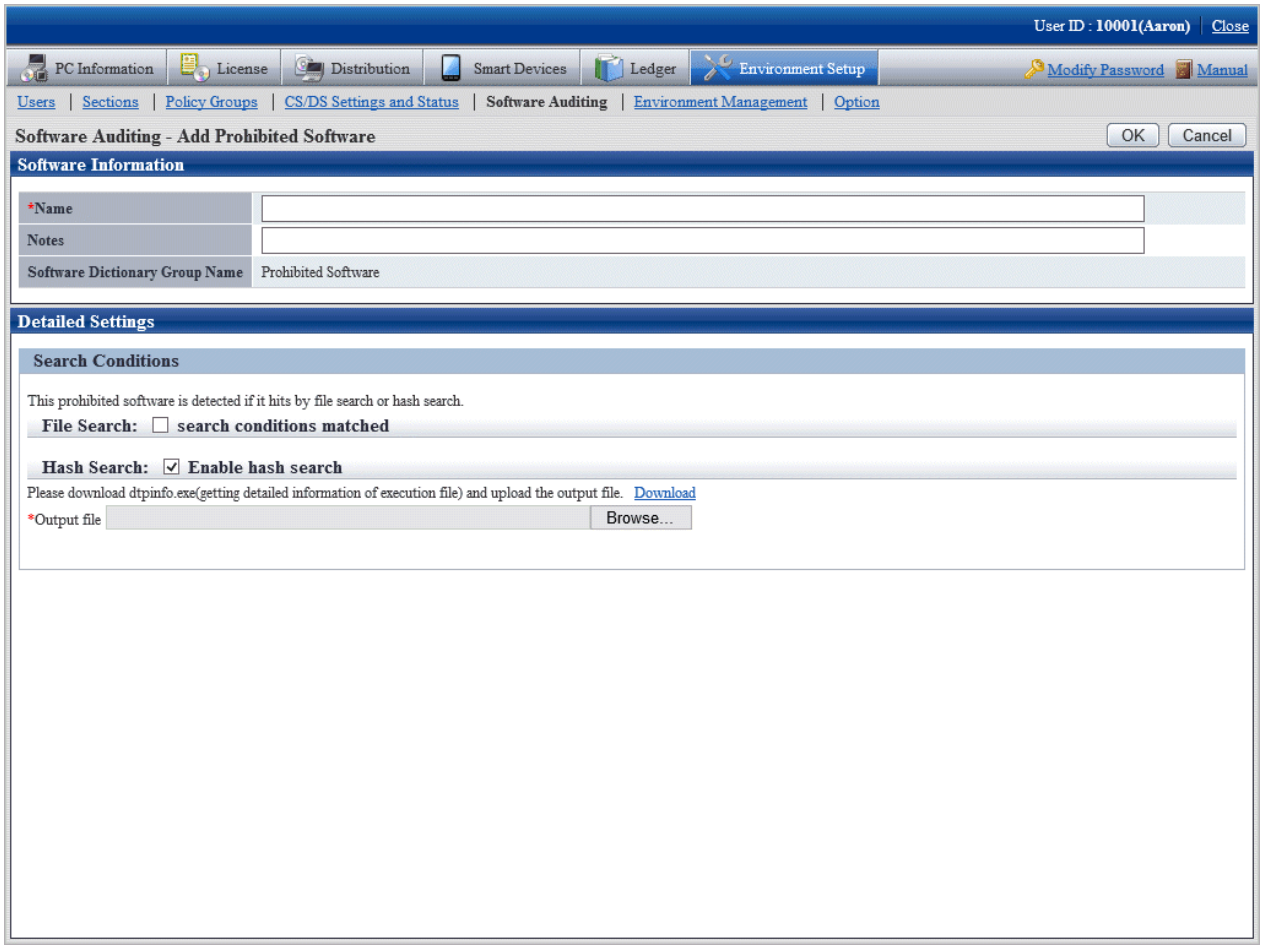
2. Click **Software Auditing**.

   The following window will be displayed.



3. Click the **Add Prohibited Software** button.

   The following window will be displayed.



4. Define the following information.

   Software information

Item	Description
Name	Specify the software name to be audited with multi-byte or single-byte characters using up to 128 fullwidth characters or 256 halfwidth characters. This item cannot be omitted.
Notes	Enter the remarks. Enter within 128 multi-byte characters or 256 single-byte characters. The characters that can be specified are alphanumeric characters, hiragana, katakana and the following single-byte symbols. - @ . ( ) [ ] { } < > : ;

   Search condition

   Specify the search condition of this software.

   Search condition includes file search and hash search. The software will be detected if one of the conditions is satisfied.

   - **File Search**

     When searching prohibition software according to file name, select **File with search conditions matched**.

Item	Description
File Name	Specify the file name to be searched as software that is prohibited being used using up to 129 fullwidth characters or 259 halfwidth characters. It cannot be omitted. The following symbols cannot be specified: : \ * " < > | ? /

- **Hash search**

  When you wish to search for prohibition software according to hash information, select **Enable Hash search**.

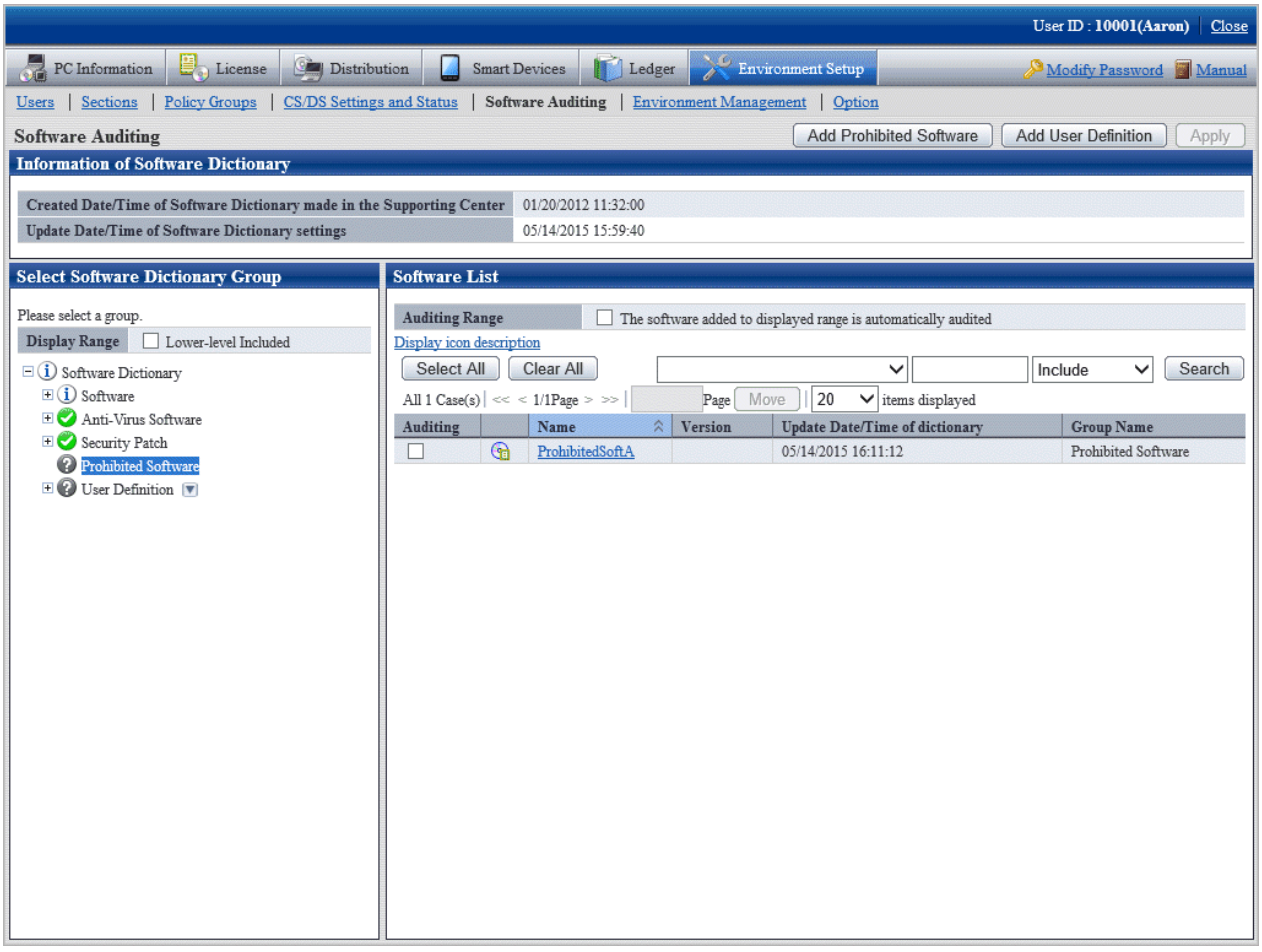
  Hash information is for registering result file output by command to server. The registration of hash information cannot be omitted. For details of command, refer to "dtpfinfo.exe (get details of executable file)" of *Systemwalker Desktop Patrol Reference Manual*.

  Hash information cannot be deleted after it has been registered. When hash search is not needed, cancel the selection of **Enable Hash Search**.

  For adding target file that is defined as prohibition software, it is recommended to back up the file/folder of hash information created previously.

5. Click the **OK** button.

   The following window will be displayed.



6. Select the check box in front of the name of software to be audited.

7. Click the **Apply** button and save the selected status.

Set auditing items

Set the security setting items to be audited in **Environment Setup** > **Policy Groups** of the main menu.

For details, refer to "4.2.2.1 Set the Auditing Items of Security Settings".

4.2.2.1 Set the Auditing Items of Security Settings

Set the auditing items of security settings.

The procedure is as follows.

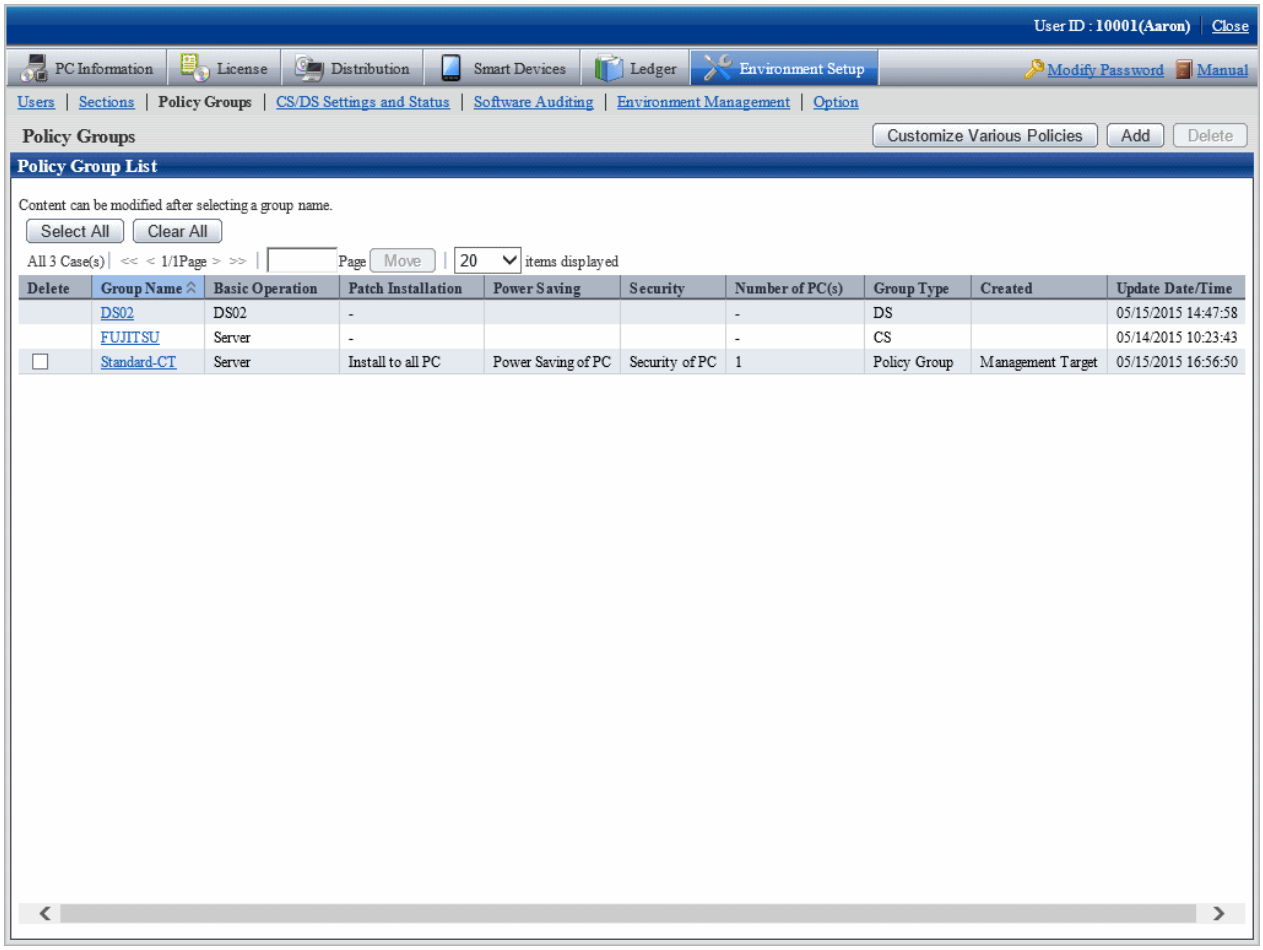
In addition, the setting of auditing items is also effective for command mode CT. When it is set to display the window, the Diagnosis result window of operation settings will be displayed.

1. Log in to the main menu, and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

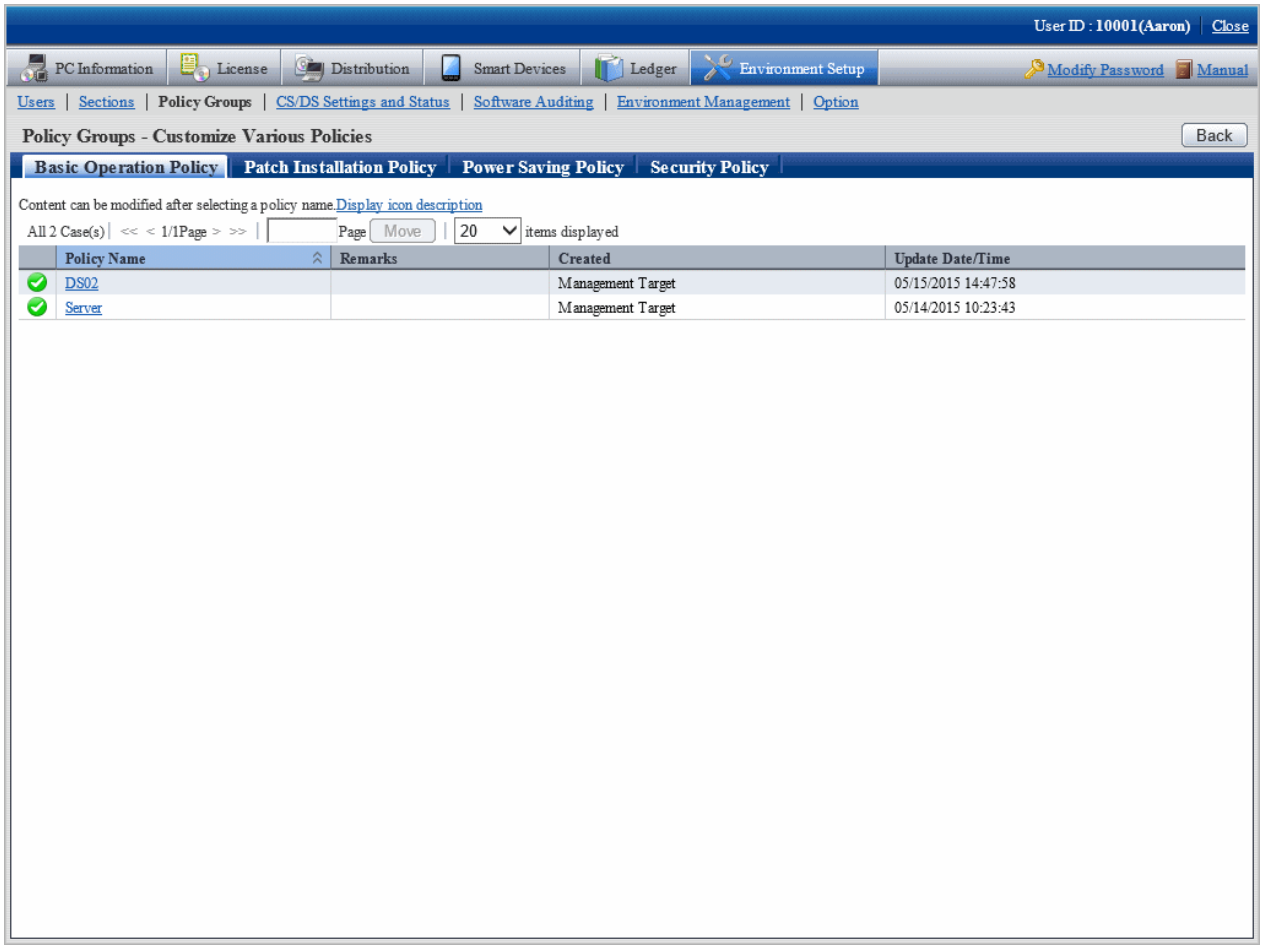
2. Click **Policy Groups**.

   The following window will be displayed.



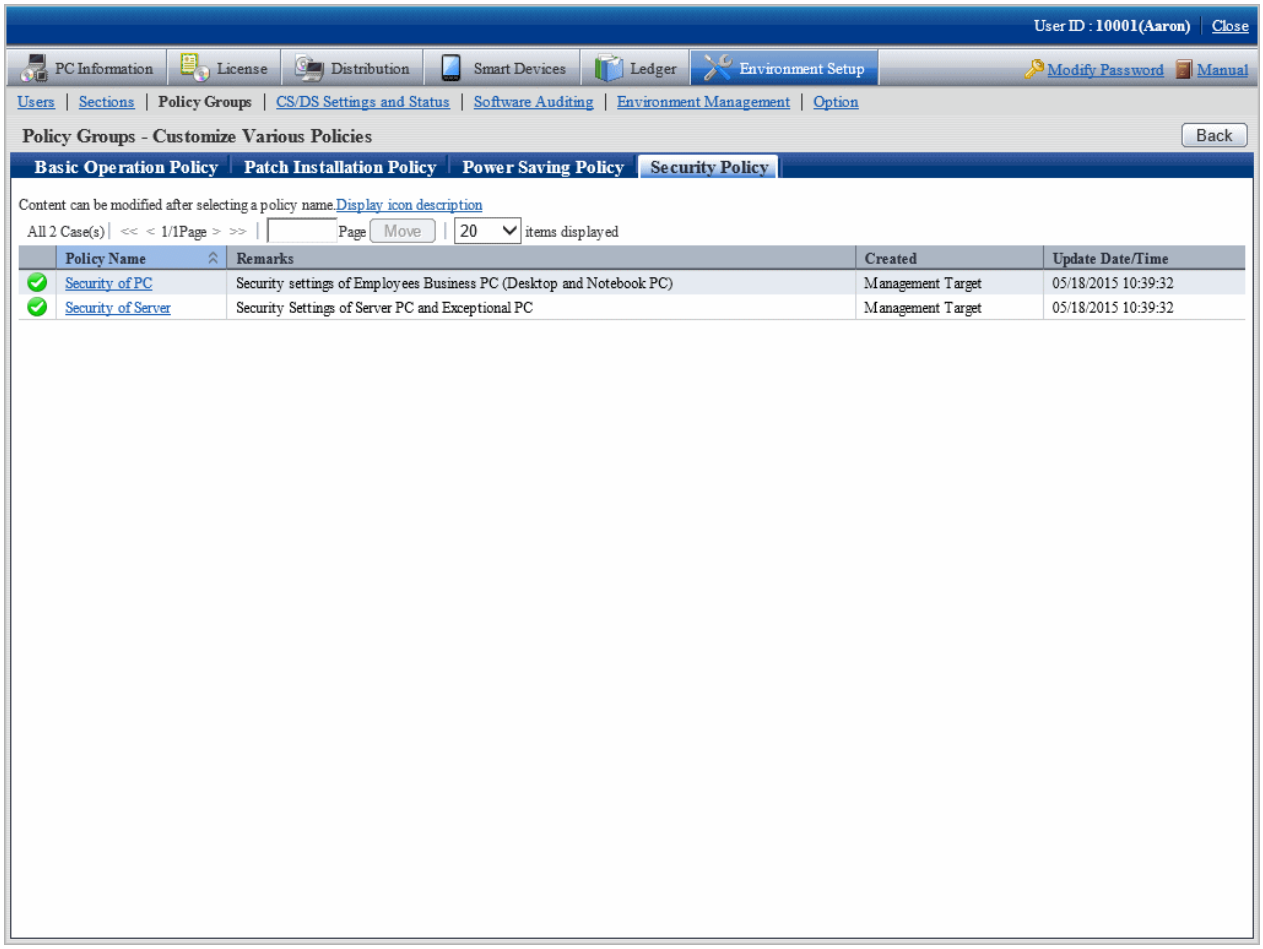
3. Click the **Customize various policies** button.

   The following window will be displayed.



4. Click the **Security policy** tab.

   The following window will be displayed.



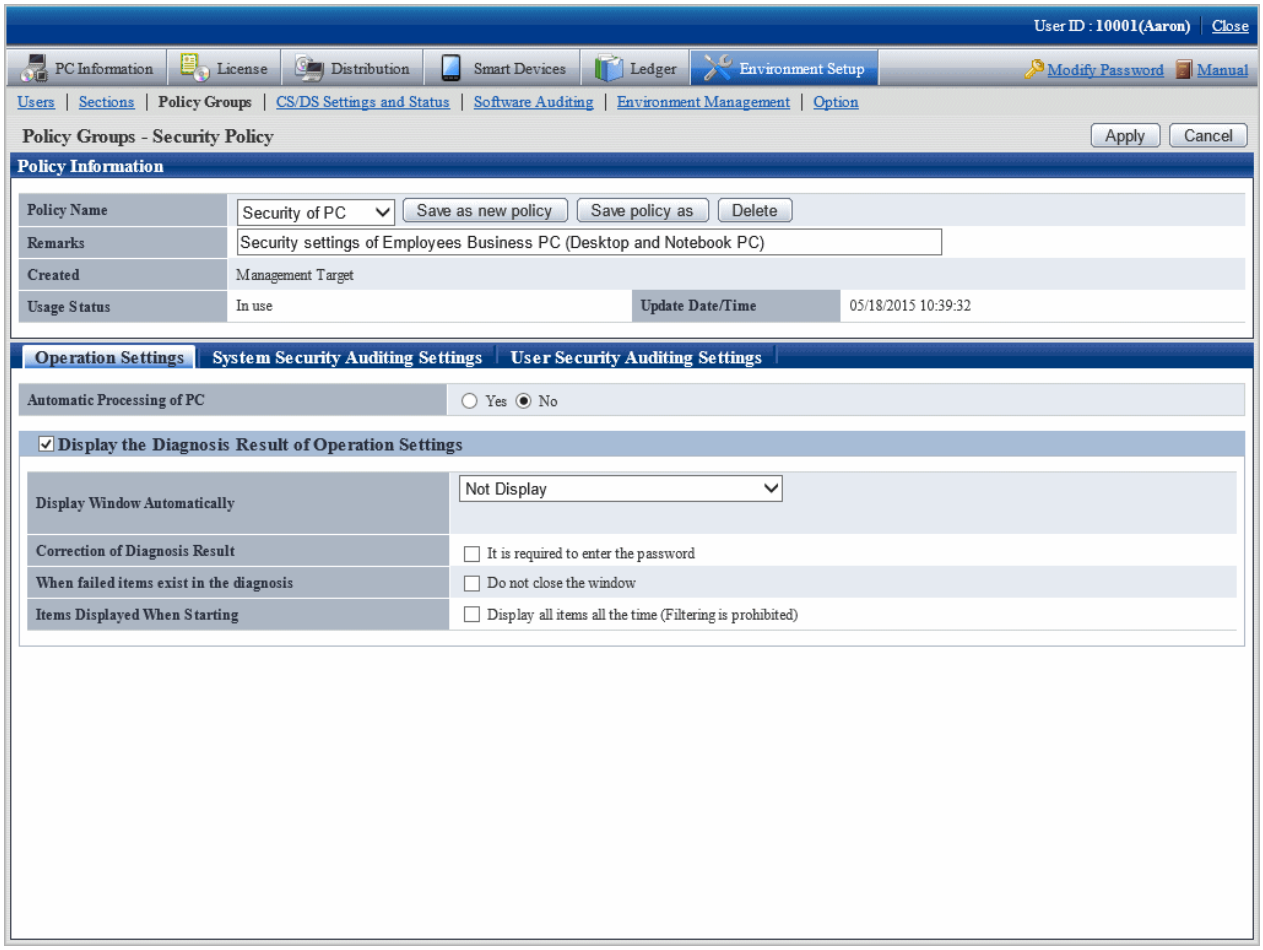
5. Select one of the following setting patterns based on purpose and click the link of policy name.

   Recommended value has been set in each policy. Customization can be performed according to the setting.

Purpose	Auditing Contents
Security of PC	It is the security auditing settings for business PC (desktop PC, notebook PC) used by general employees. Set to audit for all security auditing items.
Security of Server	It is the security auditing settings for server PC. Set to audit for auditing items apart from security patches.

6. Perform the operation settings of the Diagnosis result window of operation settings.

   Click the **Operation Settings** tab, and the following window will be displayed.



   Set the following items.

Item	Description		Initial Value
Automatic Processing of PC	Set whether Systemwalker Desktop Patrol will modify settings automatically for failed items.		**No**
Display the Diagnosis Result of Operation Settings (Note)	Set whether to display the Diagnosis result window of operation settings. When it is selected, the following items can be set.		Selected
	Display Window Automatically	Select the timing to automatically display the diagnosis result window from the following. - **Not Display** - **Display During Logon** When **Display During Logon** is selected, display in the following timing. - At Windows logon - When PC is in standby on the previous and restore from standby on the next day	**Not Display**

Item	Description		Initial Value
		- **Display During Logon and Specified Time** When **Display During Logon and Specified Time** is selected, specify the time. The default is 1pm.	
		- **Perform Inventory collection when displaying** When the diagnosis result window is displayed, select it to execute inventory collection. When it is not selected, the result of last inventory collection will be displayed.	
	Corrction of Diagnosis Result	When using the function that corrects the diagnosis result of auditing items that cannot be processed automatically to OK, specify whether it is required to enter a password. Specify single-byte alphanumeric characters and symbols with no more than 1~32 characters for password.	Not selected
	When failed items exist in the diagnosis	If failed items exist, select it when the user cannot close the Diagnosis result window of operation settings.	Not selected
	Items Displayed When Starting	When the audit window is started, select it to display all items constantly.	Not selected

Note)

The setting that is different from the power saving policy and security policy can be performed in this item.

The operation of performing different settings for each policy is as follows.

Setting Item		Power Saving Policy	Security Policy	Action
Display the Diagnosis Result of Operation Settings	-	Selected/Not selected	Selected/Not selected	Display the selected tab. When none of them is selected, the window will not be displayed.
	Display Window Automatically	Not Display	Not Display	Window will not be displayed automatically.
		Not Display	Display During Logon	Window will be displayed automatically at logon.
		Not Display	Display During Logon and Specified Time	Window will be displayed automatically at logon and at specified time.
		Display During Logon	Not Display	Window will be displayed automatically at logon.
		Display During Logon	Display During Logon	Window will be displayed automatically at logon.

Setting Item		Power Saving Policy	Security Policy	Action
		Display During Logon	Display During Logon and Specified Time	Window will be displayed automatically at logon and at specified time.
		Display During Logon and Specified Time	Not Display	Window will be displayed automatically at logon and at specified time.
		Display During Logon and Specified Time	Display During Logon	Window will be displayed automatically at logon and at specified time.
		Display During Logon and Specified Time	Display During Logon and Specified Time	Window will be displayed automatically at logon and at specified time.(*1)
	Perform Inventory collection when displaying	Selected/Not selected	Selected/Not selected	After it is selected, inventory collection can be performed at the timing specified in **Automatic Display of Window**. Operation can be set according to each policy.
	Corrction of Diagnosis Result	-	Selected/Not selected	This item can only be set in security policy.
	When failed items exist in the diagnosis	Selected/Not selected	Selected/Not selected	When failed items exist in the selected tab, it will be unable to close the window.
	Items Displayed When Starting	Selected/Not selected	Selected/Not selected	The narrowing function of the selected tab will be disabled.

*1) In power saving policy and security policy, when the time that is different from the specified one is set, the window will be displayed automatically in the following three timings.

- At logon
- Specified time set in power saving policy
- Specified time set in security policy

7. Set the item of system security auditing.

   Click the **System Security Auditing Settings** tab, The following window will be displayed.

Set the following auditing items.

Hardware

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
BIOS/Hard Disk Password	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Startup Password	Audit whether the startup password of BIOS has been set. (Administrator password). Select from the following. - **Auditing** - **Audit Notebook only** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
	Setup Password	Audit whether the setting password of BIOS has been set. (User password). Select from the following. - **Auditing** - **Audit Notebook only** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
	Hard Disk Password	Audit whether the hard disk password has been set. Select from the following. - **Auditing** - **Audit Notebook only** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**

OS

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
Operation System	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Support Status	Audit whether the operating system being used is the supporting OS (SP Included). Select from the following items.	Unable to process automatically	**Auditing**	**Auditing**

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
		- **Auditing** - **Not Auditing** - **Display Only**			
Windows Update Program	**Installation Status**	Audit whether all security patches have been installed. Select from the following. - **Auditing** - **Not Auditing** - **Display Only**	Install security patches when it is set to audit	**Auditing**	**Not Auditing**
Logon Status	**Settings of Automatic Logon**	Audit whether automatic logon is disabled. Select from the following. - **Auditing** - **Not Auditing**	Set to disabled	**Auditing**	**Auditing**
	Whether to display the Welcome Screen	Audit whether the Welcome screen is not displayed. Select from the following. - **Auditing** - **Not Auditing**	Set to not displayed	**Auditing**	**Auditing**
	Whether to display the Last User Name	Audit whether the last logon user is not displayed on the logon window. Select from the following. - **Auditing** - **Not Auditing**	Set to not displayed	**Auditing**	**Auditing**
Windows Account	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Guest Security	Audit whether the Guest account is disabled and whether a proper password has been set if it is enabled. (Note 1) Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
Windows Security Information	**Settings of Windows Update (Automatic Update)**	Audit whether the setting of Windows Update is automatic update. Select from the following. - **Auditing**	Set to automatic update	**Not Auditing**	**Not Auditing**

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
		- **Not Auditing**			
	Settings of User Account Control (UAC)	Audit whether UAC (User Account Control) is enabled or not. Select from the following. - **Auditing** - **Not Auditing**	Set to enabled	**Auditing**	**Auditing**
Shared Folder	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Setup Status	Audit to ensure the shared folder with redundant authority is not set for all users (Everyone account). Select from the following. - **Any access is not allowed is OK** - **Read-only is OK** - **Not Auditing**	Unable to process automatically	**It is OK when read only**	**It is OK when read only**
Screen saver	**Password Protection on Wakeup**	Audit whether it is required to enter a password when restoring from standby. Select from the following. - **Auditing** - **Not Auditing**	Set to enabled	**Auditing**	**Auditing**
Password Policy	**Set Complicated Password Required**	Audit whether **Password should satisfy required complexity** is enabled in **Password Policy** of Windows group policy. (Note 2) Select from the following. - **Auditing** - **Not Auditing**	Set to enabled	**Not Auditing**	**Not Auditing**

Note 1) In **Guest Security**, audit whether a simple password is used through trying to enter the logon password.

Therefore, according to the system settings, the failed change of password for the user to be audited will be recorded in the event log. In addition, when performing the Lockout setting of account in the group policy of Windows, make sure the execute one of the following processing. When this processing is not executed, the Guest account will be locked out due to the auditing function.

- The lockout of account over 5 times has been set in the group policy of Windows.
- Set not to audit password of Guest account using the CustomPolicy.exe command.

Note 2) When **Set Complicated Password Required** is set as auditing item, auditing and processing will be performed for the group policy of Windows.

Even if the password currently used cannot meet the requirement of complexity, if it has been defined in the group policy of Windows, it is still OK. After processing has been executed and the password has been modified to the one that does not meet the requirement of complexity, Windows will require the password to meet complexity requirement.

In addition, in the following edition of Windows, since group policy function is not provided, even if it is set to **Auditing**, auditing and processing will not be performed.

- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows 7 Home Premium
- Windows 8 (except for Windows 8 Pro and Windows 8 Enterprise)

Software

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
Firewall	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Setup Status	Audit whether the setting of firewall is enabled. Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
Encrypted Software	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Installation Status	Audit whether the encryption software has been installed. Select from the following. - **Auditing** - **Not Auditing** When **Auditing** is selected, check the name of encryption software to be audited. (Note 1)	Unable to process automatically	**Auditing**	**Auditing**
Anti-Virus Software	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Installation Status	Audit whether anti-virus software has been installed. Select from the following. - **Auditing** - **Not Auditing** When **Auditing** is selected, check the name of anti-virus software to be audited.(Note 2)	Unable to process automatically	**Auditing**	**Auditing**

Item	Details	Description	Value Set at Auto-processing	Initial Value	
				Security of PC	Security of Server
	Virus Definition Status	Audit whether the virus pattern is appropriate in security. Specify the number of generations allowed for virus pattern. Select from the following. - **OK within X generations** - **Not Auditing** * The selectable range is within 1~10 generations.	Unable to process automatically	**OK within 10 generations**	**OK within 10 generations**
	Real-time Scan Status	Audit whether the real-time scan has been set. Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
	Scheduled Scan Status	Audit the scheduled scan has been set and has been executed in a week. Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
	Scan Scope	Audit whether all files are taken as scan target. Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**
Prohibited Software	**Installation Status**	Audit whether the prohibition software has been installed. Select from the following. - **Auditing** - **Not Auditing** When **Auditing** is selected, check the name of prohibition software to be audited. (Note 3)	Delete the prohibition software	**Auditing**	**Auditing**

Note 1) When selecting the encryption software to audit, it is required to select the encryption software under **Software** of **Environment Setup** > **Auditing Software** in advance.

Example) **Software dictionary** > **Software** > **Control Break International**
Software dictionary > **Software** > **Fujitsu BSC** > **FENCE** > **Pro**

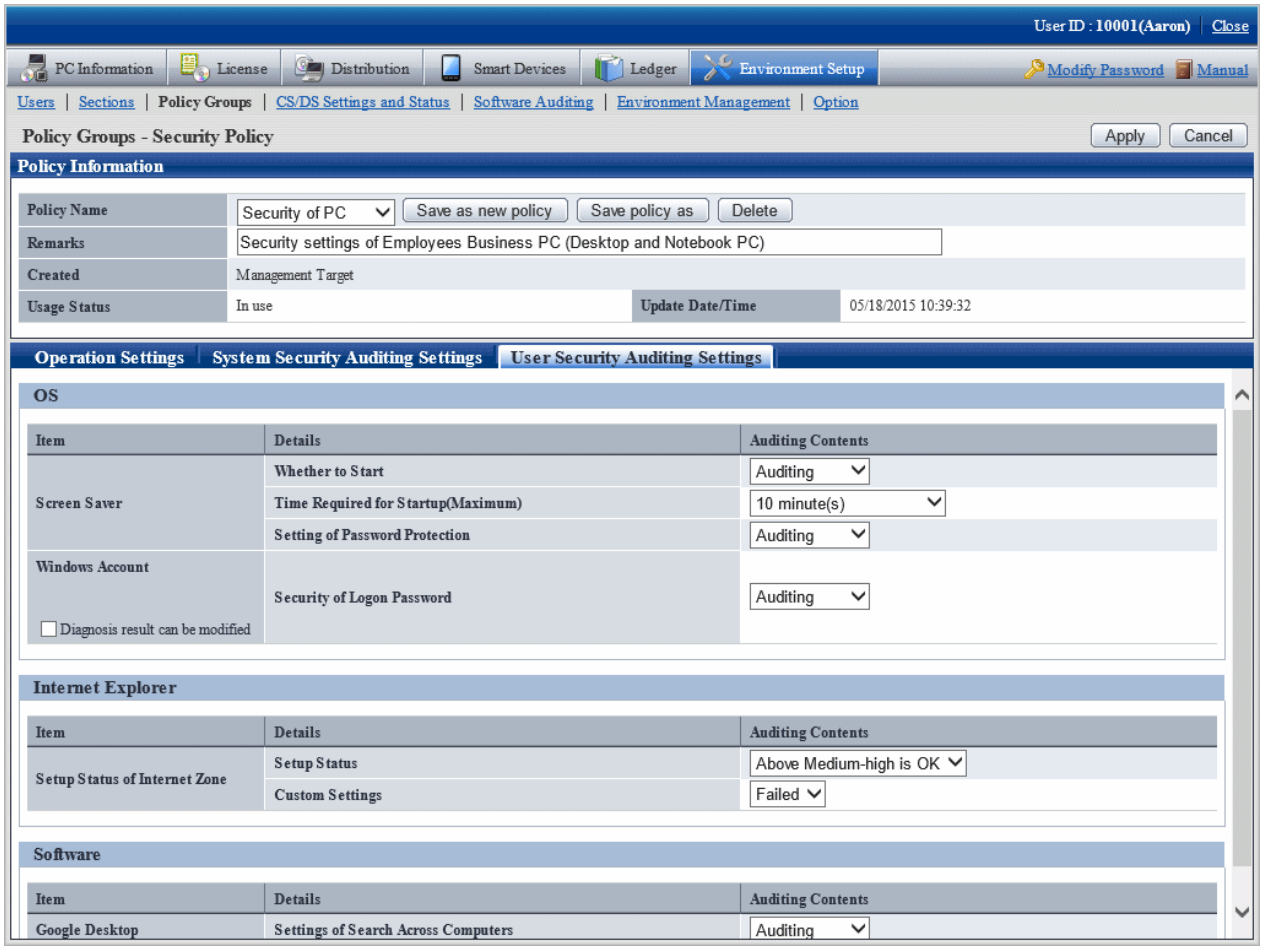
Note 2) When selecting the anti-virus software to audit, it is required to select the anti-virus software under **Software** of **Environment Setup** > **Auditing Software** in advance.

Example) **Software dictionary** > **Software** > **TrendMicro**
Software dictionary > **Software** > **Symantec**
Software dictionary > **Software** > **Network Associates**

Note 3) When selecting the prohibition software to audit, it is required to select the prohibition software under **Software** of **Environment Setup** > **Auditing Software** in advance.

8. Set the item of user security auditing.

   Click the **User Security Auditing Settings** tab, and the following window will be displayed.



   Set the following auditing items.

   In addition, the so-called "Value at Auto-processing" refers to the value that is automatically assigned by Systemwalker Desktop Keeper when the following settings/operations are performed.

- When **Yes** is selected in **Automatic Processing of PC** of the **Operation Settings** tab
- When the **Process** button is pressed in the **Diagnosis result of operation settings** of CT

OS

Item	Details	Description	Value at Auto-processing	Initial Value	
				Security of PC	Security of Server
Screen saver	**Whether to Start**	Audit whether it has been set to start screen saver. Select from the following.	Set to start	**Auditing**	**Auditing**

Item	Details	Description	Value at Auto-processing	Initial Value	
				Security of PC	Security of Server
		- **Auditing** - **Not Auditing**			
	Time Required for Startup(Maximum)	Audit whether the screen saver is started after an appropriate waiting time. - ***n* minute(s)** - **Not Auditing** * The selectable range is 1~60 minutes.	Brightness Setting of Display	**10 minutes**	**10 minutes**
	Setting of Password Protection	Audit whether the setting of password protection is enabled. Select from the following. - **Auditing** - **Not Auditing**	Set to enabled	**Auditing**	**Auditing**
Windows Account	**Diagnosis result can be modified**	Select it when it is expected to set the diagnosis result to correctable.	-	-	-
	Security of Logon Password	Audit whether an appropriate password has been set for the logon user. (Note) Select from the following. - **Auditing** - **Not Auditing**	Unable to process automatically	**Auditing**	**Auditing**

Note) In **Security of Logon Password**, audit whether a simple password is used through trying to enter the logon password.

Therefore, according to the system settings, the failed change of password for the user to be audited will be recorded in the event log. In addition, when performing the Lockout setting of account in group policy, make sure the execute one of the following processing. When this processing is not executed, the account will be locked out due to the auditing function.

The lockout of account over 5 times has been set in the group policy.
Set **Not Auditing** in **Security of Logon Password**, and set **Auditing** in **Specify Complex Password or Not**.

Internet Explorer

Item	Details	Description	Value at Auto-processing	Initial Value	
				Security of PC	Security of Server
Setup Status of Internet Zone	**Setup Status**	Audit whether the security zone of Internet Explorer has been set correctly. Select from the following. - **Above High is OK**	Brightness Setting of Display	**Medium-high or above is OK**	**Medium-high or above is OK**

Item	Details	Description	Value at Auto-processing	Initial Value	
				Security of PC	Security of Server
		- **Above Medium-high is OK** - **Above Medium is OK** - **Above Medium-low is OK** - **Not Auditing**			
	Custom Settings	Set the auditing result when the security zone is customized. Select from the following. - **Failed** - **OK**	When **Failed** is selected, set to the value defined in **Setup Status**	Auditing	Auditing

Software

Item	Details	Description	Value at Auto-processing	Initial Value	
				Security of PC	Security of Server
Google Desktop	**Settings of Search Across Computers**	Audit whether the "Data Search on Multiple Computers" function is disabled. Select from the following. - **Auditing** - **Not Auditing**	Set to disabled	**Auditing**	**Auditing**

1. To save the settings, click the **Apply** button.

   To save the settings as another setting pattern, click the **Save As** button.

Point

The file that has been detected as prohibition software and deleted by Systemwalker Desktop Patrol can be restored by the following command.

1. Display the list of deleted files.

   <DTP installation directory>\invcl\bin\prestore.exe -list

```
No Date Deleted Restored file
---+--------------------+--------------------------
1 2009/06/18 12:00:00 C:\ BitTorrent \BitTorrent.exe
2 2009/06/18 14:00:00 C:\ eD2k\eD2k.exe
```

2. Specify the file to be restored from the list and perform restoration.

   <DTP installation directory>\invcl\bin\prestore.exe -rest 2

   The specified file will be restored.

Note

About auto-processing

In the Active Directory environment, the setting of Windows group policy is effective, so it may not be able to process automatically sometimes. Modify the setting of Windows group policy to not audit for the items set in Windows group policy.

4.3 How to Operate Diagnosis result window of operation settings

This section describes how to operate the Diagnosis result window of operation settings.

4.3.1 Structure of Diagnosis result window of operation settings

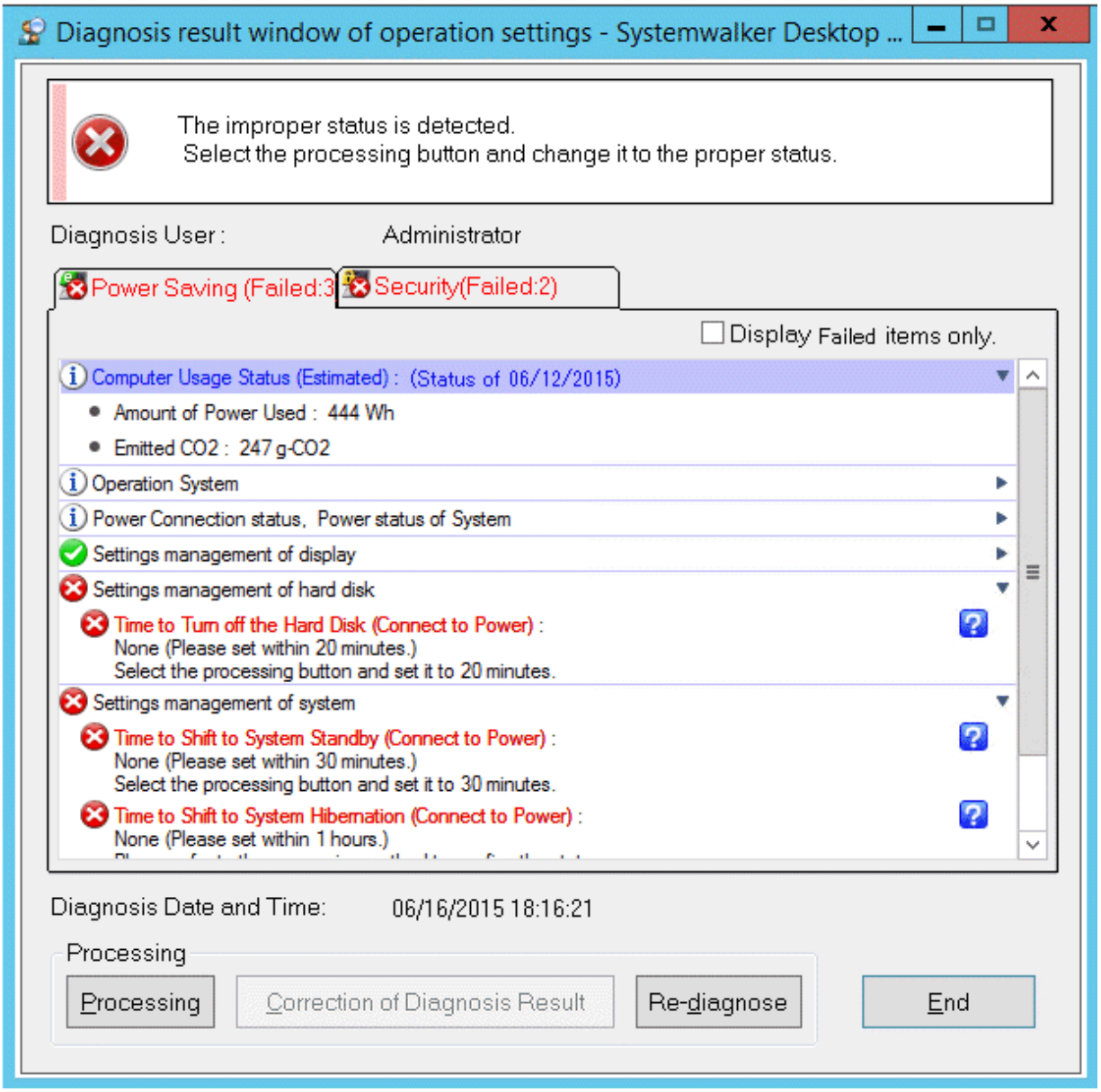
The following diagnosis result will be displayed in the Diagnosis result window of operation settings.

- Diagnosis result of power saving setting (note)
- Diagnosis result of security setting (note)

Note) The one that is set to not display in policy will not be displayed.

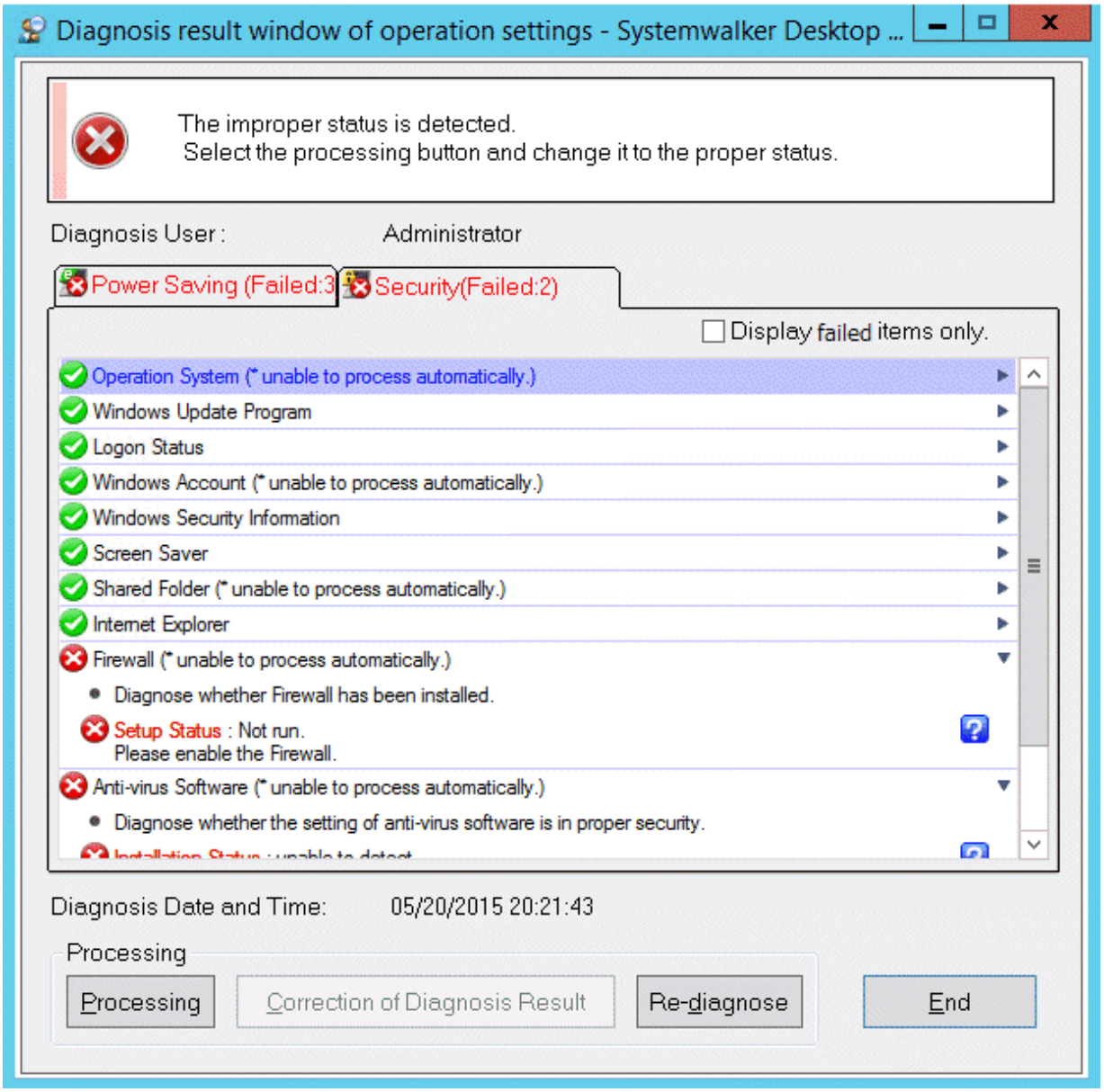
Diagnosis result of power saving

After the **Power Saving** tab is selected, the diagnosis result of power saving setting will be displayed.



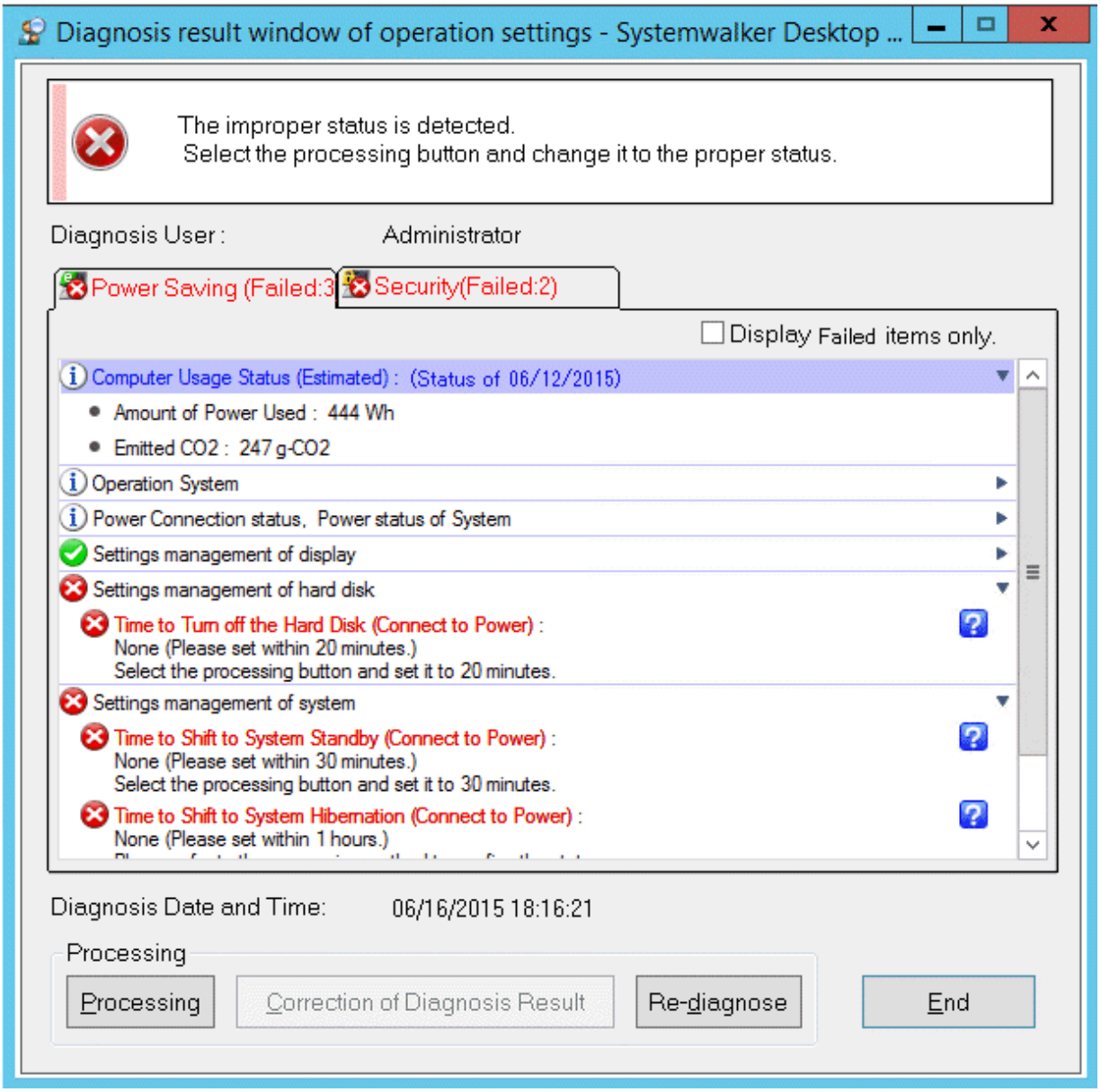
Diagnosis result of security setting

After the **Security** tab is selected, the diagnosis result of security setting will be displayed.



4.3.1.1 Structure of Diagnosis Result Window of Power Saving

After the **Power Saving** tab is selected, the diagnosis result window of operational settings is shown as follows.



Icon

The meaning of icon is as follows.

Display	Meaning
	Audit OK.
	Audit failed.
	Unable to collect information.
	Information.
	Display help.

Diagnosis result

After extracting the items, the detailed diagnosis result will be displayed for diagnosis content. The displayed content is shown below.

In addition, in case of PC with battery, the set value under both the conditions of connecting to power and using battery will be displayed. Only one value will be displayed for PC without battery.

Computer Usage Status

Item	Diagnosis Content
Computer Usage status (Estimated)	The usage condition of the computer being used will be displayed. - Amount of Power Used - Emitted CO2 This item does not diagnose audit OK and audit failed.

Operating system

Item	Diagnosis Content
Operating System	The operating system being used will be displayed. This item does not diagnose audit OK and audit failed.

Power Connection status, Power status of System

Item	Diagnosis Content
Current power status	The following status will be displayed. - Whether it is operating using battery - Whether it is operating by connecting to power This item does not diagnose audit OK and audit failed.
Display Information	Display the information of display connected to the PC. - Whether it uses CRT display - Whether it uses liquid crystal display This item does not diagnose audit OK and audit failed.

Setting management of display

Item	Diagnosis Content
Time to Cut off the Power of Monitor	The diagnosis result of the time till the power of display is cut off will be displayed. The threshold value (time) that is larger than the one set by administrator cannot be set. When the threshold value (time) is set to 0, it will not be displayed in the Diagnosis result window of operation settings as the item not to be audited. - When OK <Collection Result> minutes later Example) 20 minutes later - When failed

Item	Diagnosis Content
	<Collection Result> (set a value within <Threshold Value> minutes) Example) 300 minutes (set a value within 20 minutes)
Brightness settings of display	The auditing result of brightness settings of display will be displayed. When the set value is larger than the threshold value set by the administrator (10 stages), the auditing result will be failed. This item is only audited under Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

Setting management of hard disk

Item	Diagnosis Content
Time to Turn off the Hard Disk	Diagnose the time till the power of hard disk is cut off. When the set time is larger than the threshold value (time) set by the administrator, the auditing result will be failed.

Setting management of system

Item	Diagnosis Content
Time to Shift to System Standby	Diagnose the time till the system shifts to standby status. When the set time is larger than the threshold value (time) set by the administrator, the auditing result will be failed.
Time to Shift to System Hibernation	Diagnose the time till the system shifts to sleep status. When the set time is larger than the threshold value (time) set by the administrator, the auditing result will be failed.
Hyper sleep	Diagnose whether the setting allows Hyper sleep. When it is different from the threshold value (ON/OFF) set by the administrator, the auditing result will be failed. This item is only audited under Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

Setting management of processor

Item	Diagnosis Content
Power management of processor	The diagnosis result of PC processor will be displayed. In case of the processor that does not support SpeedStep, it is displayed as information. (not supported by this system). The following content will be displayed as information. - The value set in the operation of the smallest processor (%) Audit OK: The value within the threshold is set Audit failed: The value beyond the threshold is set

Item	Diagnosis Content
	- The value set in the operation of the largest processor (%) Audit OK: The value within the threshold is set Audit failed: The value beyond the threshold is set This item is only audited under Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

Setting management of USB

Item	Diagnosis Content
Settings of Selective Suspension of USB	The auditing result of the setting selected in Settings of Selective Suspension of USB will be displayed. When it is different from the threshold value (enabled/disabled) set by the administrator, the auditing result will be failed. This item is only audited under Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

Display failed items only check box

After this item is selected, the displayed content can be refined to displaying failed items only. The selected state will still effective even if the window is closed.

In addition, the following item has nothing to do with the check box and will be displayed for sure.

- **Information**

This check box can be enabled/disabled according to policy.

Processing button

For the items audited as failed, they will be processed in batch by Systemwalker Desktop Patrol.

Correction of Diagnosis Result button

This button cannot be used in the diagnosis result of power saving.

Re-diagnose button

Execute the diagnosis of operational configuration again and update to the latest information.

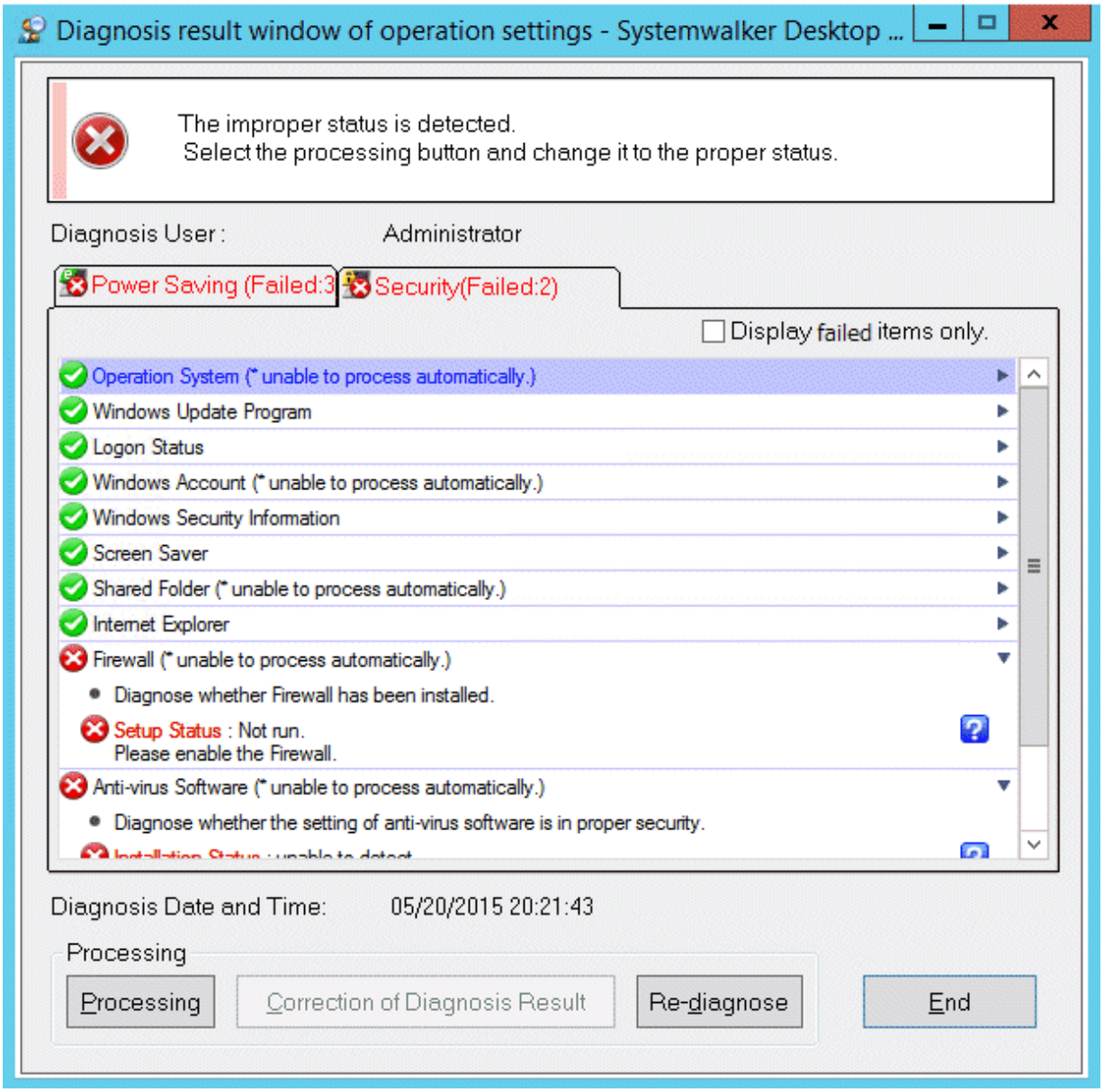
End button

Close the Diagnosis result window of operation settings.

According to the setting of the administrator, the **End** button is grayed out sometimes. At this time, after performing the processing of power saving settings to change the status to audit OK, the **End** button can be selected.

4.3.1.2 Structure of Security Diagnosis Result Window

The Diagnosis result window of operation settings when the **Security** tab is selected is shown as follows.



Icon

The meaning of icon is as follows.

Display	Meaning
	Audit OK.
	Audit failed.
	Unable to collect information.
	Display help.

Diagnosis result

After extracting the items, the detailed diagnosis result will be displayed for diagnosis content. The displayed content is shown below.

Operation System

Item	Diagnosis Content
Support Status	Diagnose whether the operating system being used is appropriate on security. Except the following operating systems and service packs, the auditing result will be failed. - Windows Vista(R) SP2 or later - Windows(R) 7 SP1 or later - Windows(R) 8 - Windows Server(R) 2008 SP1 or later - Windows Server(R) 2008 R2 SP2 or later - Windows Server(R) 2012

Windows Update Program

Item	Diagnosis Content
Application Status	Diagnose the application status of Windows update program. Audit whether all security patches have been installed. If the patch that is not installed exists, **Failed** will be displayed 7 days after it is detected. It will be displayed as OK within the 7 days. Other update programs can become auditing target through reflecting to the software dictionary manually.

Logon status

Item	Diagnosis Content
Use auto-logon	Diagnose whether the logon setting of Windows has been set to automatic logon. When it has been set to automatic logon, it will be audited as failed.
Display the last user ID	Diagnose whether to display the last user name. When the user name of last logon is displayed in the logon window, it will be audited as failed.

Windows Account

Item	Diagnosis Content
Security of Logon Account	Diagnose whether the Windows logon password for displaying the Diagnosis result window of operation settings has been set and whether the password that matches with the user name has been used. When the password is not set and when the user name and password are matched, it will be audited as failed.

Item	Diagnosis Content
Security of Guest	Diagnose if the password of Guest account has been set, and whether the account and password are matched. When Guest account is enabled, but password is not set. It will be audited as failed. (Note 1) When Guest account is OFF, it will be audited as failed as well. When Guest account is disabled, it will be audited as failed as well.

Note 1) It is allowed to only audit whether the Guest account is enabled without auditing the password.
Use the CustomPolicy.exe (Change of policy for customized settings) command to change the auditing method. For how to use CusttomPolicy.exe, refer to *Systemwalker Desktop Patrol Reference Manual*.

Password policy

Item	Diagnosis Content
Set Complicated Password Required	In password policy, diagnose whether **Password satisfies required complexity** is enabled or not. When **Password satisfies required complexity** is disabled, it is displayed as "It is the setting that does not require complex password.". When it is not audited, this item will not be displayed.

Windows Security Information

Item	Diagnosis Content
Windows Update(Automatic Update) Settings	Diagnose whether Windows Update is disabled. The default is auditing as failed when **disabled** only. The following setting will be audited as OK. - **Automatic** (recommended) - **Download update automatically and execute installation manually** - **Only notify updates but not download automatically or execute installation**
UAC(User Account Control) Settings	Diagnose whether the setting of user account control (UAC) is enabled. When the user account control is set to disabled, it will be audited as failed. This item is only diagnosed in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012. In other OS, this item will not be displayed.

Screen Saver

Item	Diagnosis Content
Setting Status	Diagnose whether the screen saver is set to start.

Item	Diagnosis Content
	When the screen saver is not started, it will be audited as failed. **Status Information** of **Startup Time (seconds)**, **Release Password** will not be displayed.
The waiting time for the startup of screensaver startup is set to	Diagnose whether the startup time of screen saver is within the allowed range specified by the administrator. In default, when the value that is larger than 600 seconds (10 minutes) is set, it will be audited as failed. This item will not be displayed if setting not to start screen saver.
Settings of Password Protection	Diagnose whether the password to recover from screen saver has been set. When the password to recover from screen saver is not set, it will be audited as failed. This item will not be displayed if setting not to start screen saver.
Password to Restore from Standby	Diagnose whether a password is required when restoring from the standby status. When password is not required for restoring from standby, it will be audited as failed.

Shared Folder

Item	Diagnosis Content
Setting status	Diagnose whether the setting of shared folder is appropriate on security. - **Status** The auditing result will be displayed. In default status, when the shared folder with read only (r) or read and write (w) authority that is set to Everyone exists, it will be audited as failed. - **Shared folder** Display the shared folder that has been set. - **Authority** Display the authority that is set to Everyone.

Internet Explorer

Item	Diagnosis Content
The setting status of security zone	Diagnose the security zone of Internet Explorer. One of the following will be displayed in information. - **Low** - **Medium-Low** - **Medium** - **Medium-High** - **High**

Item	Diagnosis Content
	- **Customized** When the setting is lower than the default **Medium**, it will be audited as failed. In case of **Customized**, it can be diagnosed as OK/failed according to settings. In addition, the version of Internet Explorer being used and the update version will be displayed.

Firewall

Item	Diagnosis Content
Setting Status	Diagnose the setting status of firewall. When the set firewall is being operated, it will be audited as OK. When the firewall is not set, it will be audited as failed. The audited firewall is Windows firewall, and the personal firewall of anti-virus software.

BIOS hard disk password

Item	Diagnosis Content
Boot password	Diagnose whether the startup password of BIOS has been set (password used by administrator). When password is not set, it will be audited as failed. According to settings, it is allowed not to audit desktop computer. At this time, this item will be not displayed.
Setting password	Diagnose whether the setting password of BIOS has been set (password used by user). When password is not set, it will be audited as failed. According to settings, it is allowed not to audit desktop computer. At this time, this item will be not displayed.
Hard disk password	Diagnose whether the hard disk password has been set. When password is not set, it will be audited as failed. PCs for which the hard disk password cannot be set will be judged as having the password **Not set**, and will be audited as failed. According to settings, it is allowed not to audit desktop computer. At this time, this item will be not displayed.

Anti-virus Software

Item	Diagnosis Content
Installation status	Diagnose whether the anti-virus software has been installed. When not installed, it will be failed.

Item	Diagnosis Content
	For supported anti-virus software, refer to *Systemwalker Desktop Patrol User's Guide*. *It is required to set for searching anti-virus software.
Status of Virus Pattern	The diagnosis result of whether the virus pattern is within the set generations will be displayed.
Status of scheduled scan	Whether the scheduled scan has been set in anti-virus software and the diagnosis result of whether the scheduled scan has been executed will be displayed. When scheduled scan is not set or the scheduled scan is not executed within the set period, it will be audited as failed.
Settings of real-time scan	The diagnosis result of anti-virus software set in real-time scan (Auto-Protect) will be displayed. When anti-virus software does not exist in real-time scan, it will be audited as failed.
Target range of scanning	Audit the scan target file set in the anti-virus software. When none of the file is the target for scanning, it will be audited as failed.

Encryption Software

Item	Diagnosis Content
Installation status	Diagnose whether the encryption software has been installed. The following products will be audited by default. - SafeBoot - FencePro Other products can be defined as auditing target in the user definition of software dictionary. When encryption software is not installed, it will be audited as failed.

Status of Google desktop

Item	Diagnosis Content
Setting of data search on multiple computers	Diagnose whether the "Data Search on Multiple Computers" function is disabled. When the "Data Search on Multiple Computers" function is enabled, it will be audited as failed. When Google Desktop is not installed, it will be displayed as **Not installed**.

Prohibition Software

Item	Diagnosis Content
Installation Status	Diagnose whether the prohibition software has been installed. - Prohibition software

Item	Diagnosis Content
	Display the prohibition software name that has been detected. When not detected, it will be displayed as **No Problem**.

Display failed items only check box

After this item is selected, the displayed content can be refined to displaying failed items only. The selected state will still effective even if the window is closed.

This check box can be enabled/disabled according to policy.

Processing button

For the items audited as failed, they will be processed in batch by Systemwalker Desktop Patrol.

For items that cannot be executed by the processing button, **Unable to Auto-Processing** will be displayed.

Correction of Diagnosis Result button

Modify the security diagnosis result to OK manually.

For details, refer to "Correction of diagnosis result".

Re-diagnose button

Execute the diagnosis of operational configuration again and update to the latest information.

End button

Close the Diagnosis result window of operation settings.

According to the setting of the administrator, the **End** button is grayed out sometimes. At this time, after performing the processing of power saving settings to change the status to audit OK, the **End** button can be selected.

4.3.2 Operate Diagnosis Result Window of Power Saving

This section describes how to operate the diagnosis window (auditing of power saving) of operational configuration.

1. On CT, click **Start** > **Systemwalker Desktop Patrol CT** > **Diagnosis result window of operation settings**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Diagnosis of Operational Configuration**.

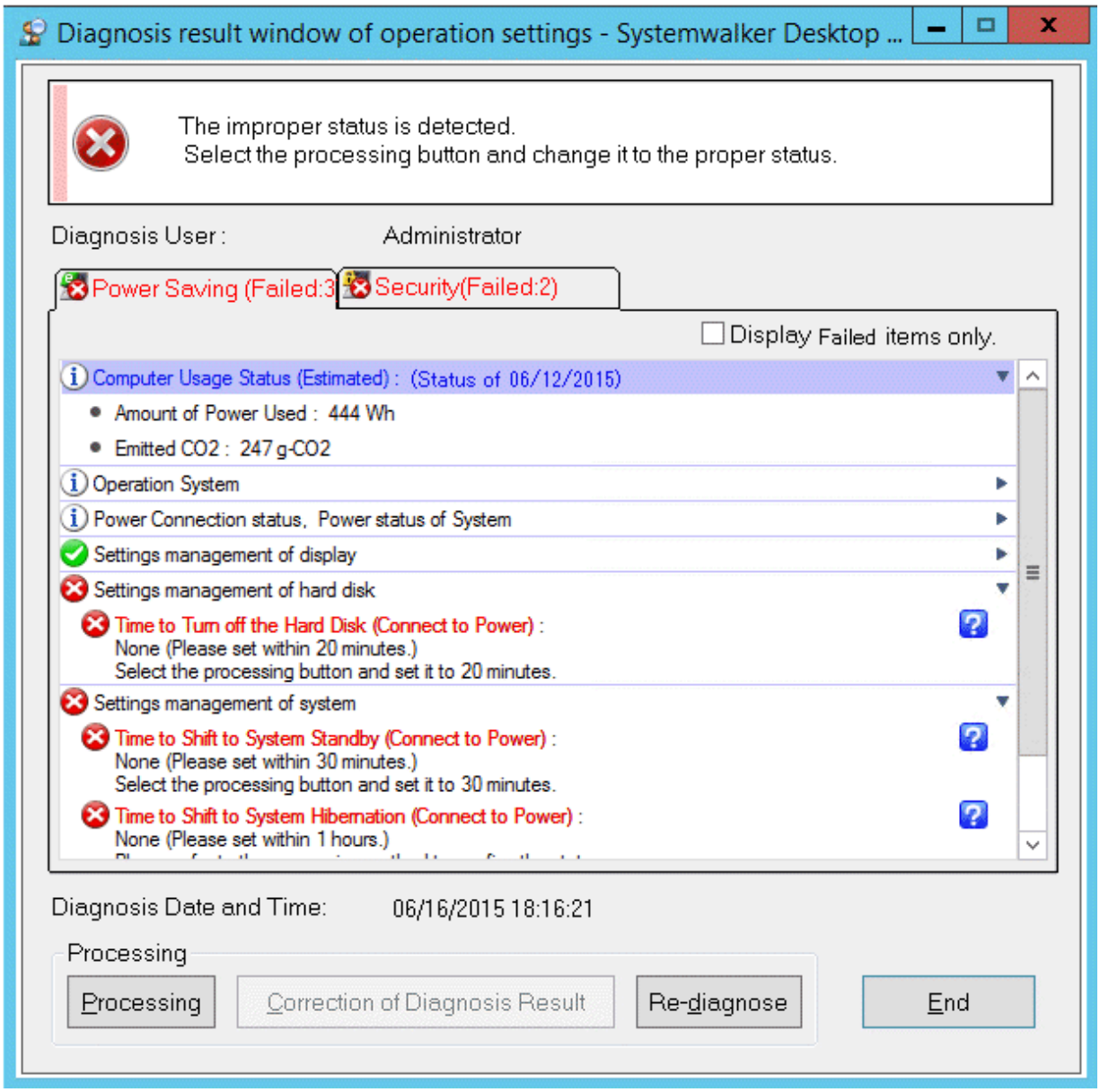
   The **Diagnosis Result window of Operation settings** window will be displayed.

   In addition, according to the setting of client policy, when setting to display the Diagnosis result window of operation settings at logon of Windows, it will be displayed at logon to Windows.

2. When multiple tabs are displayed, selected the **Power Saving** tab.

3. Extend the line that is displayed as the icon of audit failed.

   The failed content will be displayed in the tree view.



4. Perform processing of power saving settings.

   Click the **Processing** button and the processing will be started automatically.

5. Click the **Re-diagnose** button.

   The diagnosis result of power saving will be updated to the latest information.

6. Confirm the status icon becomes "Audit OK".

4.3.3 Operate Diagnosis Result Window of Security

This section describes how to operate the Diagnosis result window of operation settings (security auditing).

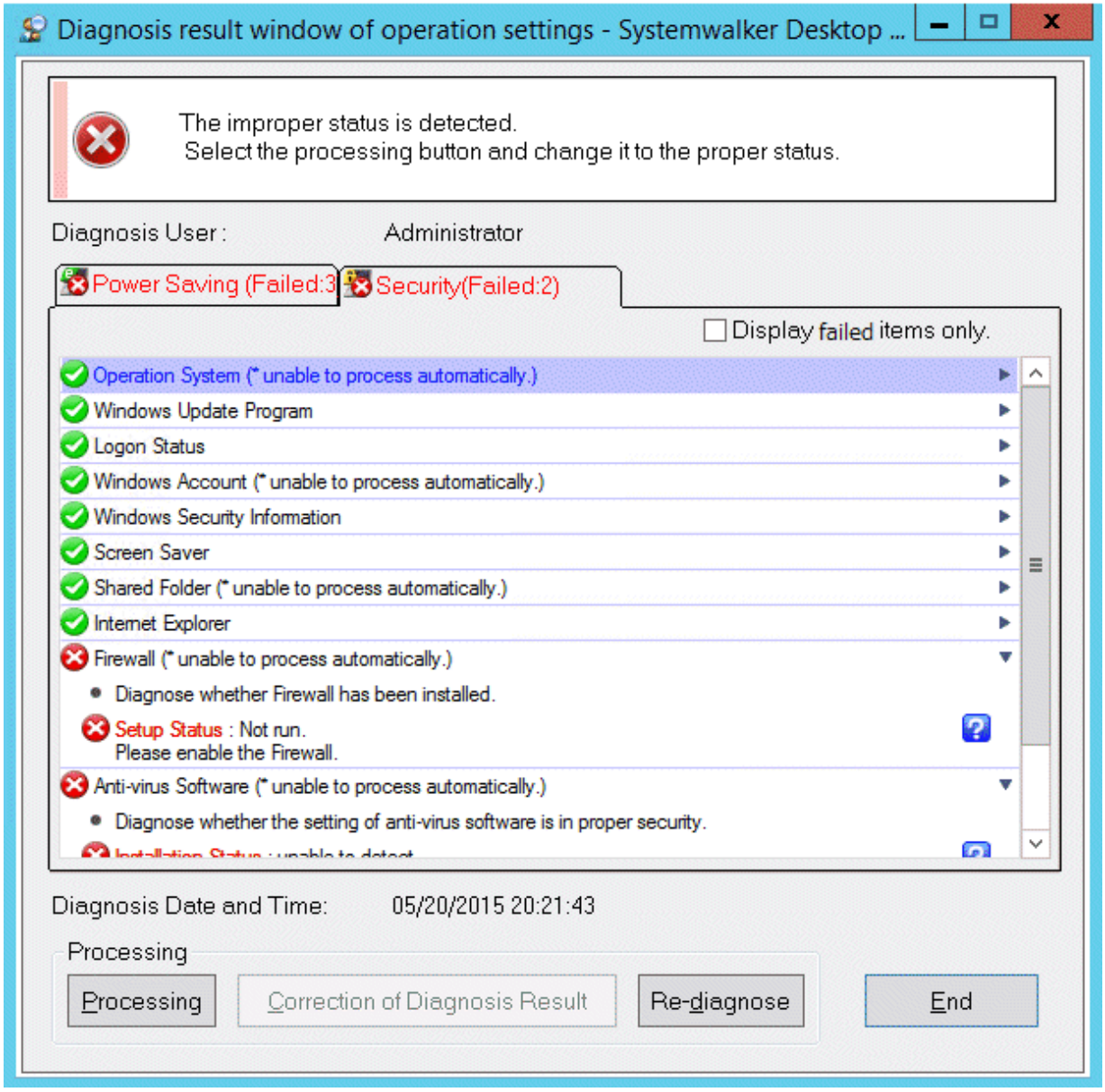
1. On CT, click **Start** > **Systemwalker Desktop Patrol CT** > **Diagnosis result window of operation settings**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Diagnosis of Operational Configuration**.

   The **Diagnosis result of operation settings** window will be displayed.

In addition, according to the setting of client policy, when setting to display the Diagnosis result window of operation settings at logon of Windows, it will be displayed at logon to Windows.

2. When multiple tabs are displayed, select the **Security** tab.
3. Extend the line that is displayed as the icon of audit failed.

   The failed content will be displayed in the tree view.



4. Perform the processing of security settings.

   Click the **Processing** button, the processing will be started automatically. When the Windows update program contains failed items, security patch will be installed. When installing security patches, the patch installation window will be displayed sometimes according to settings.

   Click the **Processing** button, and **unable to process automatically** will be displayed in the items that cannot be processed.

5. Click the **Re-diagnose** button.

   The security diagnosis result will be updated to the latest information.

6. Confirm whether the status icon becomes "Audit OK".

Correction of diagnosis result

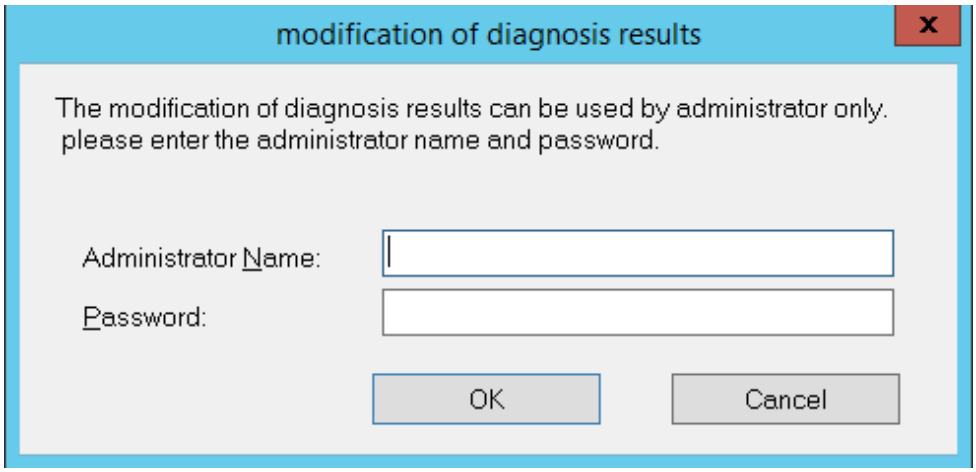
The diagnosis result of security can be corrected to "Audit OK" manually.

The procedure is as follows.

1. Click the **Correction of Diagnosis Result** button.

   The window for entering administrator name and password will be displayed.

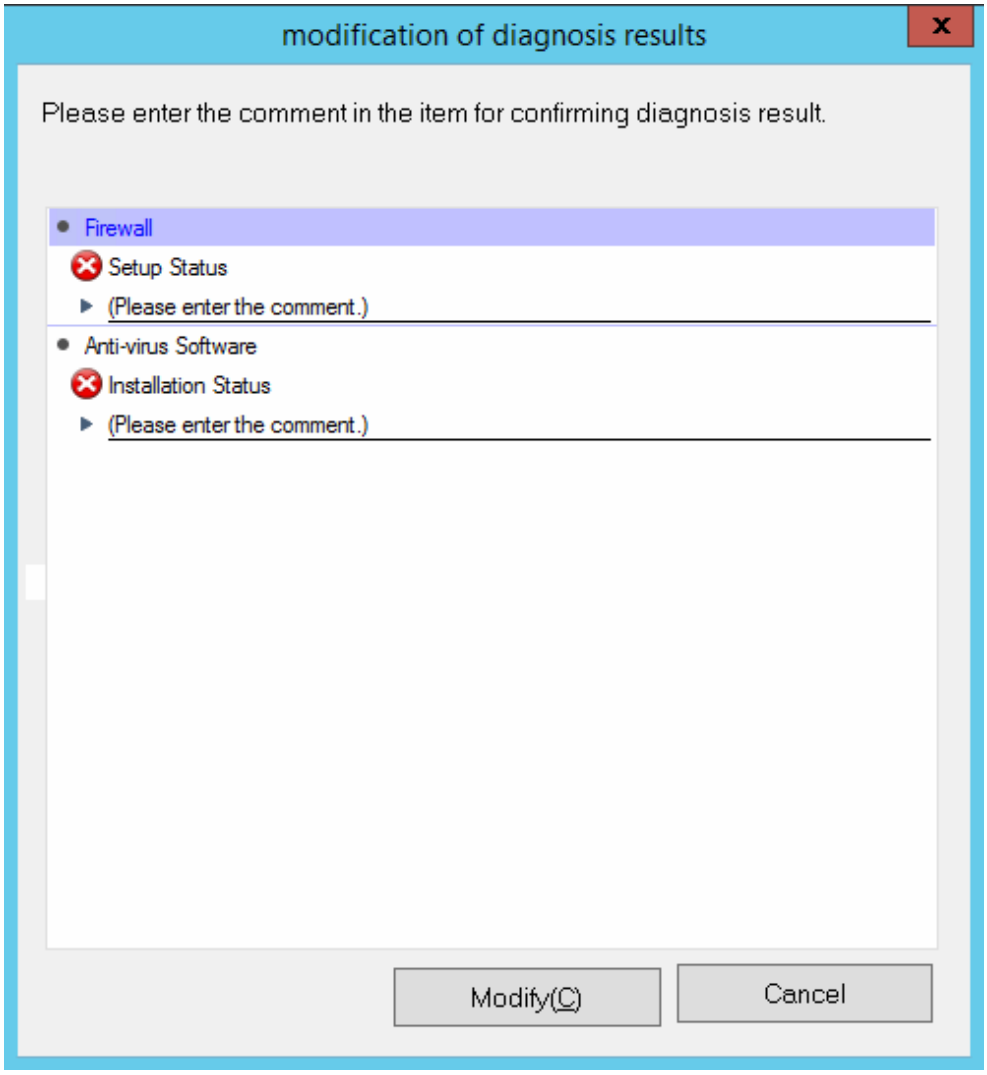
   (According setting, password may not be required.)



Item	Content
Administrator Name	Enter the name of administrator who corrects the diagnosis result. Up to 64 characters of "multi-byte characters, single-byte alphanumeric characters, single-byte space, special symbols (-@, ()[]{}<>:;/)" can be entered.
Password	Enter the set password.

2. Enter the administrator name and password.

   When the password matches, the following window will be displayed.



   Enter the comment for the category to correct diagnosis result to OK.

   For the category without commend being entered, the diagnosis result cannot be modified to OK.

Item	Content
Comment Input Line	Enter the comment. Up to 128 characters of "multi-byte characters, single-byte alphanumeric characters, single-byte space, special symbols (-@, ()[]{}<>:;/)" can be entered.
Modify button	Correct diagnosis result.
Cancel button	Cancel the correction of diagnosis result.

3. Click the **Modify** button.

   The diagnosis result will be modified.

4. Confirm whether the diagnosis result becomes "Audit OK" in the Diagnosis result window of operation settings.

Point

To notify the latest security diagnosis result to the higher server, click **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Inventory Collection**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Inventory Collection**.

4.4 Confirm Status Window

Confirm the operation status of PC in the status window.

The status window is the main menu window displayed first after login to Systemwalker Desktop Patrol.

In the status window, the following operation status can be confirmed.

- 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

For details of the status window, refer to "3.2.11 Display Operation Status and Perform Operation Processing".

4.5 Confirm Report

Confirm the operational configuration of PC (auditing/controlling status of power saving settings, security settings) in report.

For procedure of report output, refer to "Chapter 13 Output Report".

Confirm the power saving setting status report

Confirm the power saving setting status report and confirm the status of PC that satisfies the power saving policy in the whole company, section unit and location unit.

For the sections with many problem PCs, problem can be confirmed from the detailed report.

Confirm the auditing report of power consumption volume

In the auditing report of power consumption volume, confirm the status/trend of power consumption in the whole company/section/location. Confirm the effect of power saving operation.

Confirm the security auditing report

Confirm the security auditing report and confirm the status of PC that satisfies security auditing policy in the whole company/section unit.

For the sections with many problem PCs .etc, problem can be confirmed from the detailed report.

For output content of security auditing report, refer to "13.5.3 Example of Outputting Security Auditing Status".

4.5.1 Procedure of Confirming Power Saving Setting Status Report

The power saving setting status report is for confirming the power saving setting status that has been set on each PC, determining the section and PC without power saving settings and taking resolution/improvements for the determined section and PC.

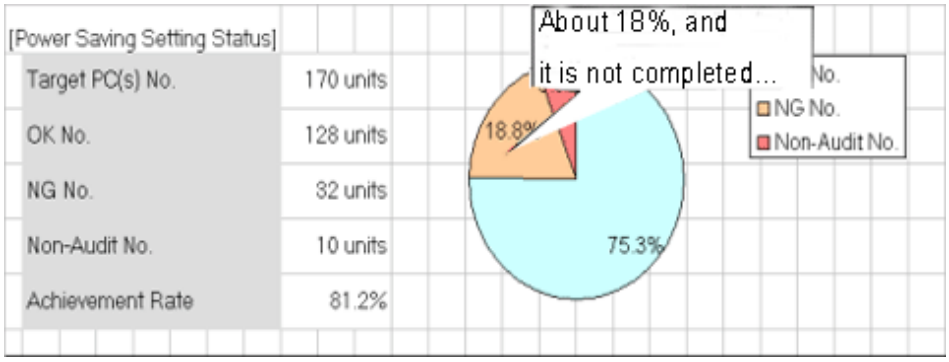
For overall description of the power saving setting status report, refer to "13.6.2 Example of Outputting Power Saving Setting Status".

The confirmation procedure is as follows.

1. Grasp the problem from the summary part.
   a. Grasp the overall status

      Confirm whether there is any problem in the power saving setting status as a whole.

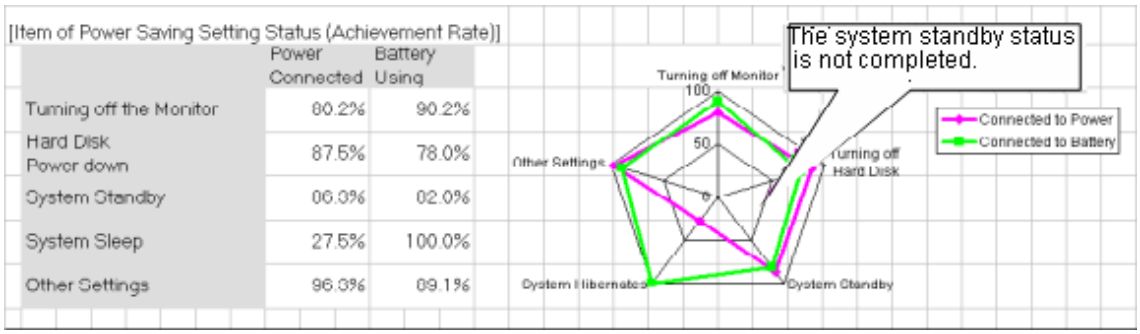
      Confirm [Power Saving Setting Status]. When the achievement rate is not 100%, resolution/improvement is required.



   b. Grasp problem

      Confirm what the problem is, whether there is problem in specific power saving setting items, whether there is problem in specific section/location.

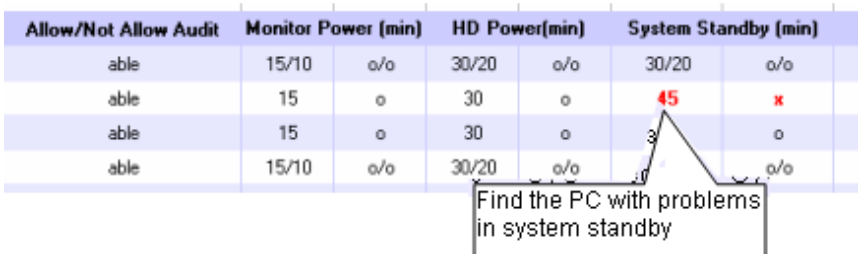
      Confirm [Item of Power Saving Setting Status], [Low achievement rates] , and "Setting Status List" sheets.



2. Grasp the PC with problems from the details part.
   a. Grasp the status of each PC

      For problems appeared in "b." of "1." above, check the details and confirm the PC with problems.

Confirm the [Details Part].



3. For problems confirmed in the report, perform resolution/improvement.

   For PC with problems, confirm the reason why the auditing result is "x" and perform improvement.

   The major reasons for the auditing result to be "x" are as follows.

   - The power saving setting is not set to "Processing"

     Resolution: Set the power saving setting to "Processing" and apply the power saving setting.

   - Intentionally modified by users

     Resolution: Confirm with the section administrator and user who is responsible for the PC.

   - Processing cannot be performed for some reasons (example: protected by another application .etc)

     Resolution: Confirm with the section administrator and user who is responsible for the PC.

4.5.2 Procedure of Confirming Auditing Report of Power Consumption

In the auditing report of power consumption, confirm whether the result of auditing/controlling power saving has been reflected in the result as power consumption. In addition, when it is not reflected in the result, confirm the problem and check whether the policy of power saving settings on each PC is correctly selected.

For overall description of auditing report of power consumption, refer to "13.7.3 Example of Outputting Power Consumption Status:

The confirmation procedure is as follows.

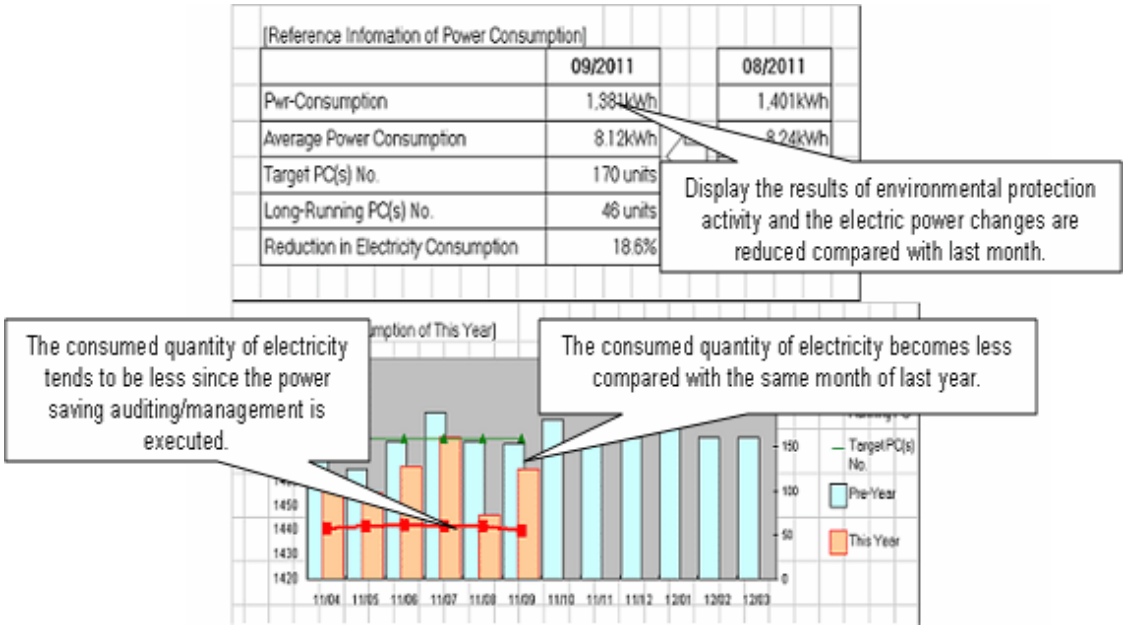
1. Confirm whether the auditing/controlling of power saving has been reflected in the result as power consumption.

   a. Grasp the situation till this month and till now

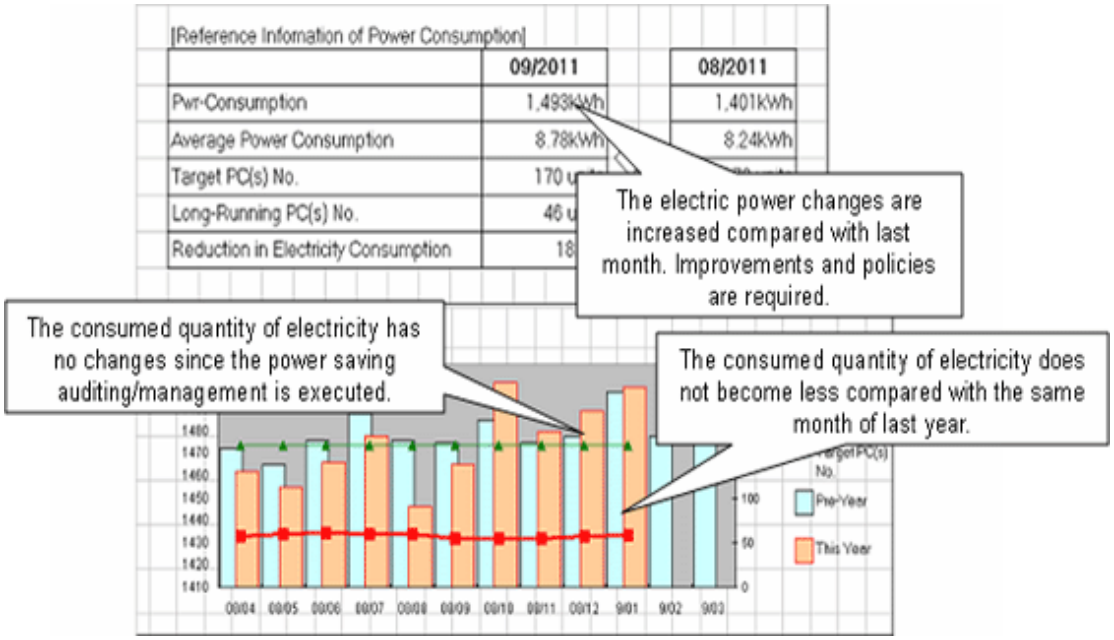
      Confirm the power consumption of that month, last month/one year.

      Confirm [Reference Information of Power Consumption], [Trend of Power Consumption of This Year].

Example) Case of reflecting the auditing/controlling of power saving as result

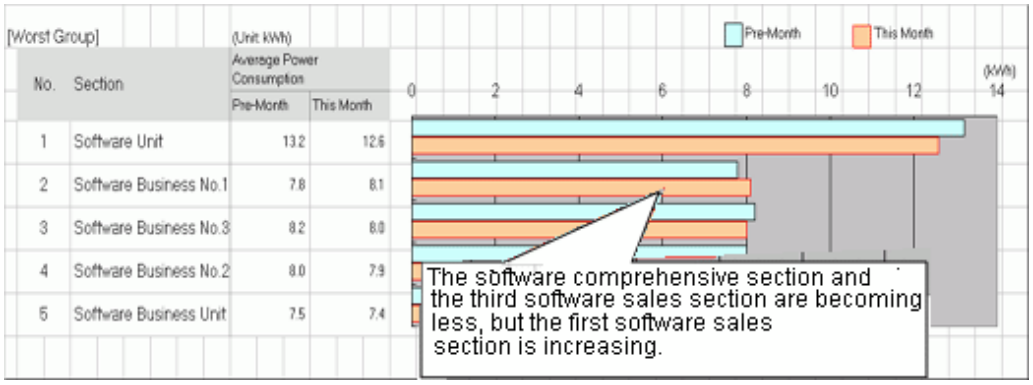


Example) Case of not reflecting the auditing/controlling of power saving as result



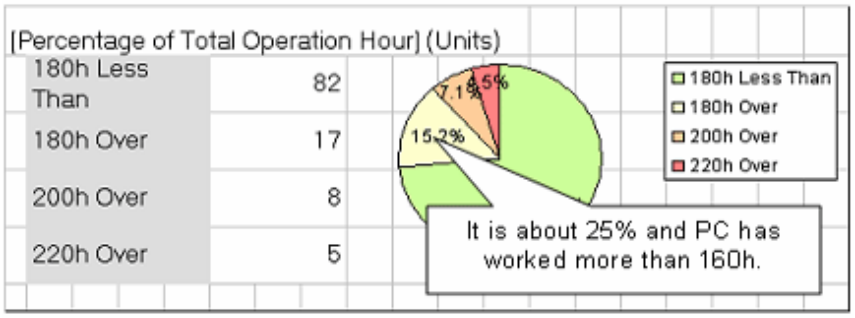
b. Confirm the group with low achievement rate of power consumption for each section/location

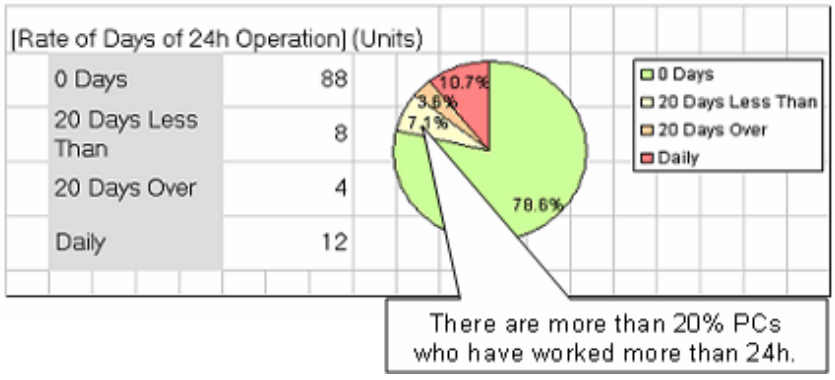
Confirm the section/location that has the highest power consumption on 1 PC in this month and last month.



c. Confirm power consumption for each section/location

Compare and confirm the power consumption on 1 PC in this month and last month and the volume of power consumption reduced from non power saving for each section/location.





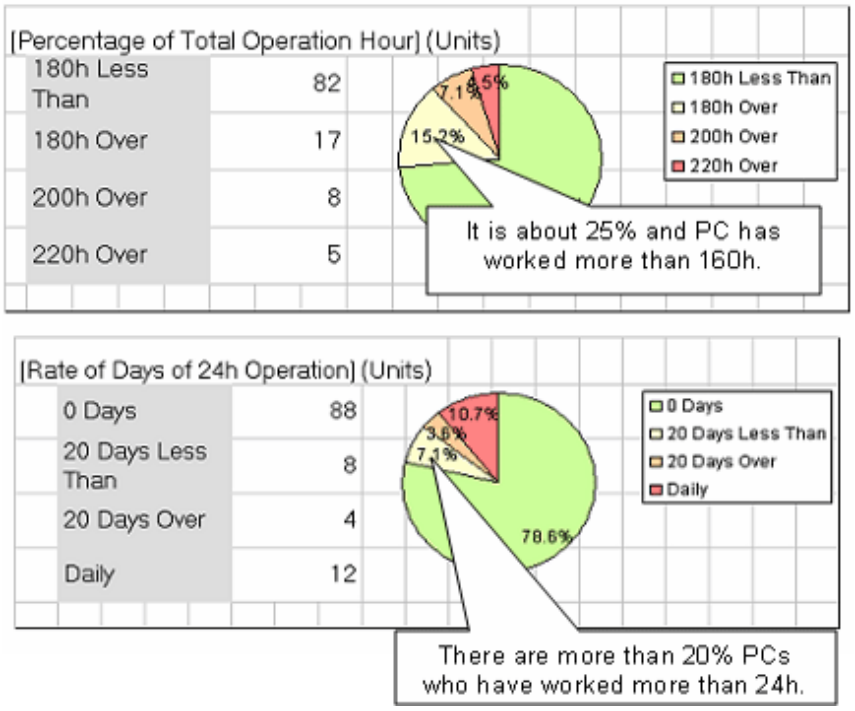
2. Confirmation of problem of not reflecting to result

a. Confirm whether there is the PC of long-time operation

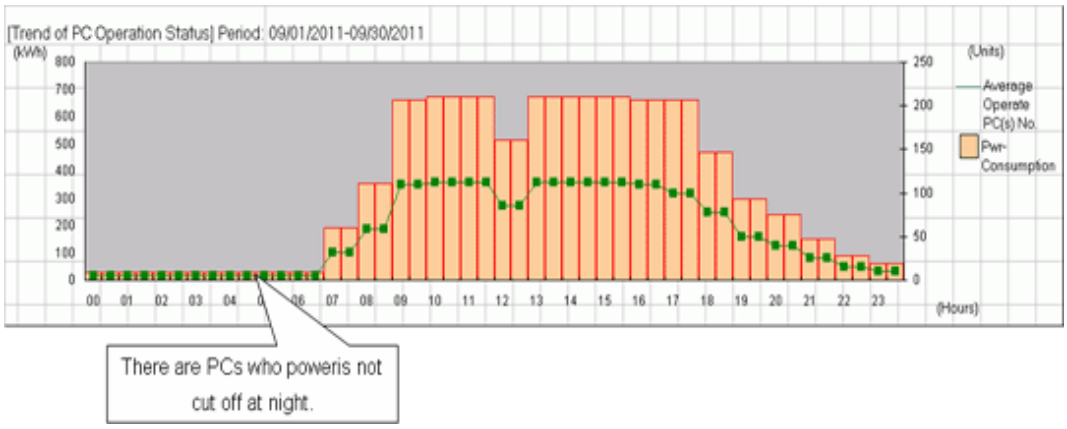
Grasp if there is a PC with problem for each power saving settings.

For example, if the PC is still in power saving setting, confirm whether there is a PC that runs 24h and whether there is a PC of long-time operation .etc.

Confirm [Percentage of Total Operation Hour] and [Rate of Days of 24h Operation].



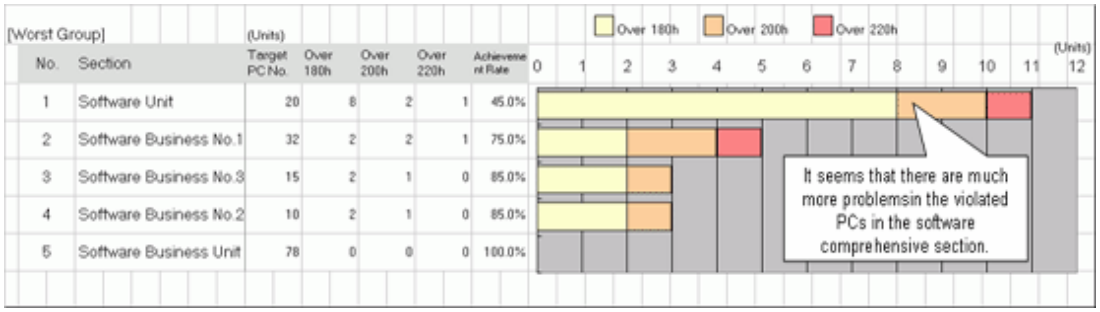
Confirm [Trend of PC Operation Status].



b. Confirm the status of PC of long-time operation for each section/location

Confirm whether there is a PC of long-time operation for each section/location.

Confirm [Low achievement rates].



c. Confirm the total operation time and power consumption status for each PC

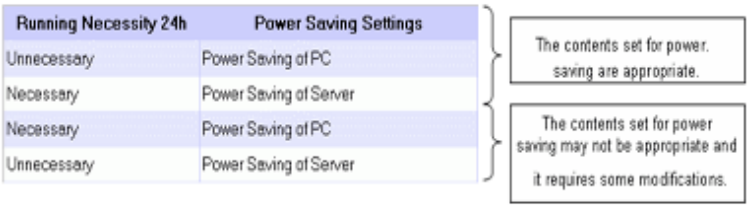
- When you wish to confirm if power saving setting has been selected correctly for each PC

  (When you wish to use it as reference information after selecting the power saving setting for each PC)

[Utilization of User Memo]

Output items such as [Running Necessity 24h] (24h operation is required/not required) set in user memo to details part.

Confirm [Running Necessity 24h] and [Power Saving Settings] of the details part and confirm whether the power saving setting has been selected correctly. For example, for PC that does not need to operate 24h, confirm whether the power saving settings for server or for the PC requires 24h operation has been set, and whether the power saving setting for PC has been set .etc.



Running Necessity 24h	Power Saving Settings
Unnecessary	Power Saving of PC
Necessary	Power Saving of Server
Necessary	Power Saving of PC
Unnecessary	Power Saving of Server

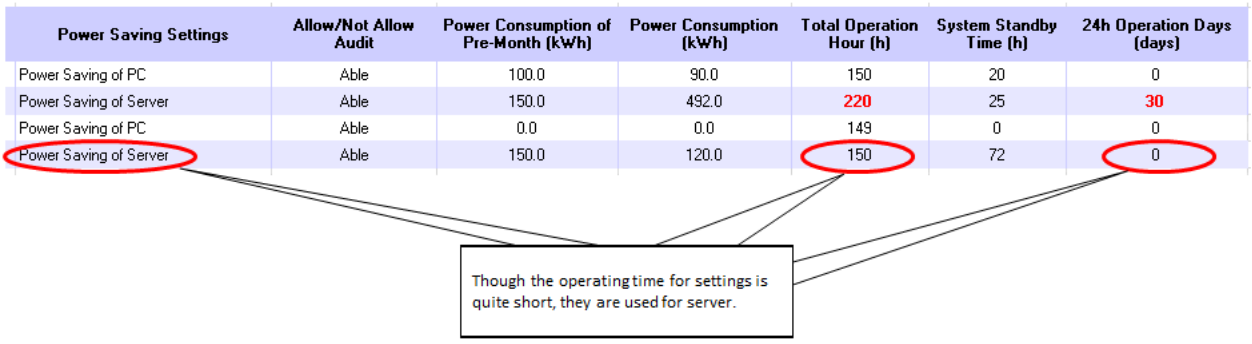
The contents set for power saving are appropriate.

The contents set for power saving may not be appropriate and it requires some modifications.

[Confirmation of Various Achievements]

Confirm [Total Operation Hour], [Number of 24h Operation Days] and [Power Saving Settings] of the details part and confirm whether the power saving setting has been selected correctly.

For example: for PC that is not set as long-time operation in total operation time or set with the days of 24h operation, confirm the power saving setting for server has been set, etc.



Power Saving Settings	Allow/Not Allow Audit	Power Consumption of Pre-Month (kWh)	Power Consumption (kWh)	Total Operation Hour (h)	System Standby Time (h)	24h Operation Days (days)
Power Saving of PC	Able	100.0	90.0	150	20	0
Power Saving of Server	Able	150.0	492.0	220	25	30
Power Saving of PC	Able	0.0	0.0	149	0	0
Power Saving of Server	Able	150.0	120.0	150	72	0

Though the operating time for settings is quite short, they are used for server.

- When you wish to confirm whether there is a PC that is used more than expected (with problem)

[Confirmation of Various Achievements]

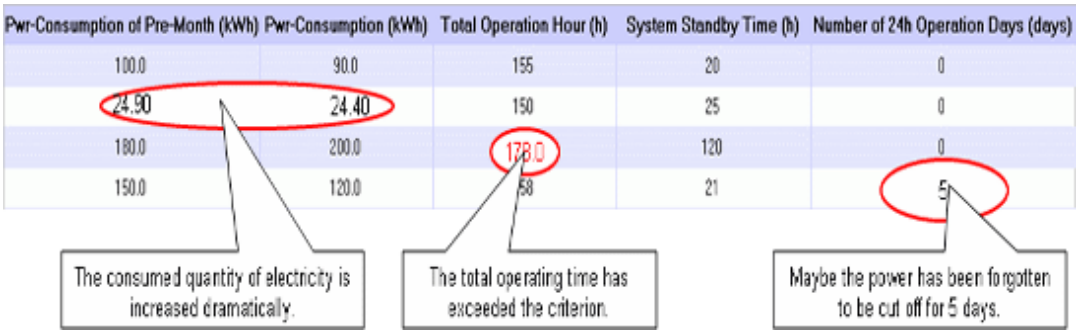
Confirm the [Pwr-Consumption of Pre-Month], [Pwr-Consumption], [Total Operation Hour] and [Number of 24h Operation Days] information of the details part and confirm if there is a PC with problems.

For example, perform the following confirmation.

-Comparing with the last month, the power consumption of this month increased greatly

-The total operation time exceeds the time as judgment standard

-The days of 24h operation exist, it is likely that you forgot to turn off the power



- When you wish to confirm whether there is a PC that can be withdrawn or reduced

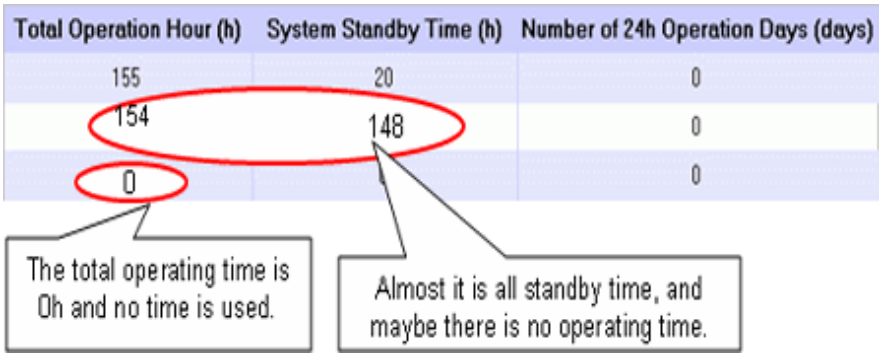
[Confirmation of Various Achievements]

Confirm [Total Operation Hour] and [System Standby Time] of the details part to check if there is a PC that is not used or basically not used.

For example, confirm the following.

-The total operation time is 0h (or several hours)

-The operation time is long, but mostly in system standby



3. Perform resolution and improvement for the problems confirmed in the report.

- When there are many PC of long-time operation in the whole company, section or setting location

  Resolution:

  - When there are many at company level, after confirming [Total Operation Hour] of each PC from the details part, re-define the time of judgment standard that has been set (example: 160h). In addition, confirm the current status to each section manager and perform operation instruction if necessary.
  - When there are many specific sections or setting locations, notify the section managers and ask them to make improvement.

- When there is a PC for which the power saving setting is not selected correctly

  Resolution:

  Allocate this PC to the appropriate group in **Environment Setup** > **Policy Groups** of the main menu.

- When there is a PC that is used more than expected

  Resolution:

  Contact the user of PC or the section administrator to confirm if the time of use is normal.

  When it is abnormal, request for correction of use time.

- When there is a PC that can be withdrawn or reduced

  Resolution:

  Contact the user of PC or the section administrator to confirm the usage purpose of PC.

When it is judged as not needed or can be shared with another PC from the utilization purpose, discuss whether to withdraw the PC or transfer the PC to another section.

Chapter 5 License Management

This chapter describes license management and applications.

5.1 Steps of License Management

The license management function is used for centralized management of the current License information of the enterprise and for understanding the availability of the software of License.

Through the license management function, the following operations can be achieved.

- Centralized management of License information of the company's internal software
- Detection of License violation PC, flexible execution of corrective operation

The following describes the operation method according to the operation flow to achieve flexible license management in Systemwalker Desktop Patrol.

Point

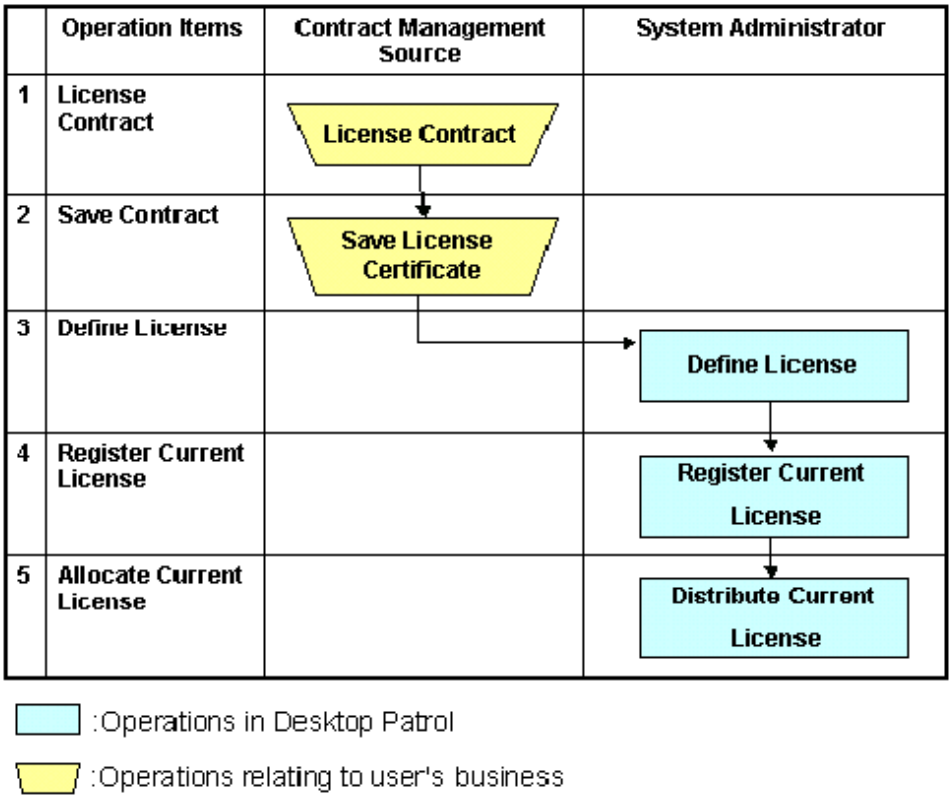
To perform license management, it's needed to select the software to be managed by License in the screen of **Software Auditing**.

5.1.1 License Management by Systemwalker Desktop Patrol

It describes how to manage the License software purchased from the software supplier by Systemwalker Desktop Patrol.

Systemwalker Desktop Patrol provides detailed information of software license management by unit and confirms the functions allocated to each PC state.

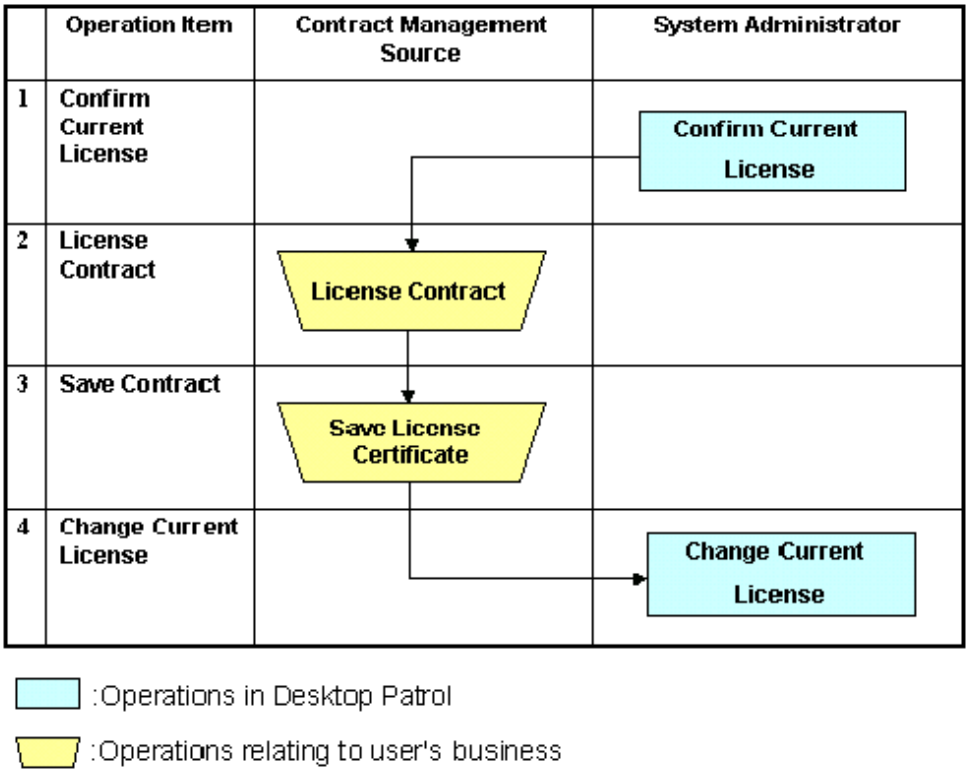
Software license management can be fulfilled with Systemwalker Desktop Patrol by going through the following flow.



1. Sign the License Contract with the software supplier.
2. Keep the License Contract of the purchased software.
3. Define the signed software License in Systemwalker Desktop Patrol. Refer to "5.2.1 Registration of License definition" for definition method.
4. It's needed to log in License information to manage the software License defined in Item "3". Refer to "5.3.1.1 Register Current License Information" for log in the License information.
5. Allocate the current License to each PC. Refer to "5.3.2 Allocate License" for License Giving method.

5.1.2 Confirm and Change Current License State with Systemwalker Desktop Patrol

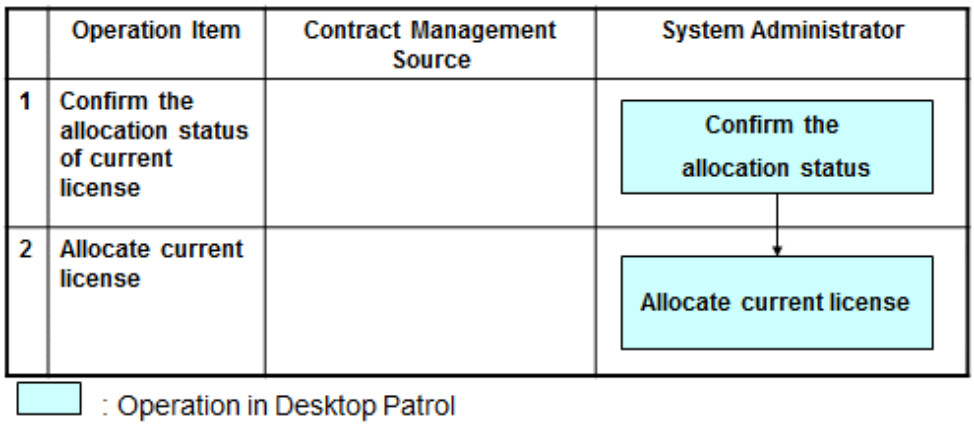
Confirm the current state related to the purchased software License, or operate according to the following flow to change the current License number.



1. Confirm the current License state at that time. Refer to relevant contents about "5.3.1 Management of Current License" for current state confirmation.
2. Sign the License Contract with the software supplier as needed.
3. Keep the contract when signing the License Contract.
4. Register the License information of the signed contract in Systemwalker Desktop Patrol to change number of the current License. Refer to relevant contents of "5.3.1.2 Modify Information of Current License" for registration method.

5.1.3 Allocate Current License with Systemwalker Desktop Patrol

Operate according to the following flow to allocate the purchased software License.

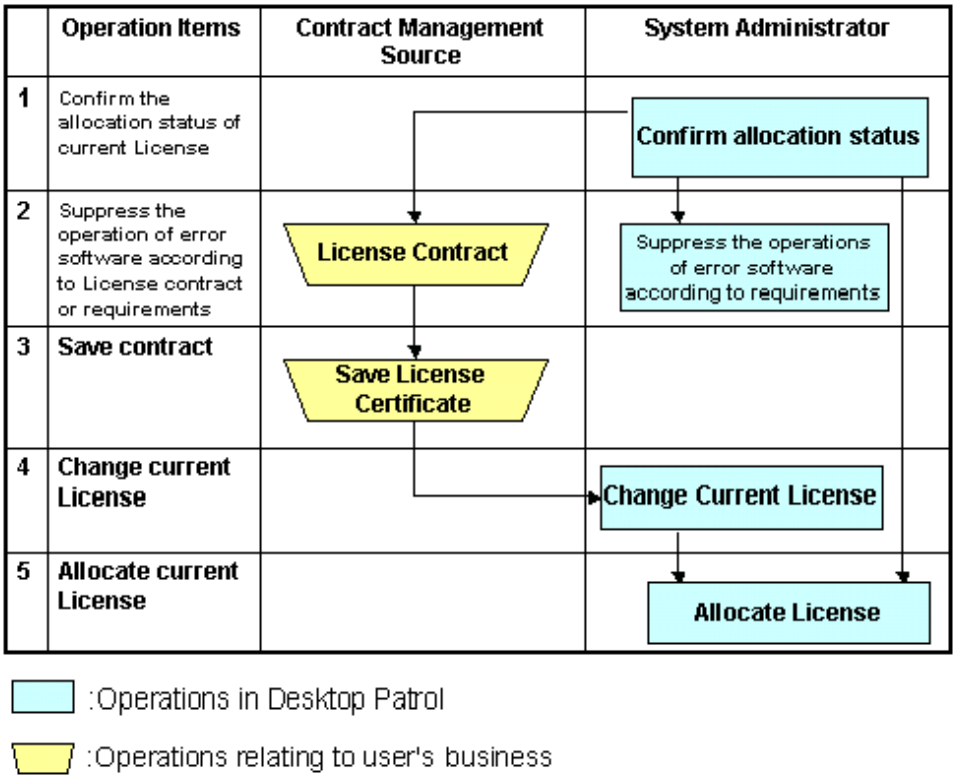


1. Confirm allocation state of current License.
   Refer to "5.3.2 Allocate License" for method of License Giving state.
2. Allocate current License to the PC as needed.
   Refer to "5.3.2 Allocate License" for method of License Giving.

5.1.4 Detect and Correct the License Violation PC with Systemwalker Desktop Patrol

Based on the collected Inventory information in Systemwalker Desktop Patrol, find the violation PC against current License.

Operate according to the following flow to find the violation PC. At the same time, explain the corrective method of License Giving.

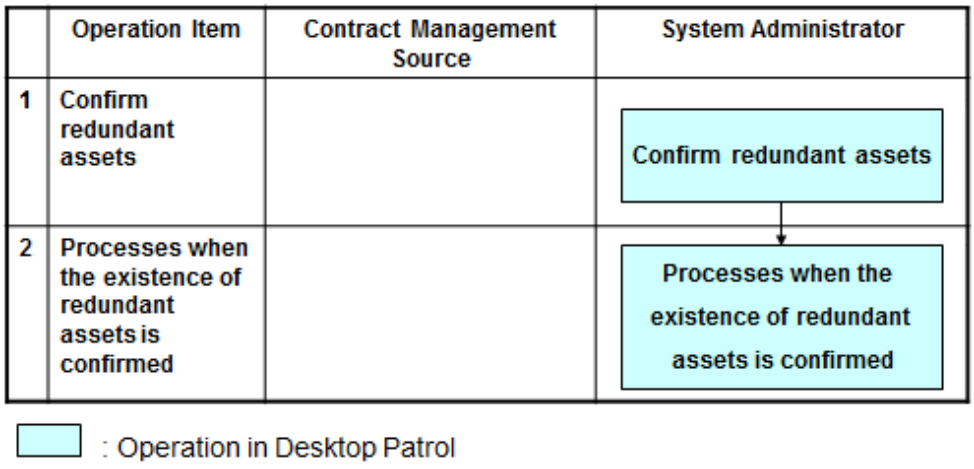


1. Confirm the current License Giving state.
   Refer to "5.3.2 Allocate License" for method of allocation state of current License. Additionally, refer to "5.3.4.1 Confirm License Violation PC" for detection method of violation PC.

2. Confirm number of current License after detection of violation PC.
   According to the corrective treatment, sign the License contract with the software supplier and prepare the License to be allocated when it's necessary to use the software.
   Execution of the software can be prohibited if the software in unlawful use is an unwanted one. Refer to "2.6 Control Executable file" for method of prohibition.
3. Keep the contract when signing the License Contract.
4. The signed License information will be registered in Systemwalker Desktop Patrol when number of the current License changes. Refer to "5.3.1.2 Modify Information of Current License" for method of registration.
5. Allocate the current License to PC as needed.
   Refer to "5.3.2 Allocate License" for details on how to allocate a current license.

5.1.5 Return License of Unwanted Software

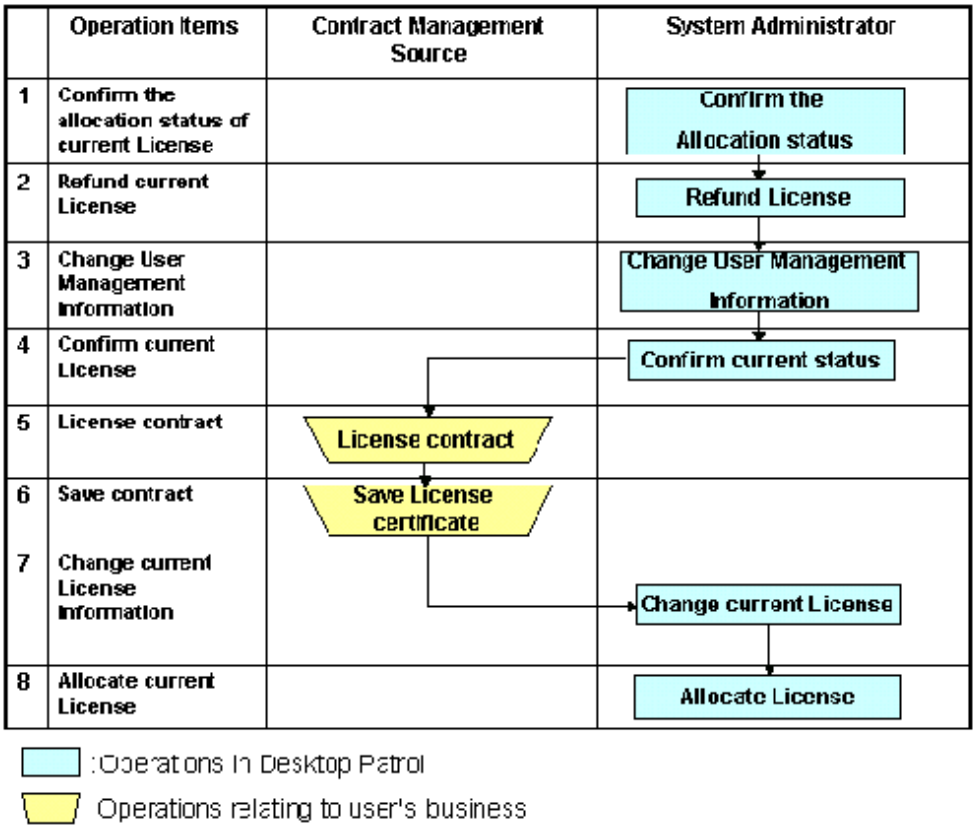
Operate according to the following flow to return License of the unwanted software.



1. Confirm the idle assets.
   Refer to "5.4.2.1 Confirm Idle Assets" for confirmation method of idle assets.
2. Perform recovery and other kinds of disposal of the current License if there are idle assets. Refer to "5.4.2.2 Processing at Confirmation of Idle Assets" for treatment method.

5.1.6 License Change Going with Personnel Change

Operate according to the following flow when personnel changes happen.



1. Confirm the current License Giving status.
   Refer to "5.3.2 Allocate License" for confirmation method of allocation status of current License.
2. For PC managed by user of personnel change, take back License if the PC is allocated with License.
   Refer to "5.3.2 Allocate License" for method of License recovery.
3. Change the user management information of the user of personnel change.
   Refer to "2.1.3 Procedure of Constructing Master Data" for change method of user management information.
4. Confirm current License status of the new section.
   Refer to "5.3.1 Management of Current License" for confirmation method of current status.
5. Sign License contract to the software supplier as needed.
6. Keep the contract after License contract is signed.
7. The signed License information will be registered in Systemwalker Desktop Patrol when number of the current License changes.
   Refer to "5.3.1.2 Modify Information of Current License" for method of registration.
8. Allocate current License to PC of changed user management.
   Refer to "5.3.2 Allocate License" for method of License Giving.

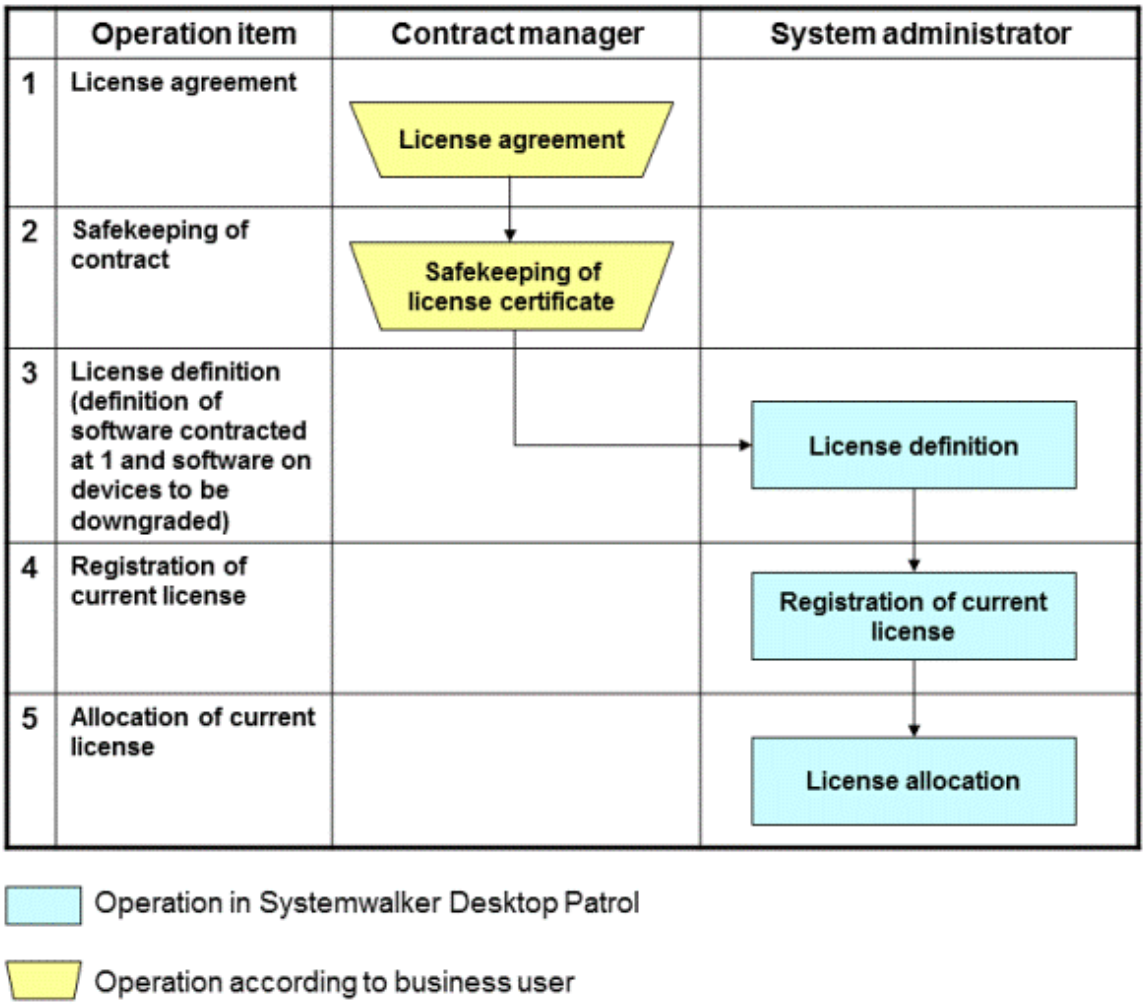
5.1.7 Manage Software License by Using Downgrade Rights

Downgrade rights allow the user to downgrade to and use an earlier version.

If you downgrade software using downgrade rights, follow the flow shown below to manage the software license.

The procedure explained below is based on the following example.

Example: Use the downgrade rights provided in the license for software A to downgrade to software B



1. Enter into a license agreement for software A with the software vendor.
2. Store the purchased software license agreement in a safe place.
3. Define the software license in Systemwalker Desktop Patrol. Register software A and software B as a single definition. Refer to "5.2.1 Registration of License definition" for details.
4. Register license information to manage the software license you defined in step 3. Refer to "5.3.1.1 Register Current License Information" for details. Clearly indicate at this time that you have downgrade rights for the items in **Other Conditions**.
5. Allocate a current license to the PC where you downgraded to software B. Refer to "5.3.2 Allocate License" for details on how to allocate a current license. Select software B and allocate the license you registered in step 4.

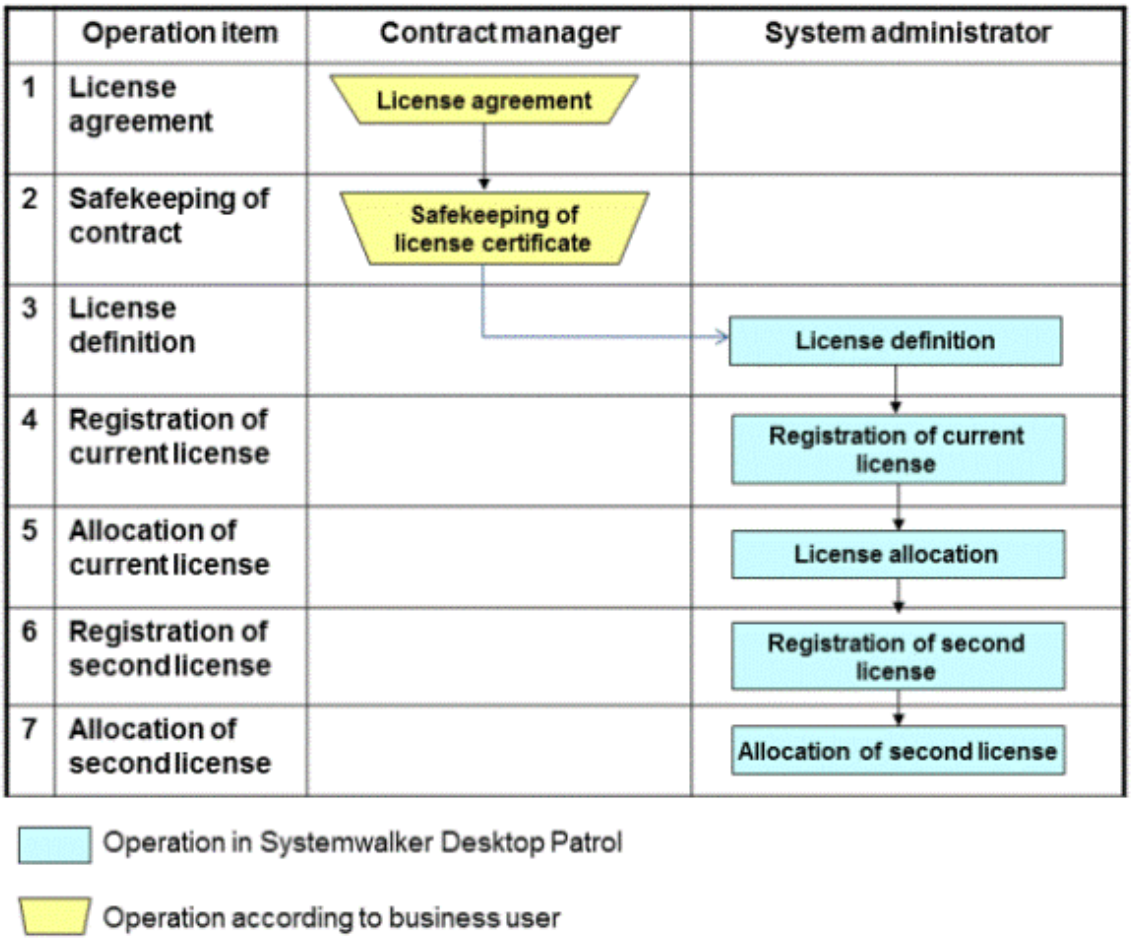
5.1.8 Manage Software License Expanded to Second License

As a rule, a software license permits installation to a single computer. A second license permits a specific computer user to install the software on one other mobile PC provided that the PC is used only by the said user.

Follow the flow shown below to manage a software license for which you have a second license and to use that second license to install the software.

The procedure explained below is based on the following example.

Example: Install software A for which you have a second license to PC1 and use the second license to install software A to PC2



1. Enter into a license agreement for software A with the software vendor.
2. Store the purchased software license agreement in a safe place.
3. Define the software license in Systemwalker Desktop Patrol. Refer to "5.2.1 Registration of License definition" for details.
4. Register license information to manage the software license you defined in step 3. Refer to "5.3.1.1 Register Current License Information" for details. Clearly indicate at this time that you have a second license for the items in **Other Conditions**.
5. Allocate the license you registered in step 4 to PC1 where you installed software A. Refer to "5.3.2 Allocate License" for details on how to allocate a current license.
6. Register information about the second license of the software license you defined in step 3. Refer to "5.3.1.1 Register Current License Information" for details. Clearly indicate at this time that this is the second license of the license you registered in step 4.
7. Allocate the license you registered in step 6 to PC2 where you installed the software using the second license of software A. Refer to "5.3.2 Allocate License" for details on how to allocate a current license.

5.1.9 Check License Usage

You can check license usage by confirming idle assets and detecting and correcting license violations. This information about license usage is useful when you next enter into a license agreement.

Follow the flow shown below:

1. Refer to "5.1.5 Return License of Unwanted Software", confirm idle assets, and take action as required.
2. Refer to "5.1.4 Detect and Correct the License Violation PC with Systemwalker Desktop Patrol" and correct license usage.
3. Check the number of purchased licenses and the remaining number of licenses in the **Current License Management** window. This information is useful when you next enter into a license agreement.

5.2 Definition of License

The purpose of License definition is to manage License as one type even the software has many versions.

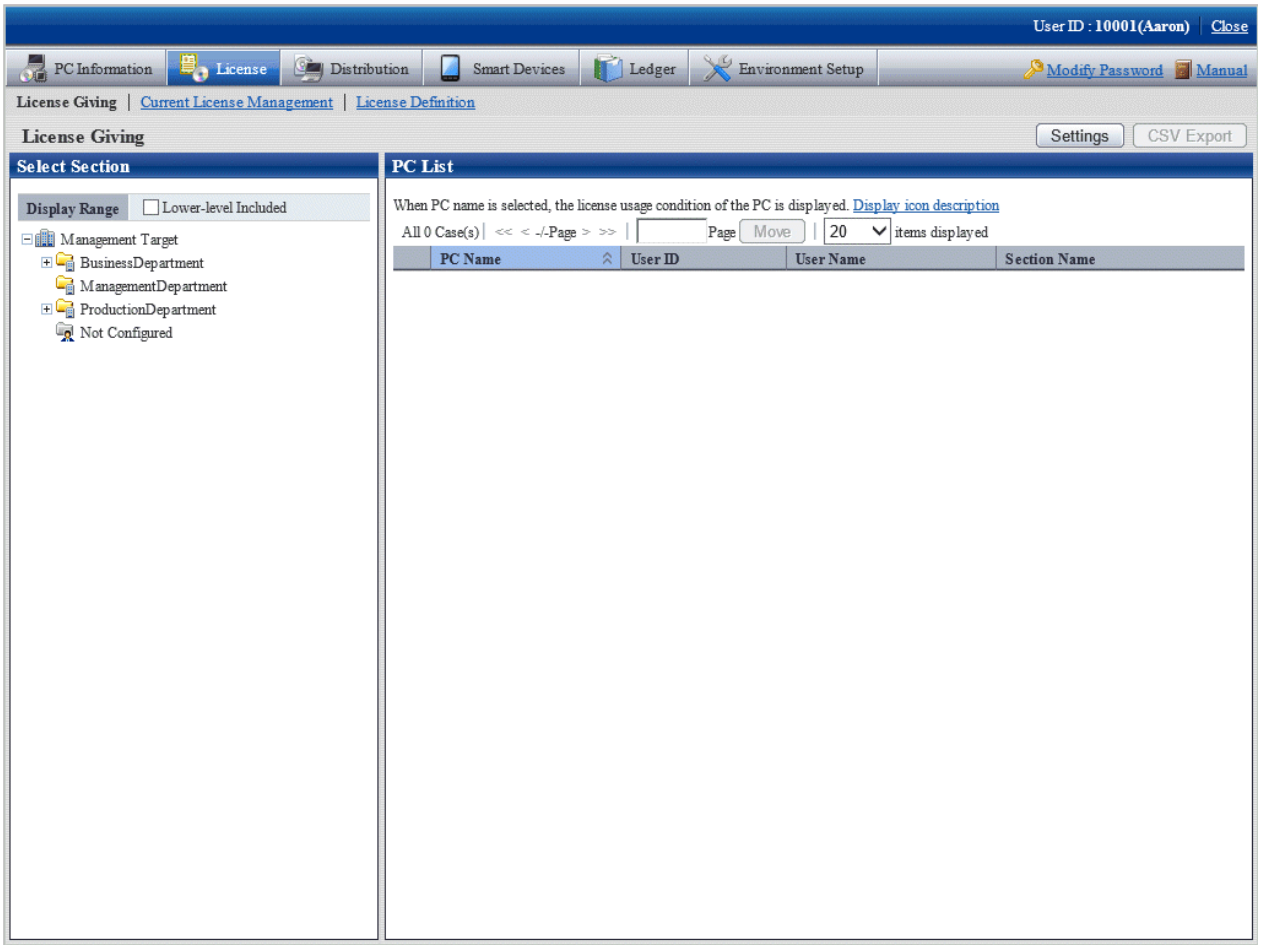
Here it describes License definition of original setup of license management business.

5.2.1 Registration of License definition

License is defined as below.

1. Log in to the main menu, and click **License**.

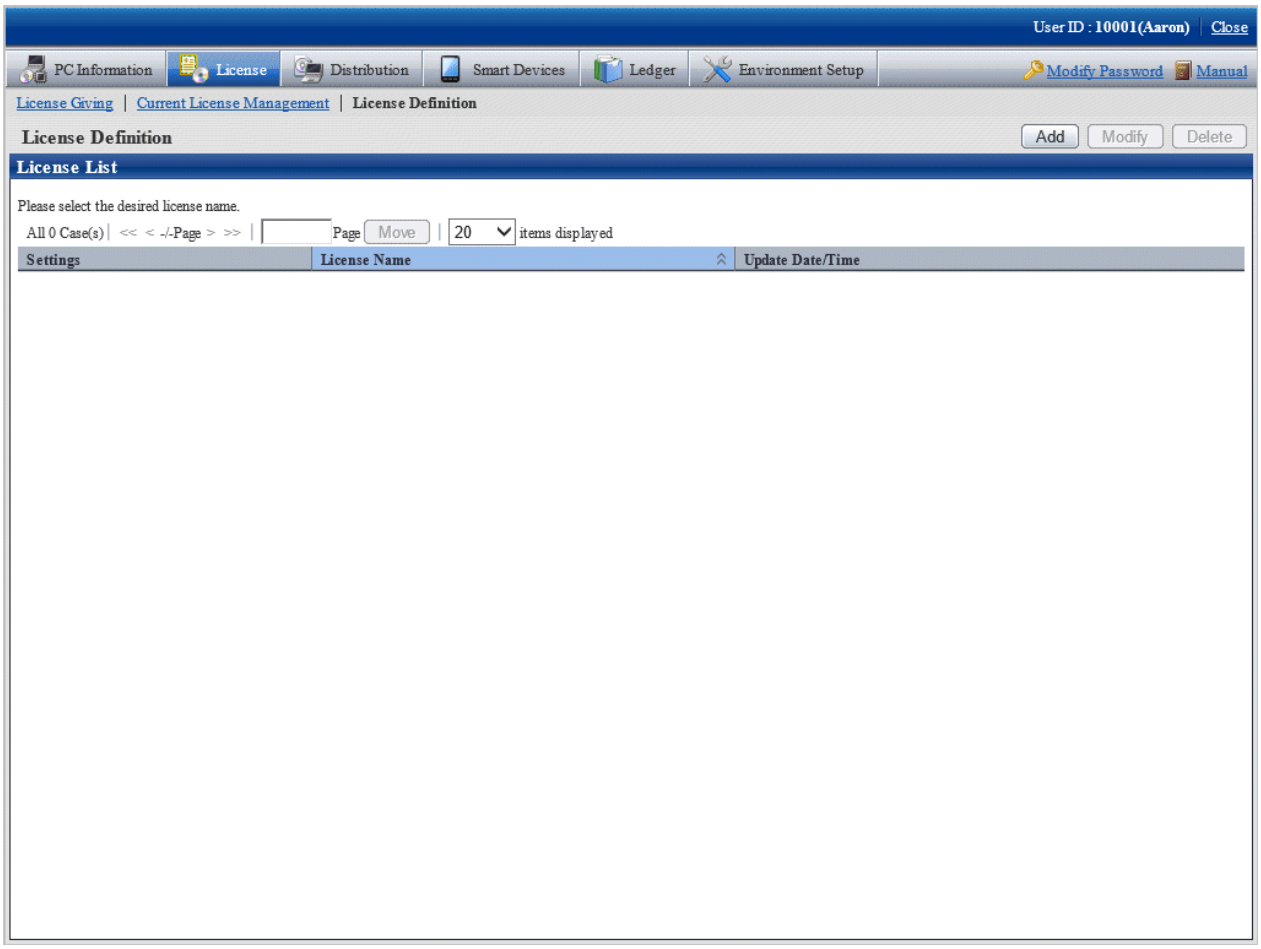
   The **License** window will be displayed.



   Link of **License Definition** will not appear when user ID of section management account is used to log in.

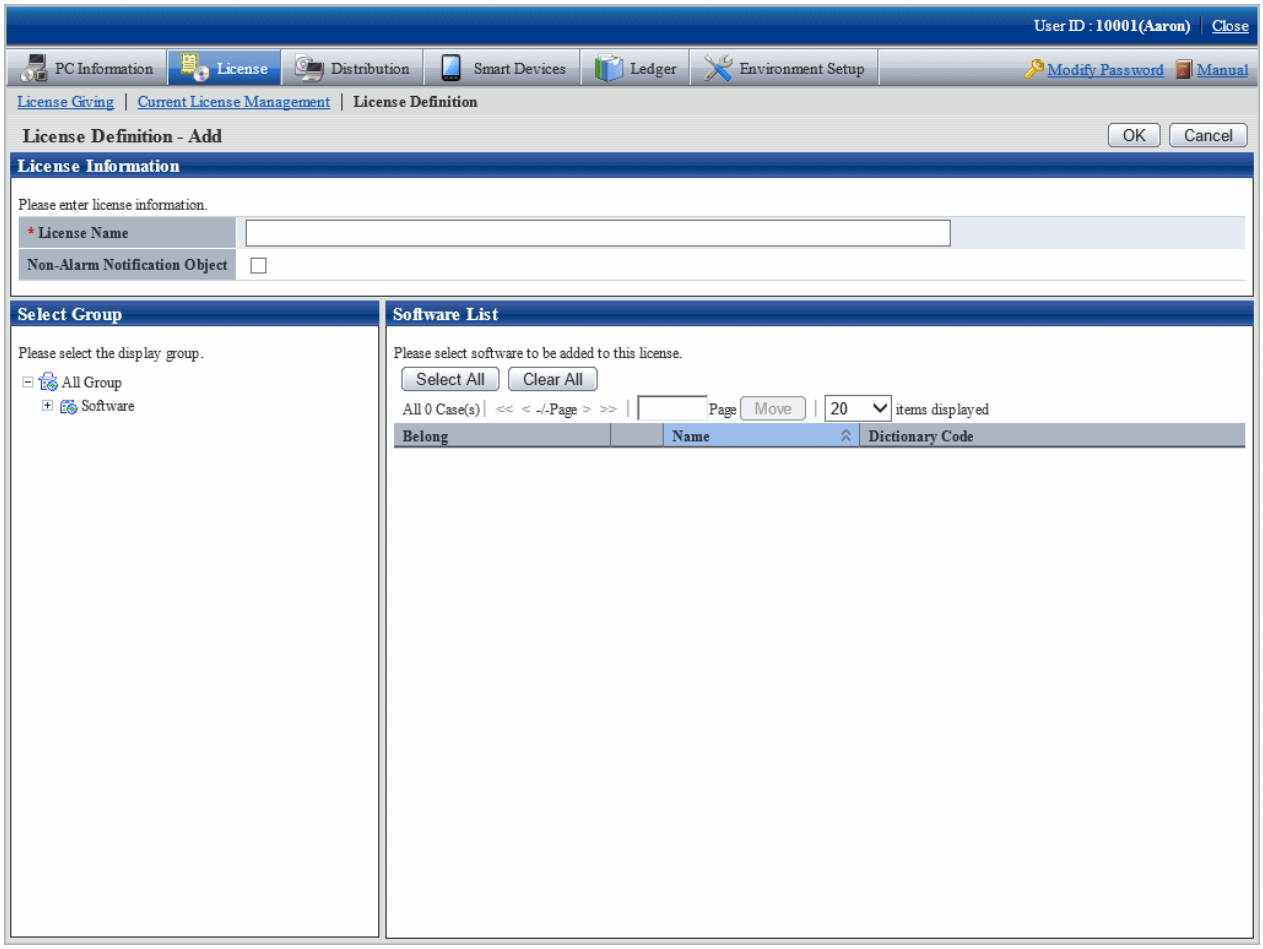
2. Click **License Definition**.

   The following window will be displayed.



3. Click the **Add** button

   The following window will be displayed.



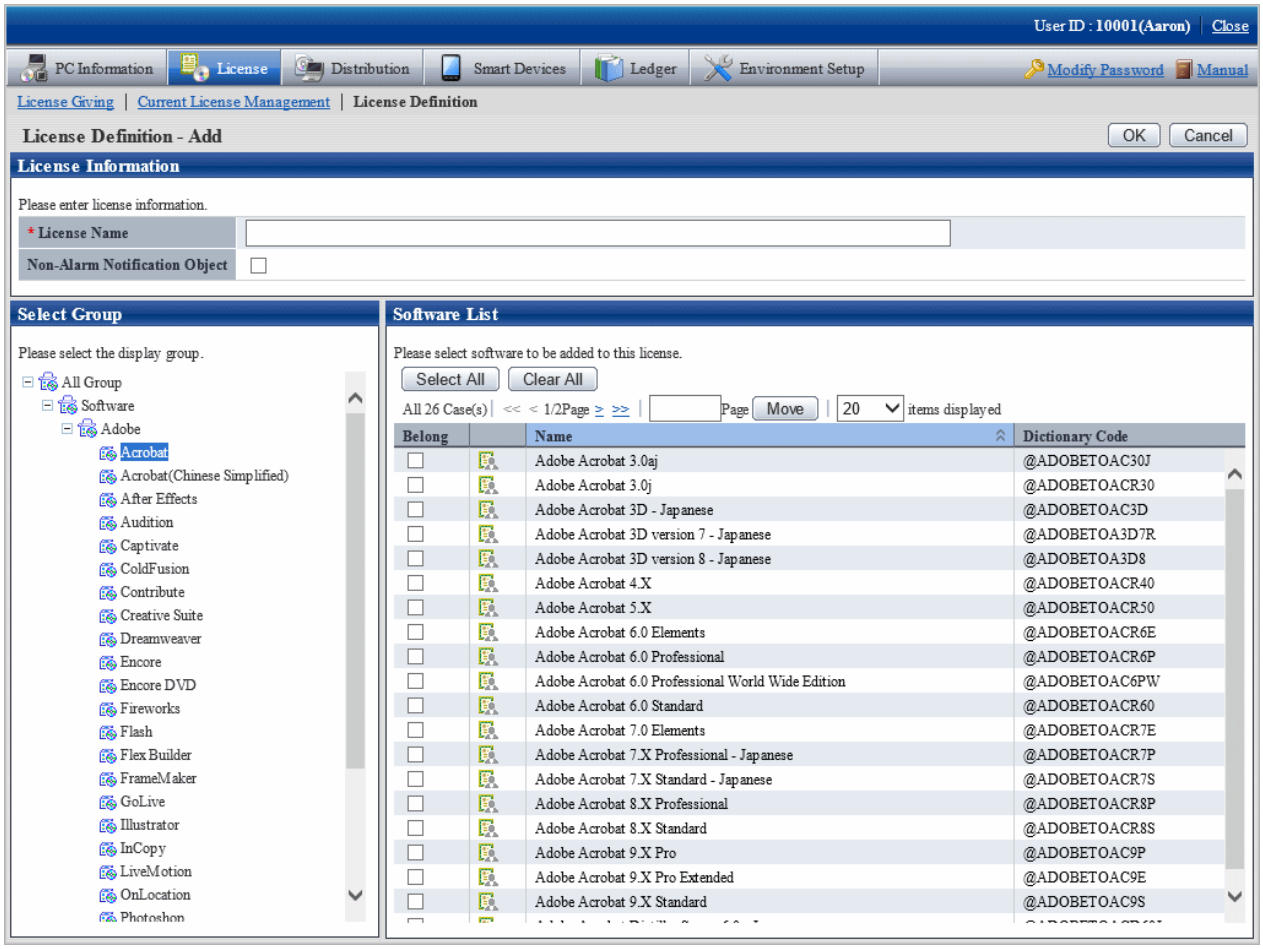
4. Input License information.

Item to be defined	Input character
License Name(required)	Enter License name in groups. Enter characters within 30 multi-byte or 60 single-byte. Specified characters can be alphanumeric characters and the following single-byte characters. ("-""@"."("")""["]"{"}"<">":";")
Non-Alarm Notification Object	When grouped software is not to be used as non-alarm notification target of License violation, select **Non-Alarm Notification Target**.

Remarks. Alarm notification of License violation is the function of notifying when software not allocated with License is in use or number of License is exceeded. For details, refer to "2.5 Set Alarm Notification".

5. Select software supplier from the tree in the field on the left.

   The software provided by the selected supplier will be displayed in the field on the right.



6. Select the check box of software of License to be defined for Alarm Notification, click the **OK** button.

   License will be defined.

   Meanings of the icons are as below.

	Software that has not given License to any PC
	Software that has given License to PC(s)

7. Refer to "5.2.2 Modify License Definition" for confirmation of software with defined License.

5.2.2 Modify License Definition

Add/cancel the registered License name or software of defined License.

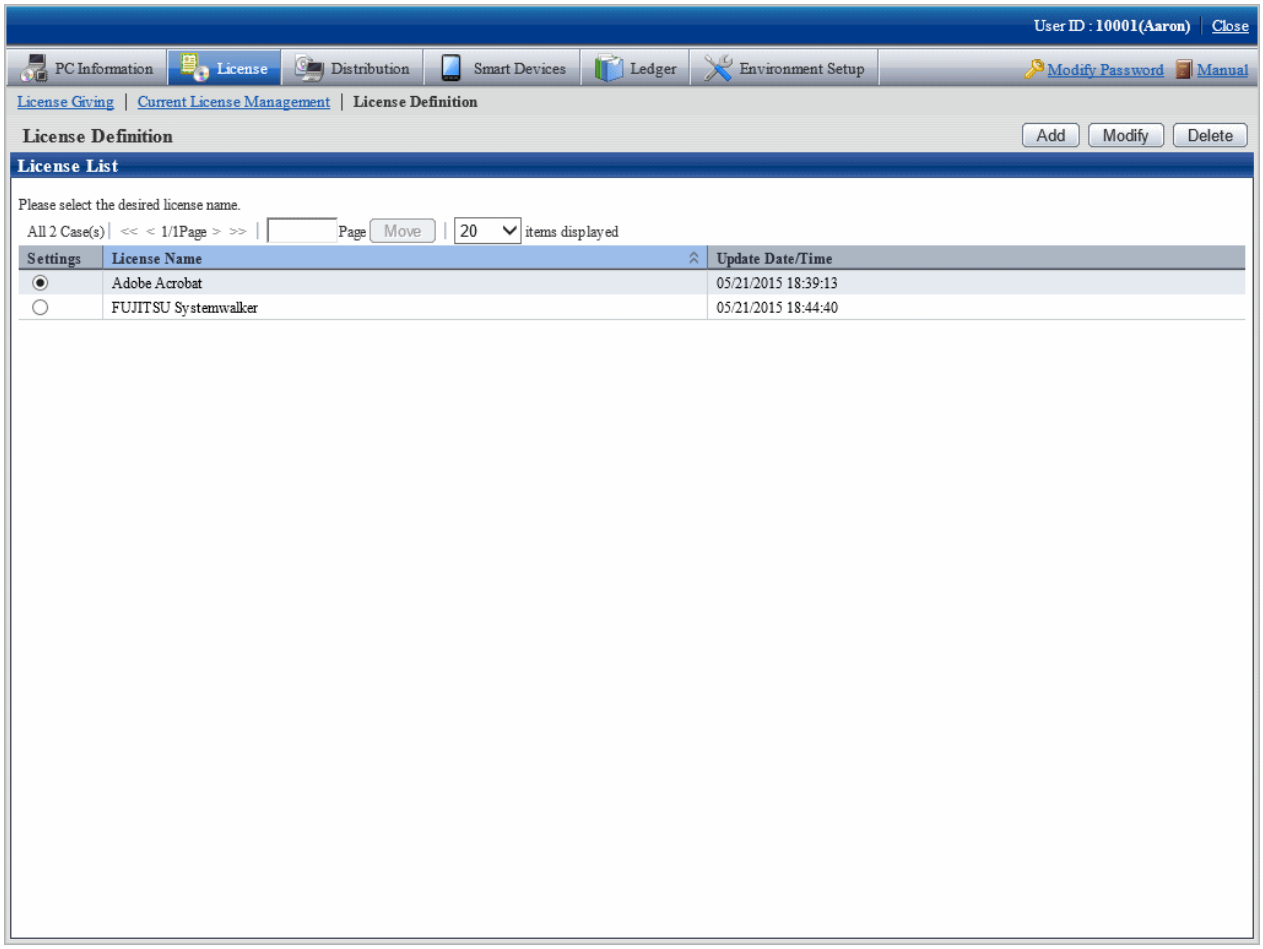
The procedure is as follows.

1. Log in to the main menu, click **License**.

   License window will be displayed.

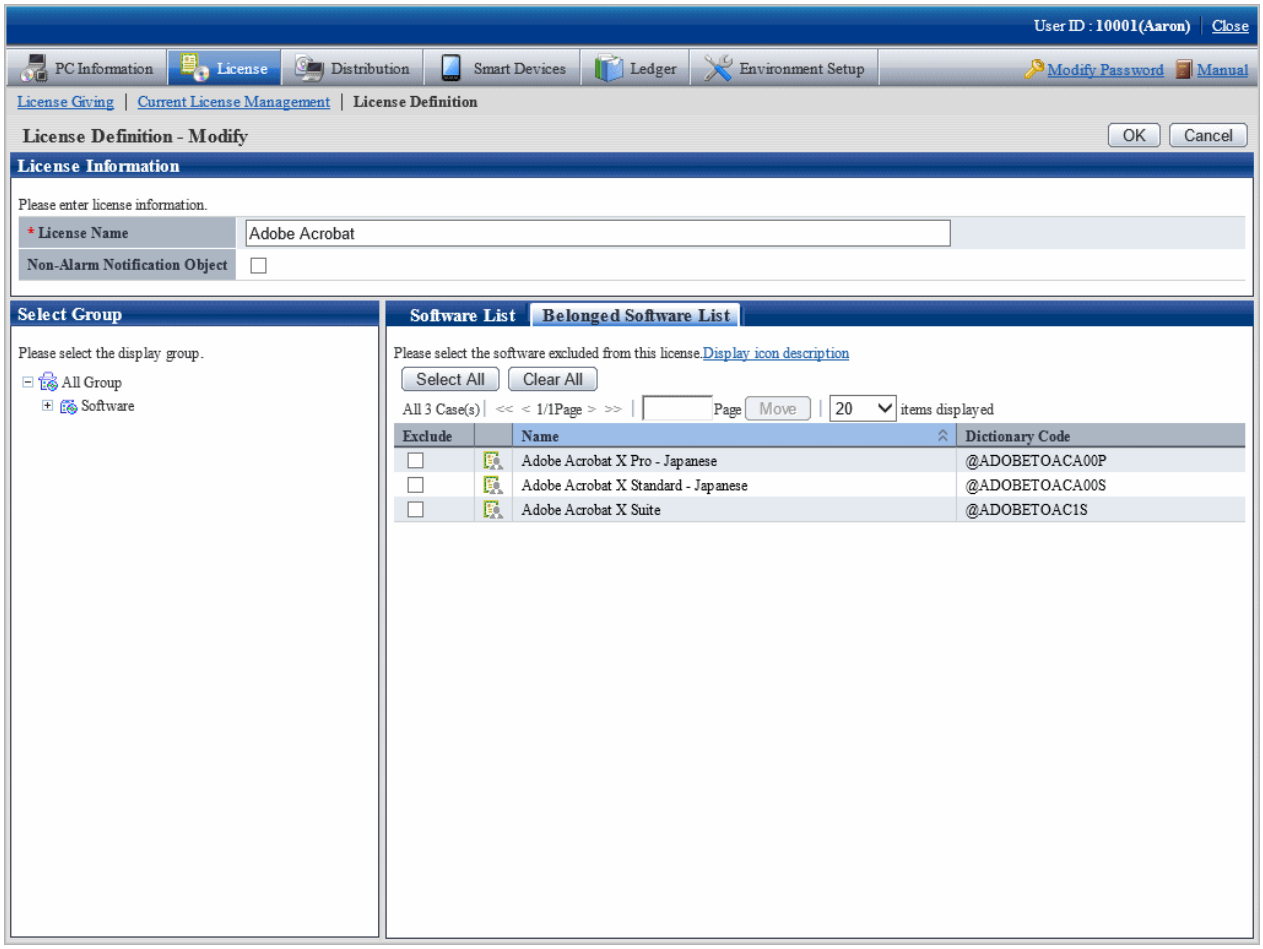
2. Click **License Definition**.

   The following window will be displayed.



3. Select the License name to be changed from the **License List**, click the **Modify** button.

   The following window will be displayed.



4. Enter the License information to be modified.

Item to be changed	Input character
License Name (required)	Enter the grouped License name. Enter characters within 30 multi-byte or 60 single-byte. Specified characters can be alphanumeric characters and the following single-byte characters. ("-""@"".""("")""["]"{"}""<"">"":";")
Non-Alarm Notification Object	When grouped software is not to be used as Non-Alarm notification target of License violation, select **Non-Alarm Notification Target**.

   Remarks. Alarm notification of License violation is the function of notifying when software not allocated with License is in use or number of License is exceeded. For details, refer to "2.5 Set Alarm Notification".

5. Perform the following operations to delete software from License.

   a. Click the **Belonged Software List** tab, select the software to be deleted from License.

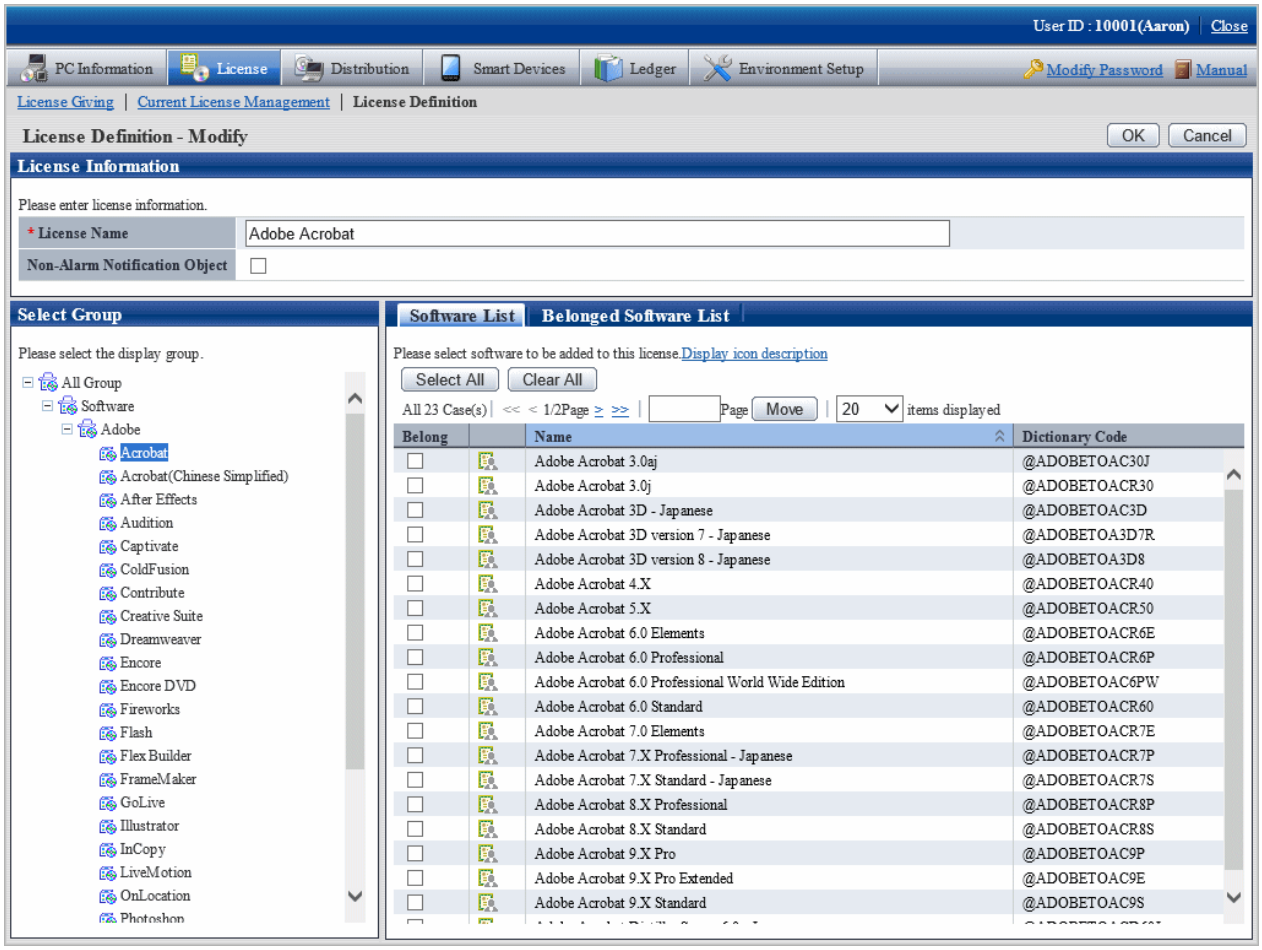
      But software allocated with License cannot be deleted. Delete after removing the allocation of License. Refer to "5.3.2 Allocate License" for removal of License Giving.

6. Perform the following operations to add software to License.

   a. Click the **Software List** tab, select software supplier from the tree in the field on the left.

      Software provided by the selected supplier appears in the field on the right.

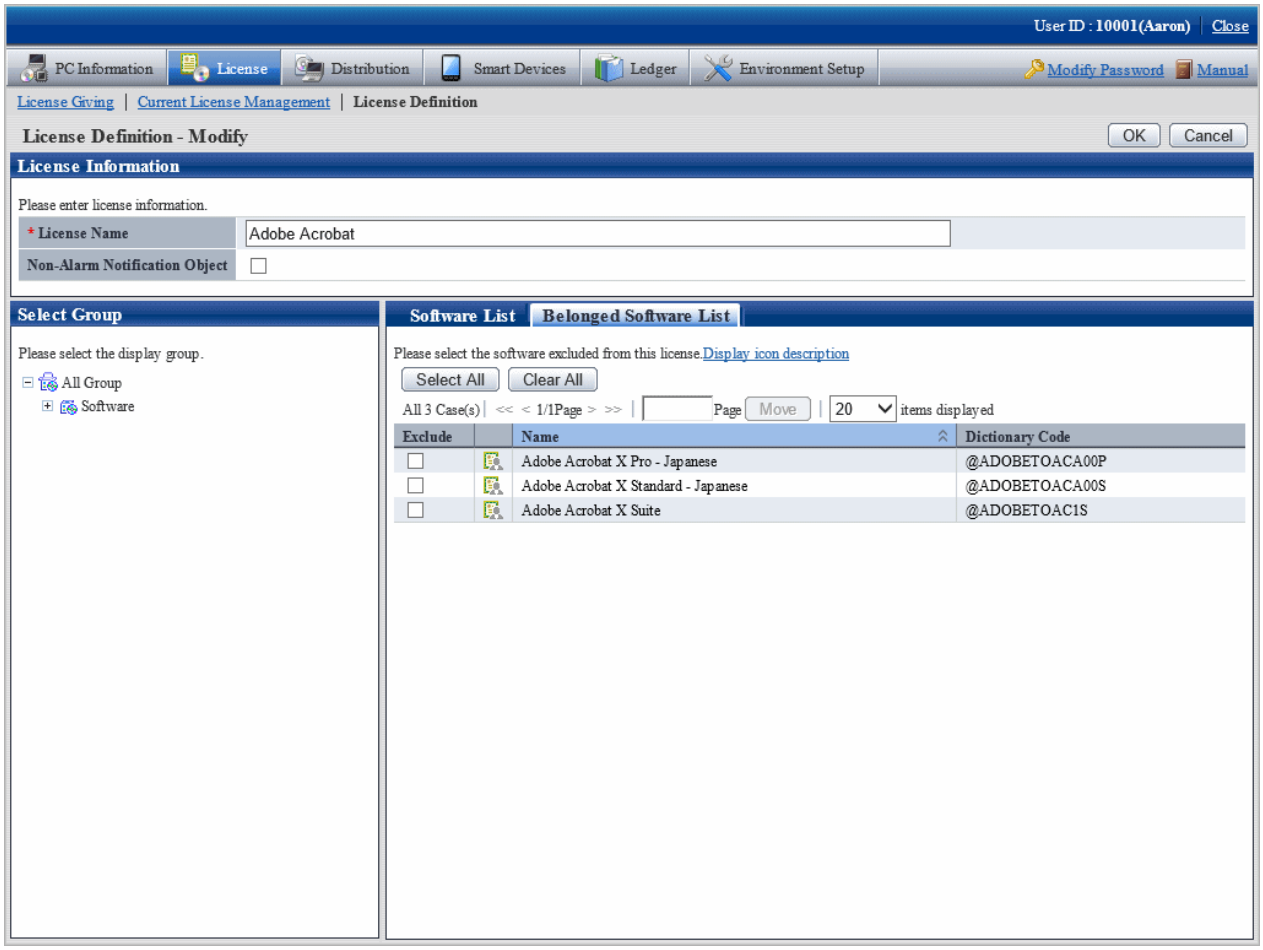
   b. Select the software to be added to License.



7. Click **OK** button.

   The defined License will be modified.

8. Repeat the steps starting from "3." after confirmation of software with changed License, click the **Belonged Software List** tab for confirmation.



5.2.3 Delete License Definition

Delete the License to be discarded for unwanted software that is being used.

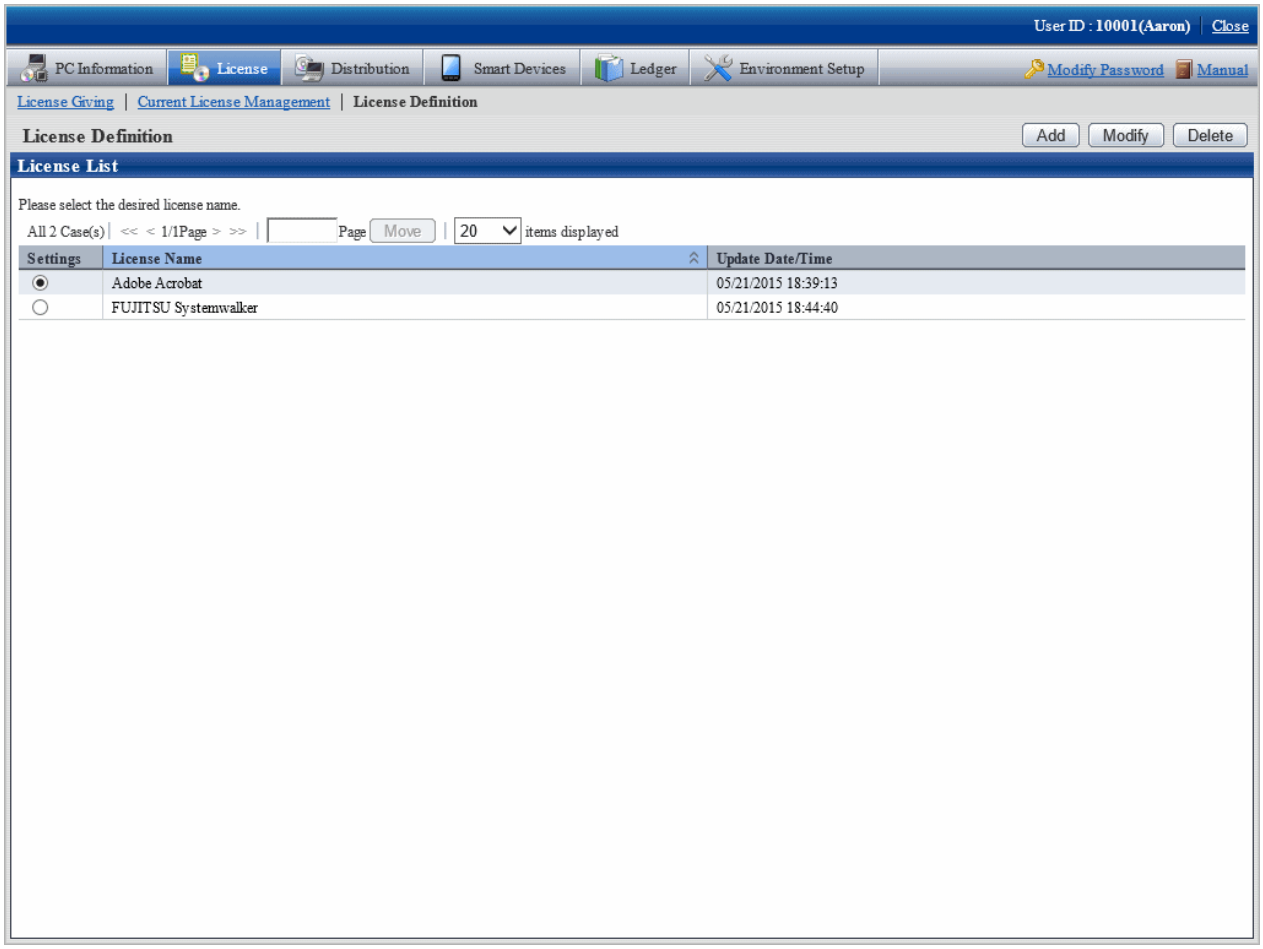
The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

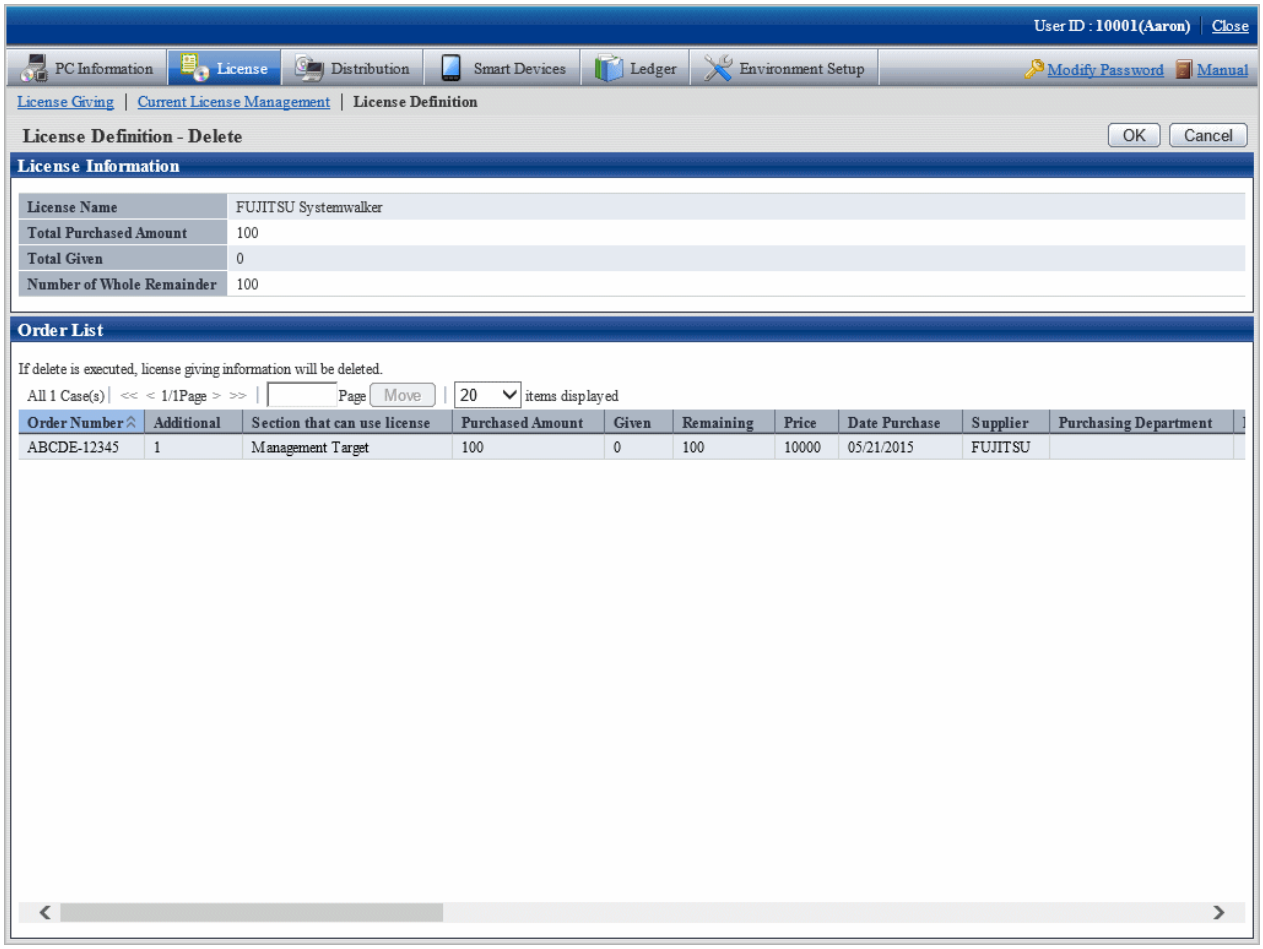
2. Click **License Definition**.

   The following window will be displayed.



3. Select the License name to be deleted from License List, and click the **Delete** button.

   The following window will be displayed.



4. Click the **OK** button.

   The following window will be displayed.

5.3 Confirm PC of License Violation

Whether the software used on CT has violated to the License policy can be confirmed.

Allocate License to PC according to the following procedure when confirming the PC with License violation.

1. Current License Management
2. License Giving

This section describes how to set and use the PC with License violation.

5.3.1 Management of Current License

Here, It describes the management of current License.

1. Confirm current status of License in the **Current License Management** window. In addition, perform the following operations as needed.

- Add: License information registration performed for managing purchased License.

- Modify: after registration of current License, information of the purchased License can be added and modified.
- Delete: the unwanted License can be deleted.
- View software: the software registered in License can be confirmed.

Confirm the status of current license

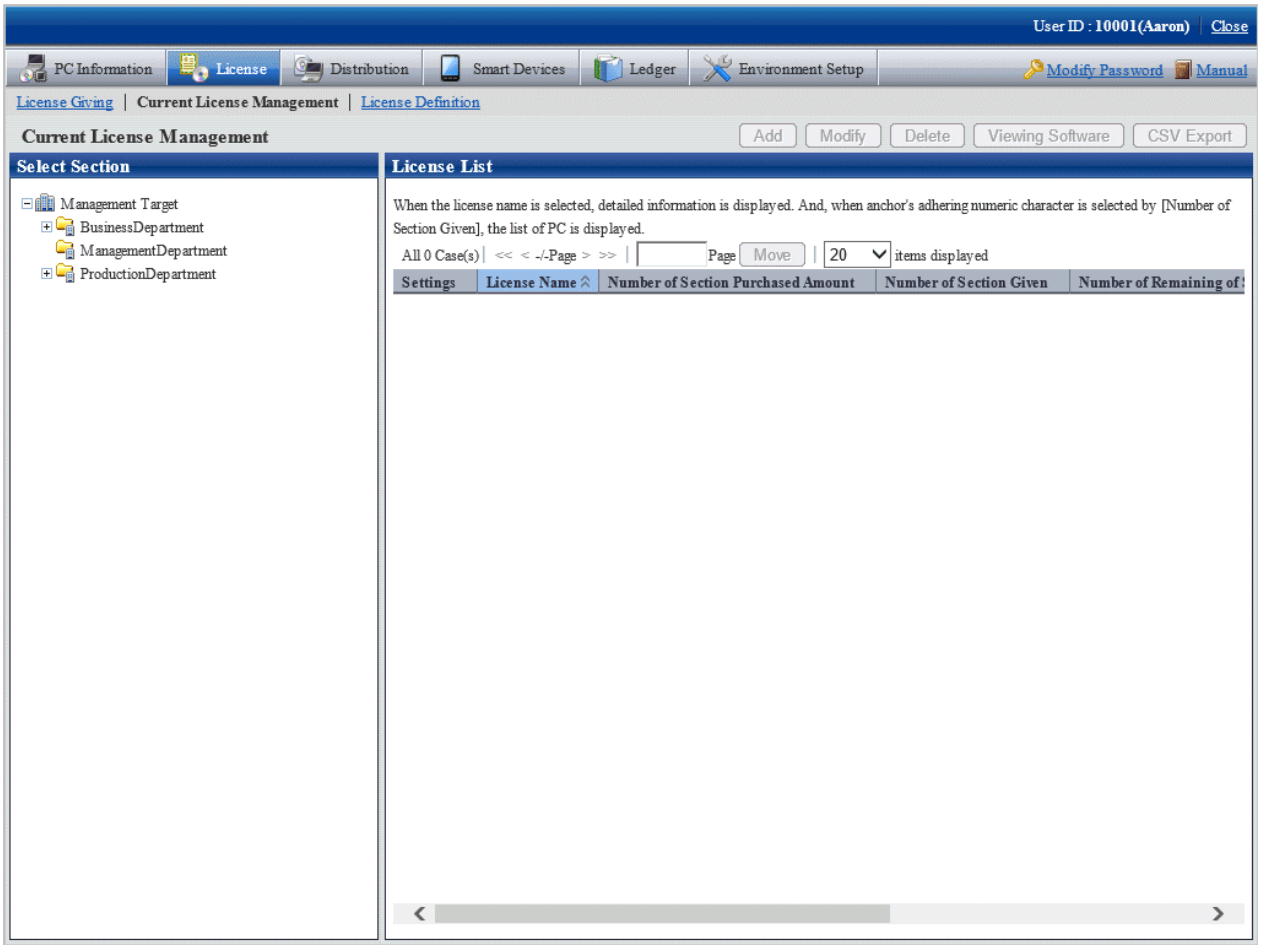
The procedure of confirming the status of the current License is as follows.

1. Log in to the main menu, click **License**.

   License window will be displayed.

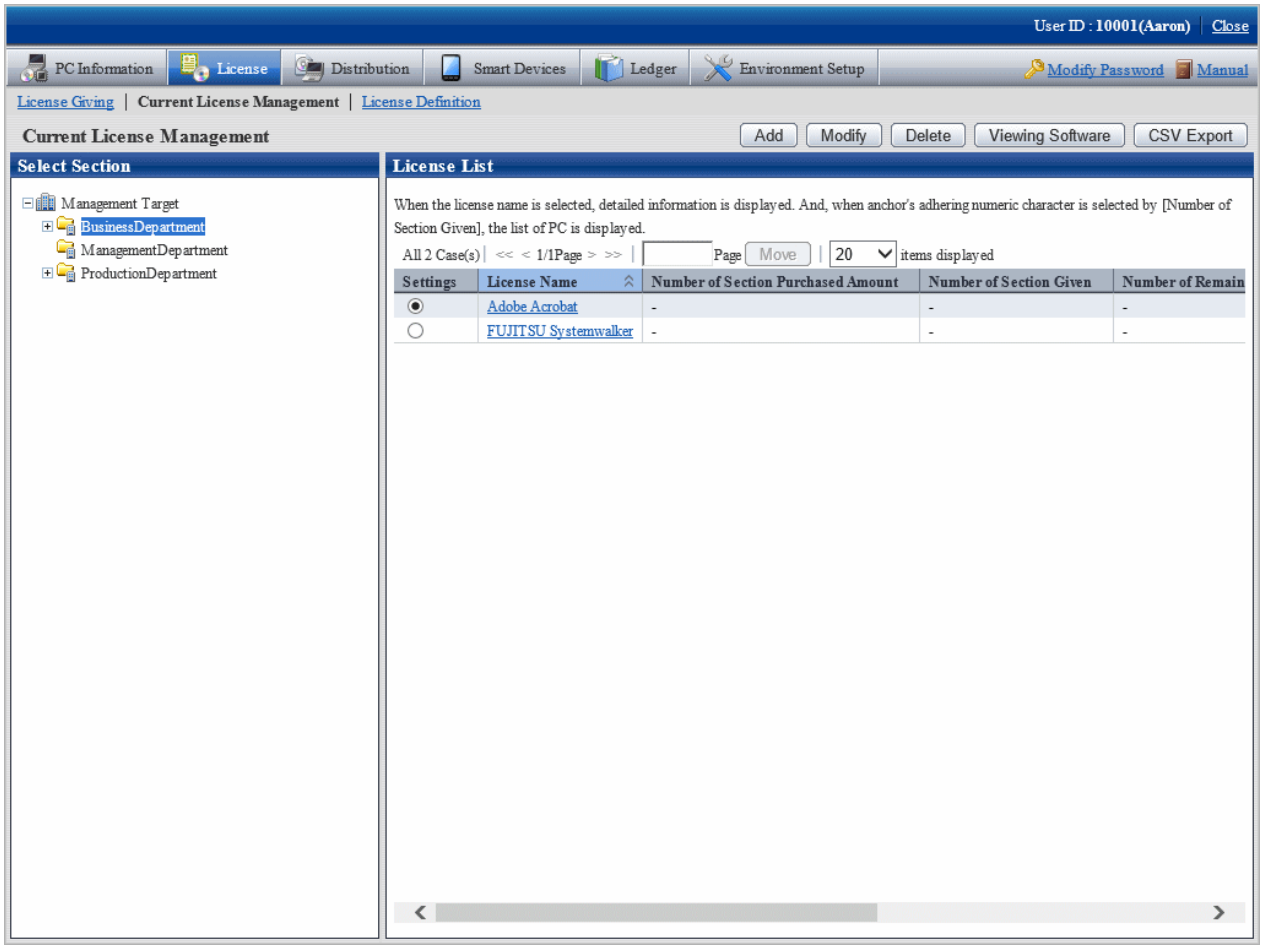
2. Click **Current License Management**.

   The following window will be displayed.



3. Select a section from the section tree in the field on the left.

   The license status of the selected section will be displayed in the field on the right.



4. Perform the following operations to export the License information displayed in the field on the right as a file in CSV format. Proceed to the next step if not to export.

   a. Select the License Name to be exported in CSV format, and click the **CSV Export** button.

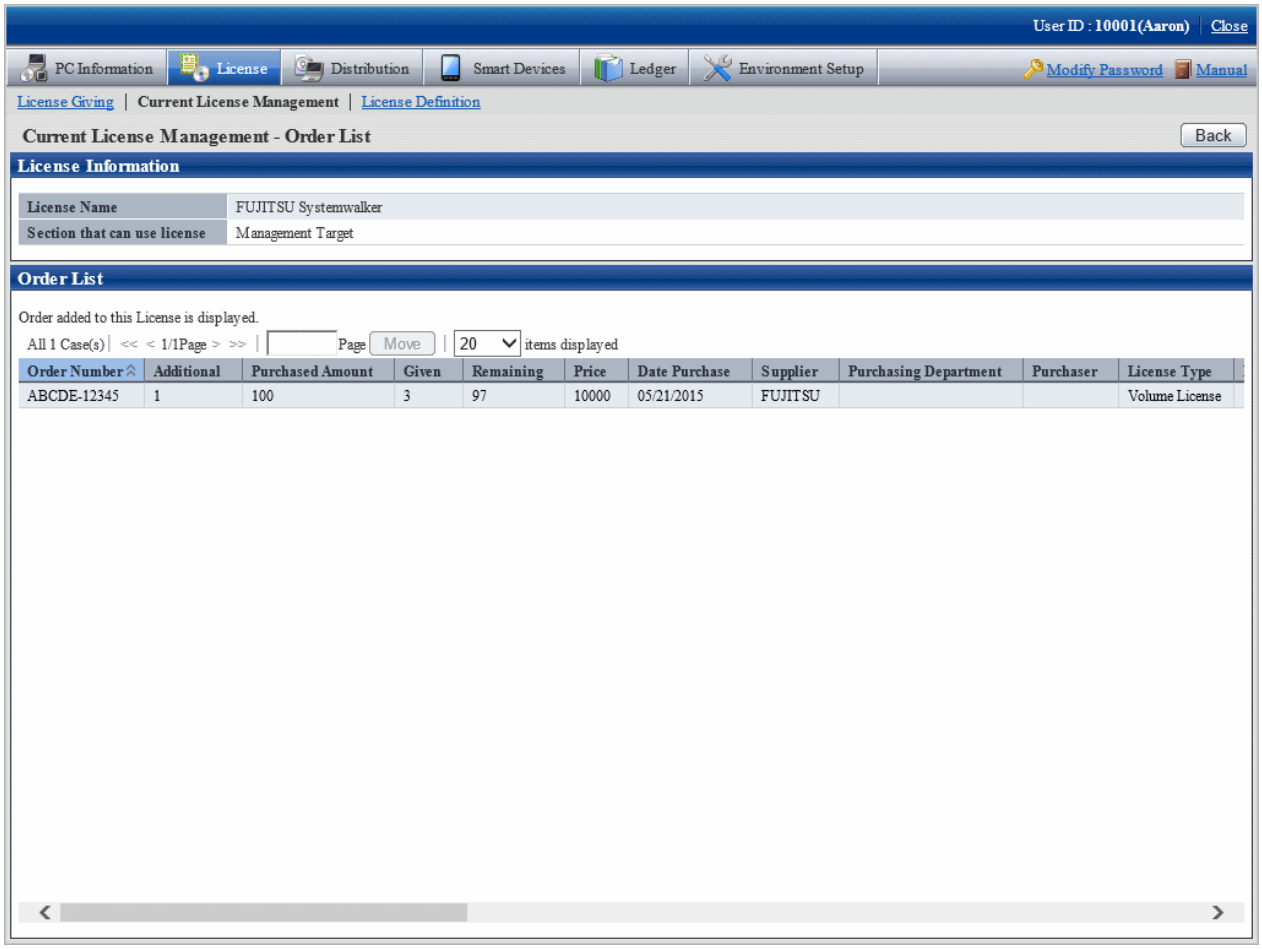
      The **Current License Management - CSV Export** window will be displayed.

   b. Export the license information to a file in CSV format according to the window.

5. Perform the following operations to view the registered License information in details. If not to view, proceed to the next step.

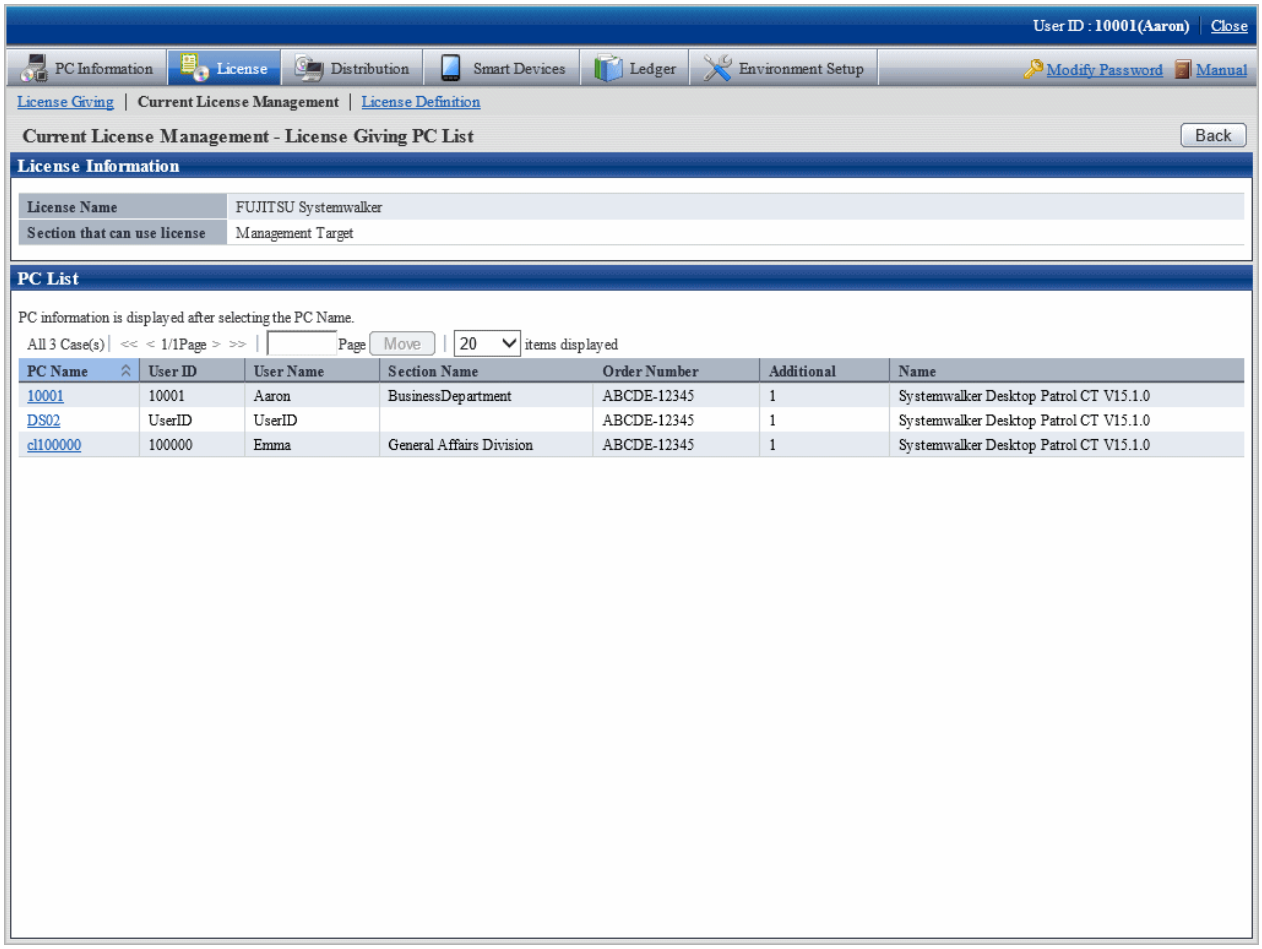
   a. Click the License Name to be viewed.

      The following window will be displayed. The details of registered License information can be viewed by order number.



b. Click the value in the column of **Number of Section Given**.

The following window will be displayed. It has nothing to do with order number, the detailed information of License Giving of section License Giving will be displayed.



5.3.1.1 Register Current License Information

In order to manage the purchased License, it is required to register License information.

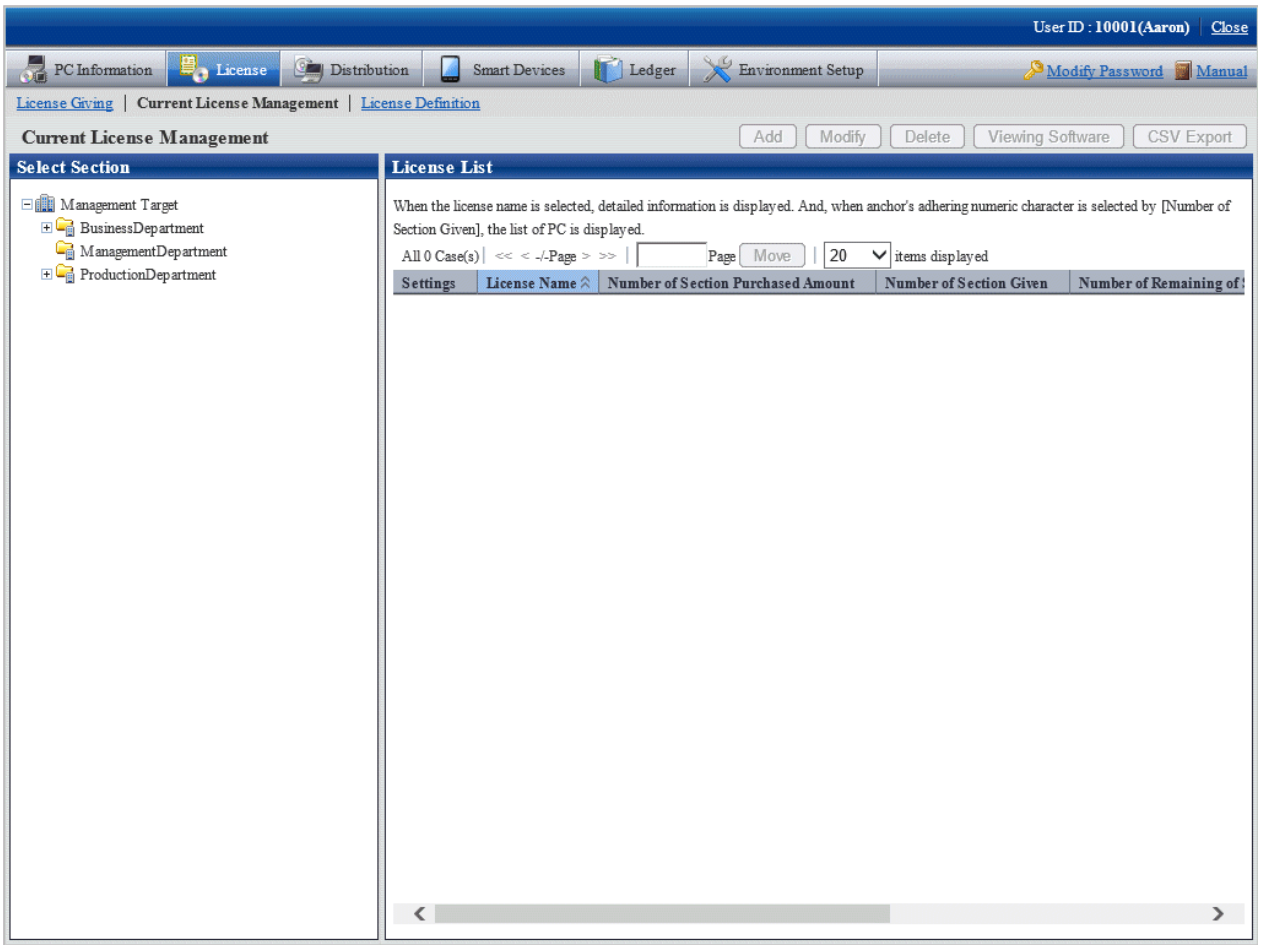
The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

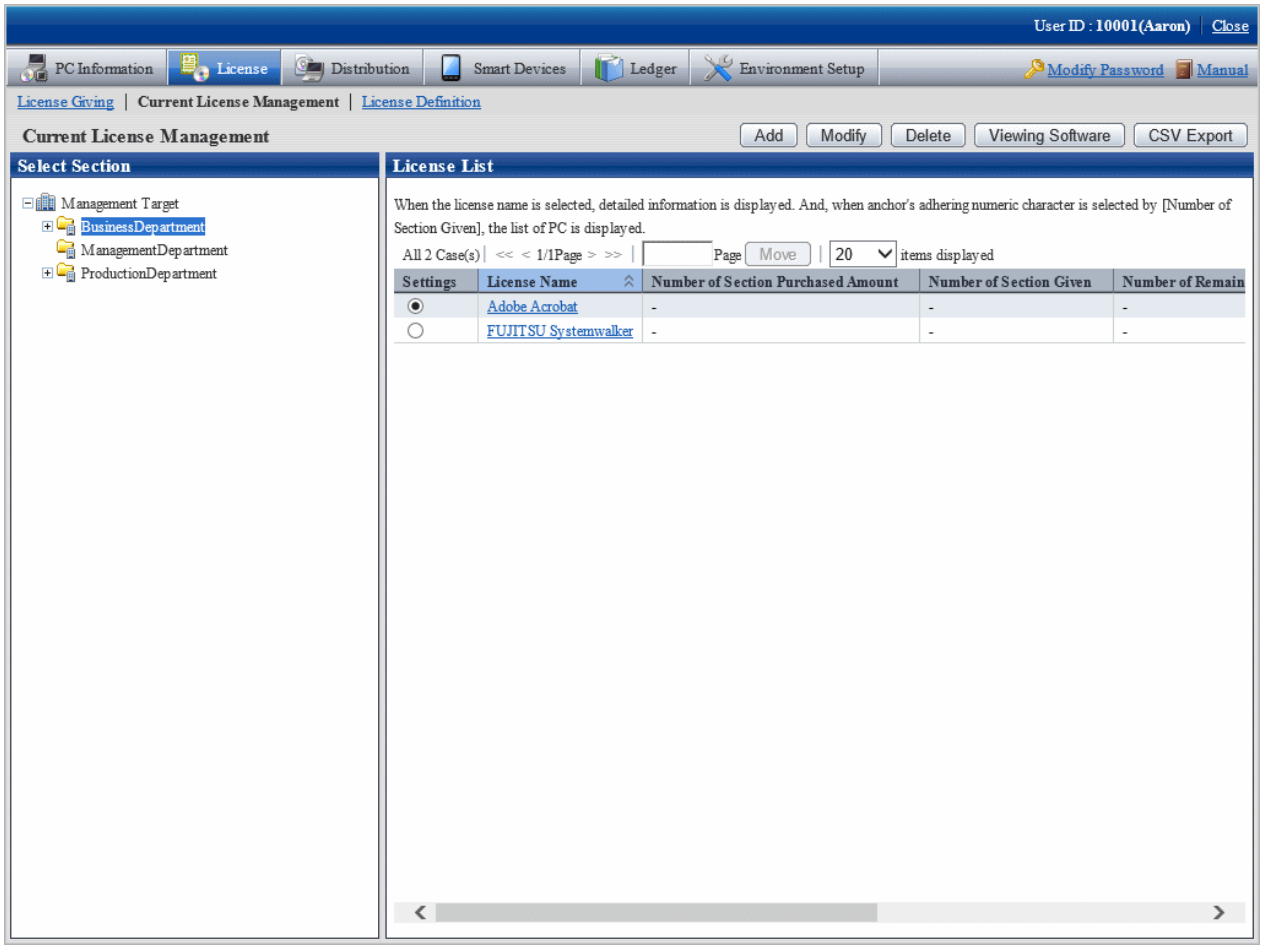
2. Click **Current License Management**.

   The following window will be displayed.



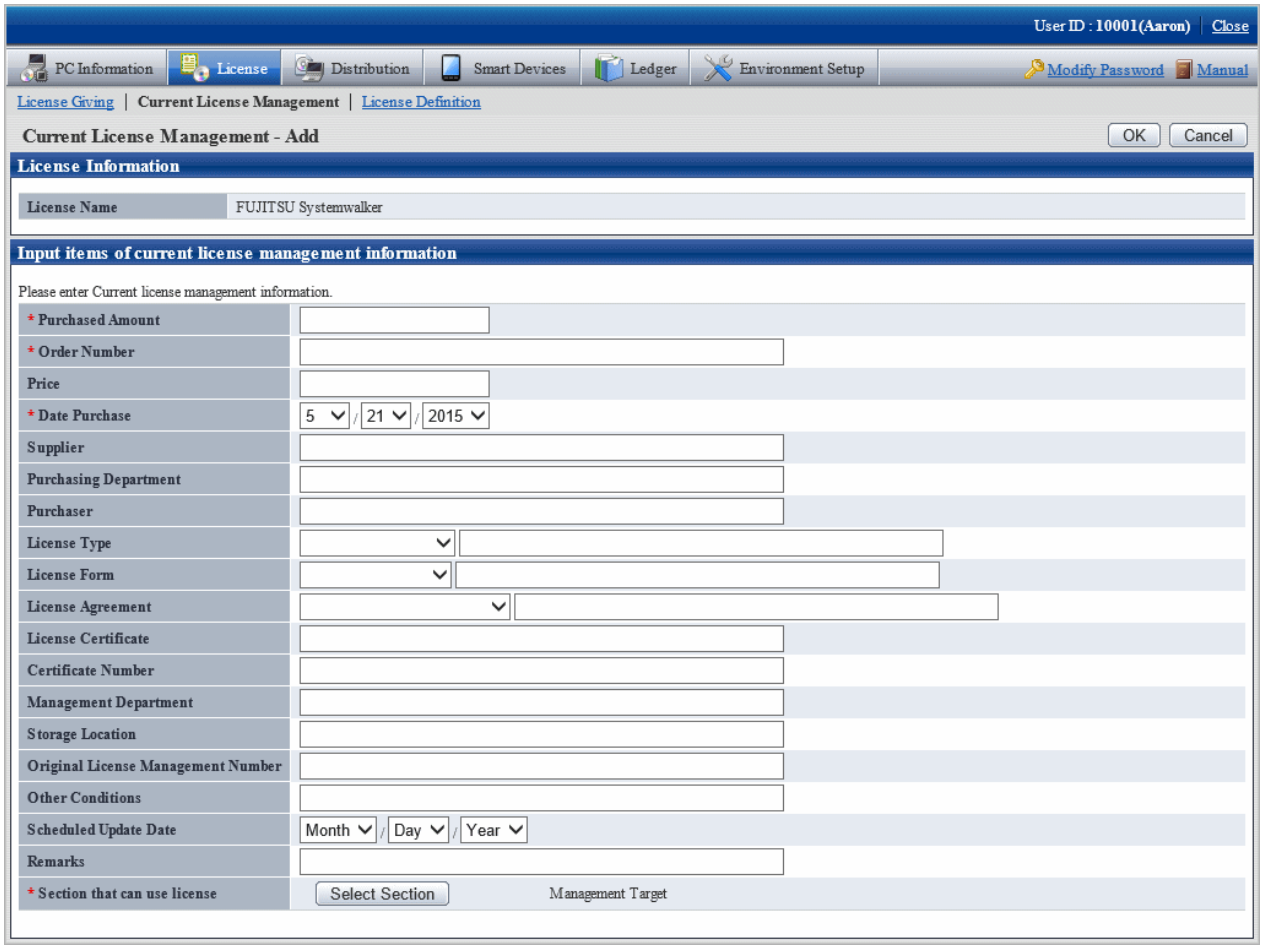
3. Select a section from the section tree in the field on the left.

   The License status of the selected section will be displayed in the field on the right.



4. Select the radio button of the purchased object from **License List** in the field on the right, and click the **Add** button.

   The following window will be displayed.



5. Enter the information of Current License Management.

Item	Description
Purchased Amount (required)	Specify purchased number of License. Single-byte numbers within 1~99999 can be entered.
Order Number (required)	Specify the order number to identify License. Single-byte numbers within 50 alphanumeric characters or hyphen "-" can be entered.
Price	Specify the Price of License. Single-byte numbers within 1~999999999 can be entered.
Date Purchase (required)	Specify the Date Purchase of License. The date from Jan. 1, 1900 to current date can be entered.
Supplier	Specify the contact who can certify the purchase history. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Purchasing Department	Specify information required for confirming the reason for the purchase and the purchase history.

Item	Description
	Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Purchaser	Specify the person who can confirm the reason for the purchase and the purchase history. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
License Type (*1)	Select one of the following license types: - Package license - Pre-install - Volume license - Other Use the text box on the right to enter the desired license type. Up to 30 fullwidth characters or 60 halfwidth characters can be entered.
License Form (*2)	Select one of the following license forms: - Full license - Upgrade license - Other Use the text box on the right to enter the desired license form. Up to 30 fullwidth characters or 60 halfwidth characters can be entered.
License Agreement (*3)	Select one of the following license agreements: - User-specific license - Processor license - Server license - Client access license - Concurrent connections license - License for the number of machines to be monitored - Site license - Other Use the text box on the right to enter the desired site license. Up to 30 fullwidth characters or 60 halfwidth characters can be entered.
License Certificate	Specify the products and information required for certifying the license. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Certificate Number	Specify the number of the license certificate.

Item	Description
	Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Management Department	Specify the department that manages the license. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Storage Location	Specify the location for storing the license. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Original License Management Number	If the license is not a full license, specify information about the original license. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Other Conditions	Specify conditions attached to the license, such as subscriptions (annual contracts) and whether downgrades are possible. Up to 100 fullwidth characters or 200 halfwidth characters can be entered.
Scheduled Update Date	Specify the update date if the license has an expiry date. A date on or after January 1, 1900 can be entered.
Remarks	Specify information relating to the license. Up to 2,048 fullwidth characters or 4,096 halfwidth characters can be entered.

6. *1: The license types are as follows:

Item	Description
Package license	A license that permits installation on one computer per product purchased.
Pre-install	A license that comes with a purchased computer.
Volume license	A license whose price is determined according to the scale, such as the number of users and computers using the software.

*2: The license forms are as follows:

Item	Description
Full license	A license that permits the new installation of the software.
Upgrade license	A license that permits the upgrade installation of the software.

*3: The license agreements are as follows:

Item	Description
User-specific license	A license required for each user who will use the software.
Processor license	A license required for each processor of the computer where the software will be installed.
Server license	A license required for each server that will use the software.
Client access license	A license required for each client that will access the server.

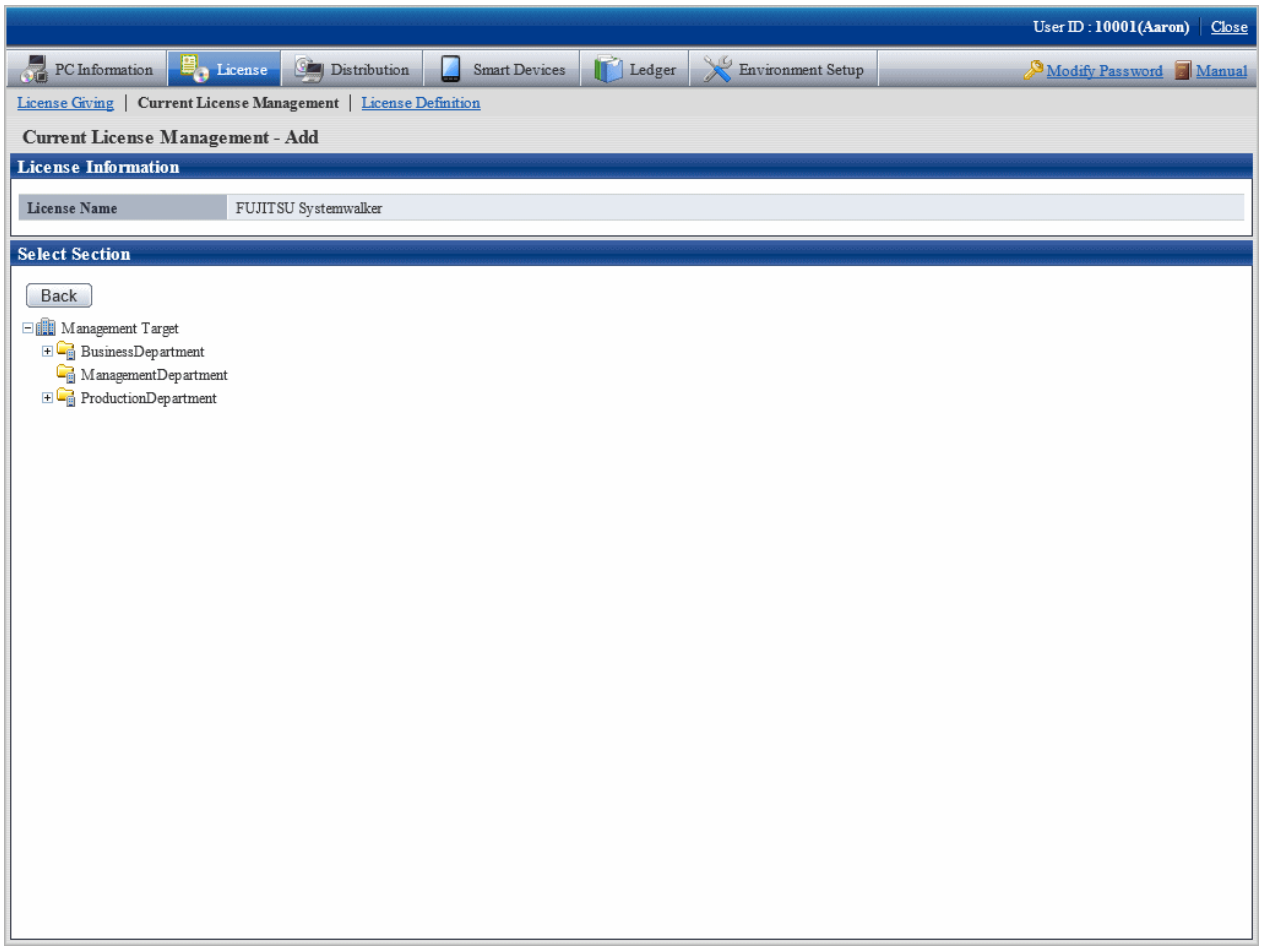
Item	Description
Concurrent connections license	A license required according to the number of users who will connect concurrently.
License for the number of machines to be monitored	A license required according to the number of machines to be monitored by the software.
Site license	A license required for each organization that will use the software.

7.

8. Perform the following operations to modify the section that can use the License. If not to modify, proceed to the next step.

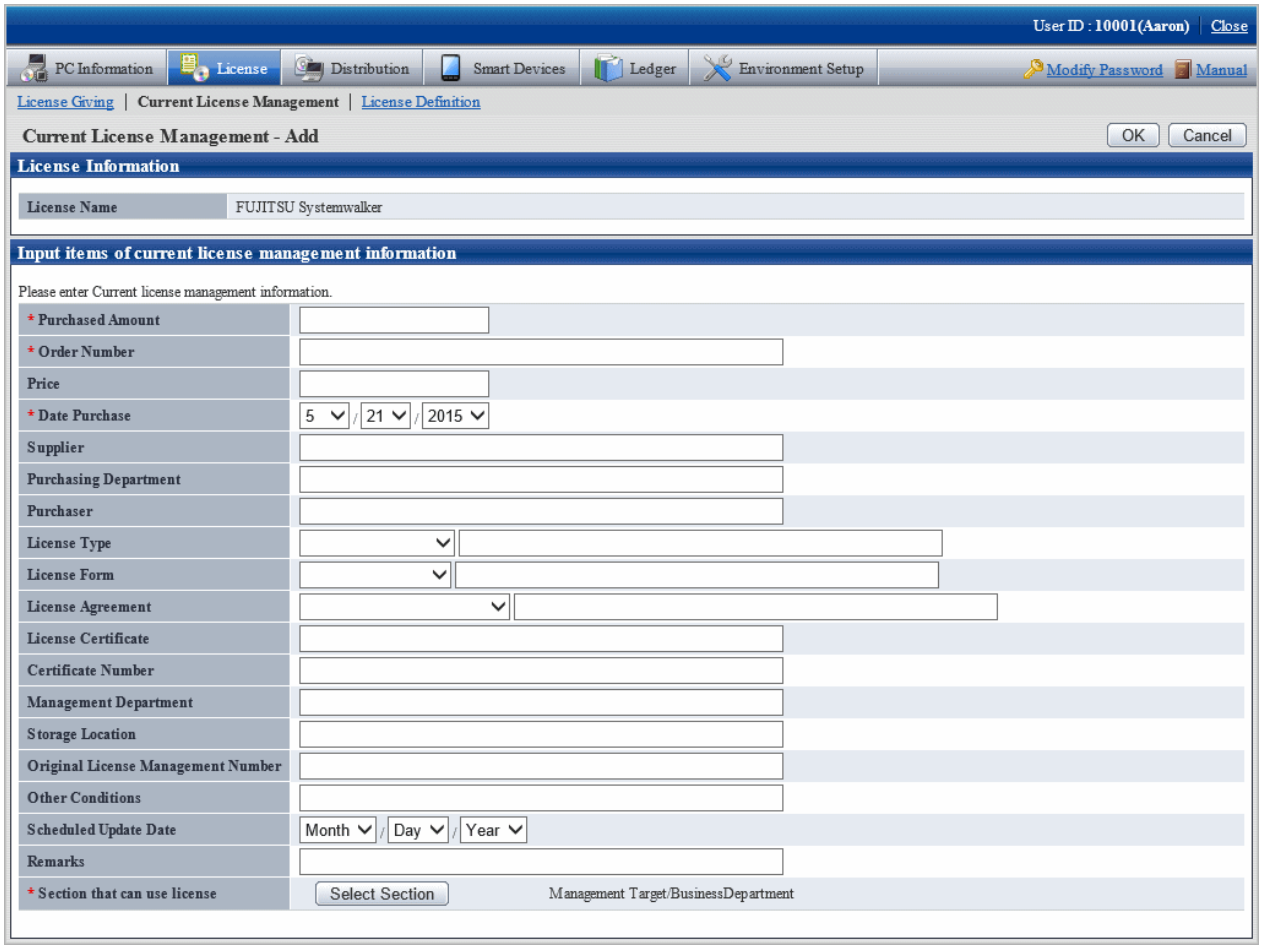
   a. Click the **Select Section** button.

      The following window will be displayed.



b. Select the section to be modified from the tree.

The following window will be displayed.



9. Click the **OK** button.

   The information of purchased License will be registered.

5.3.1.2 Modify Information of Current License

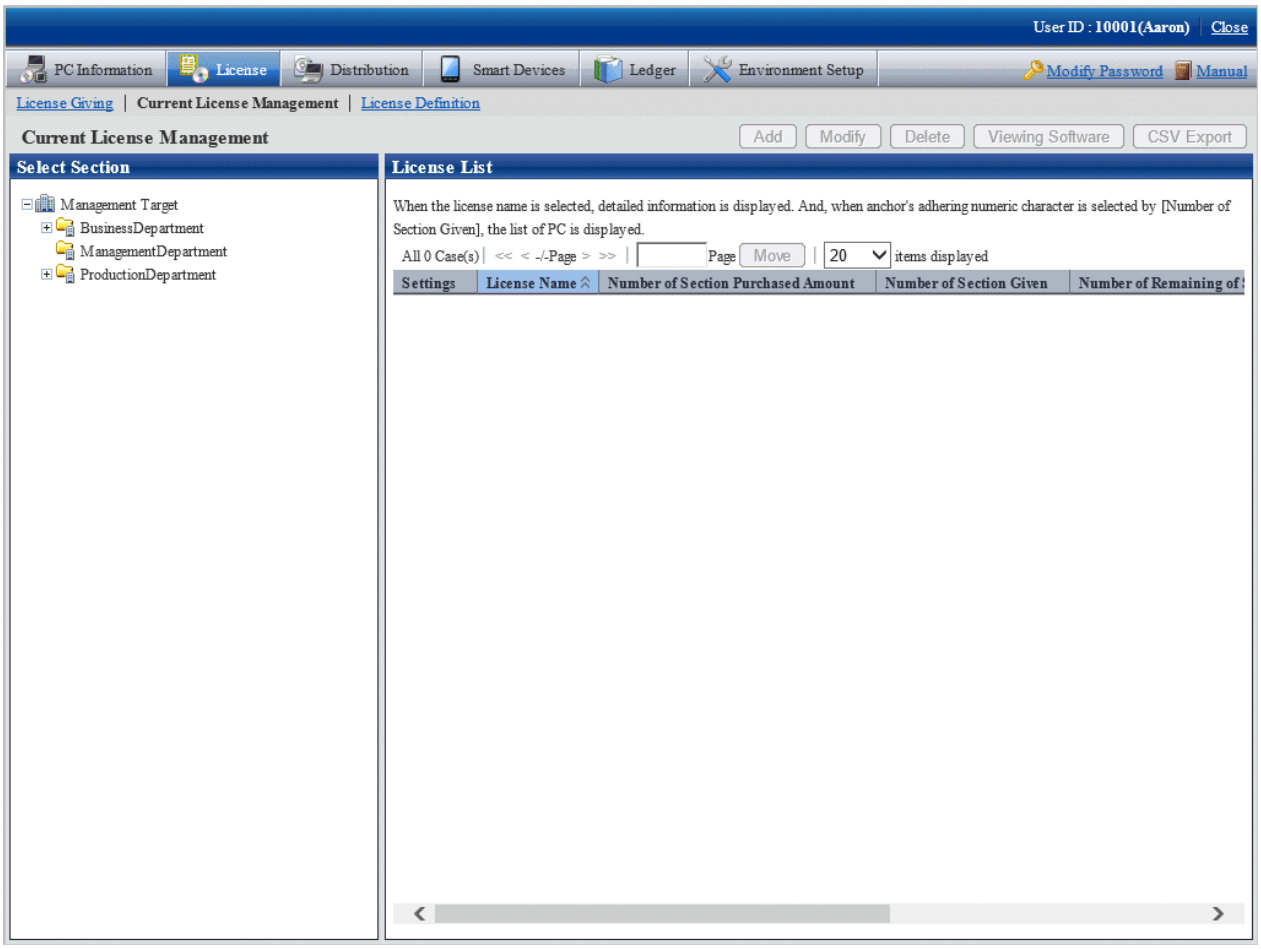
After registering information of current License, the information of purchased License modified and added. The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

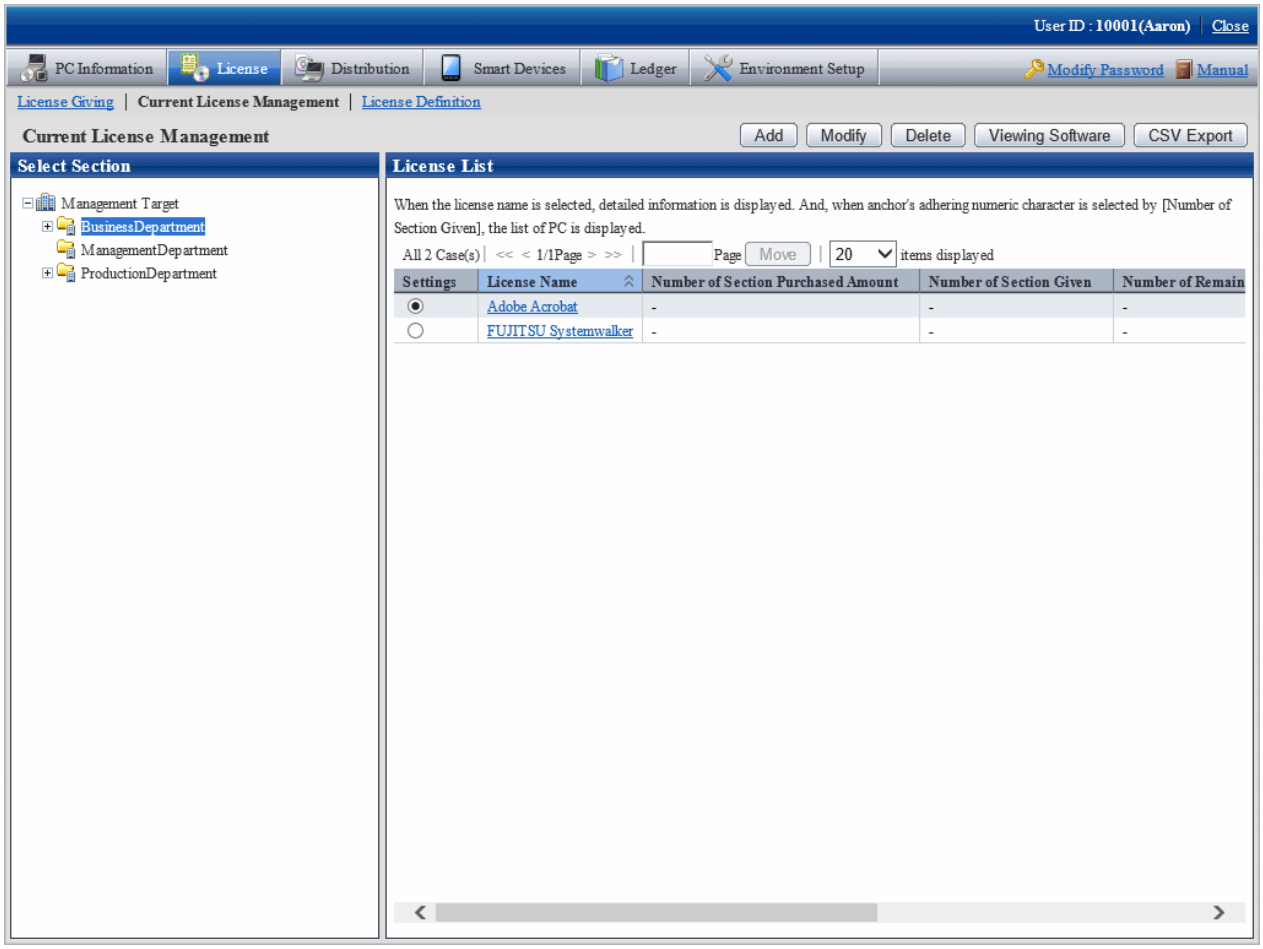
2. Click **Current License Management**.

   The following window will be displayed.



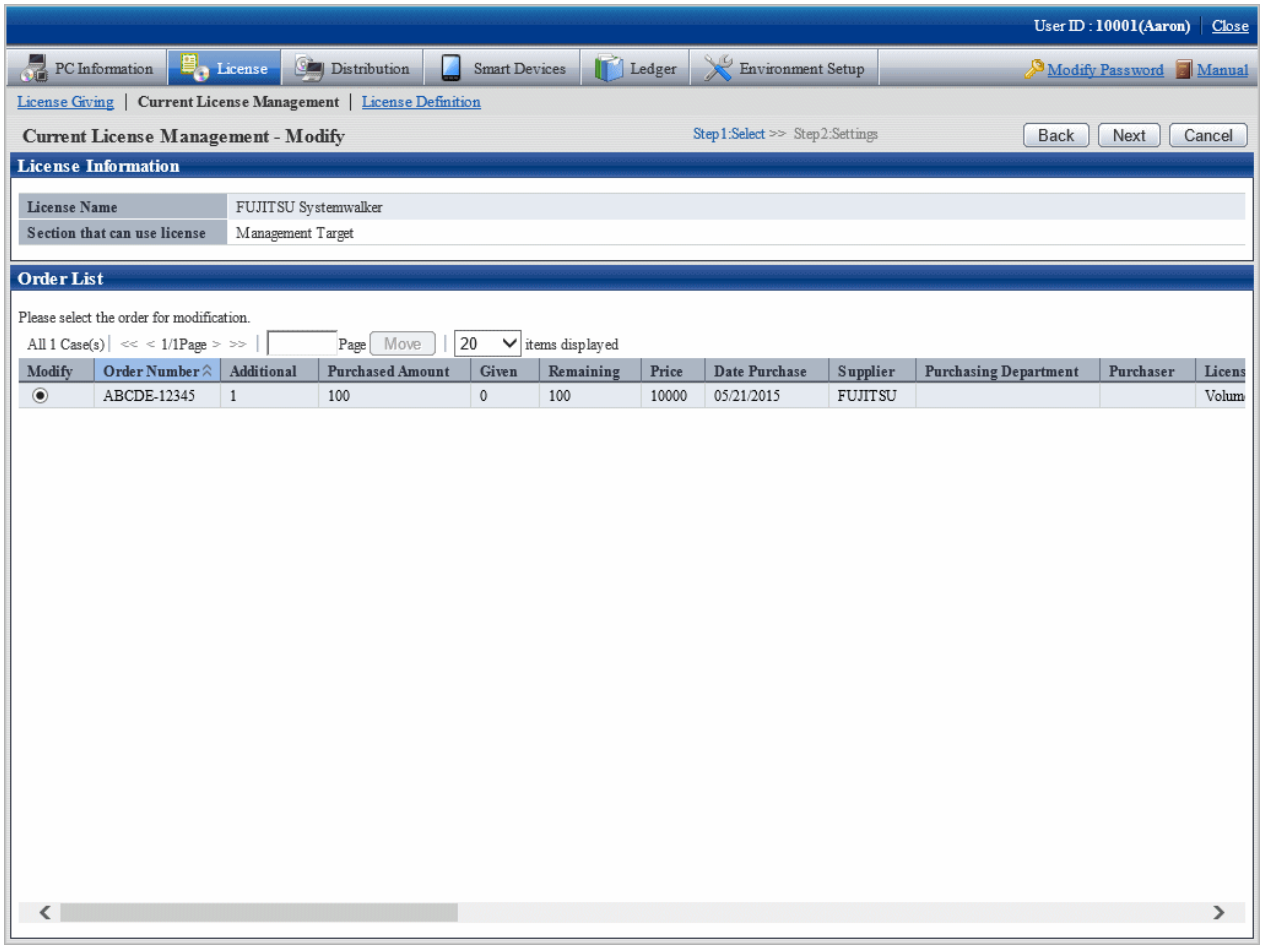
3. Select section from the section tree in the field on the left.

   License status of the selected section will be displayed in the field on the right.



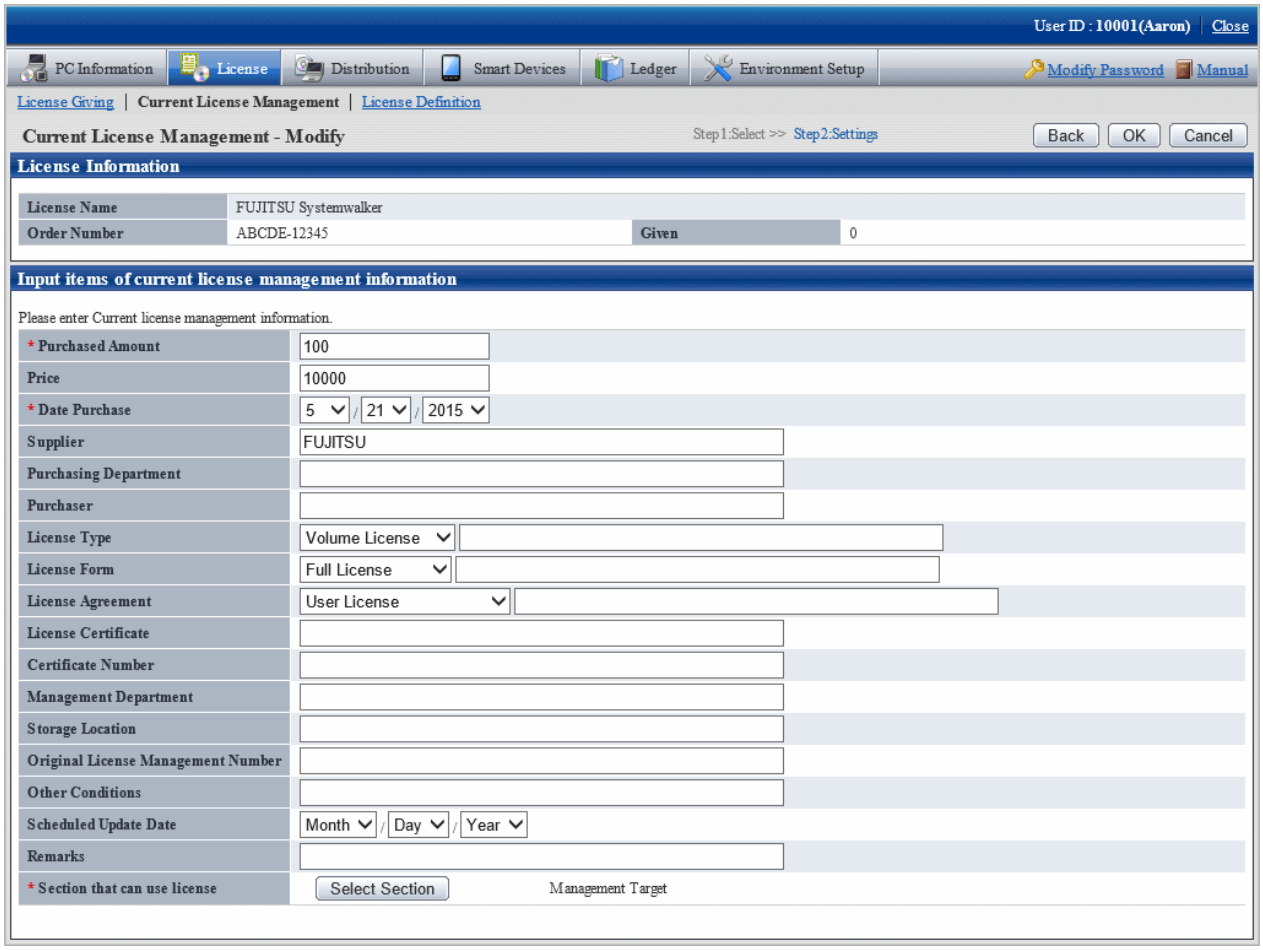
4. Select the radio button of License name of object to be modified from the **License List** in the field on the right, click the **Modify** button.

   The following window will be displayed. This window is for selecting the license to be modified by registered order number.



5. Select the radio button of order number to be modified, and click the **Next** button.

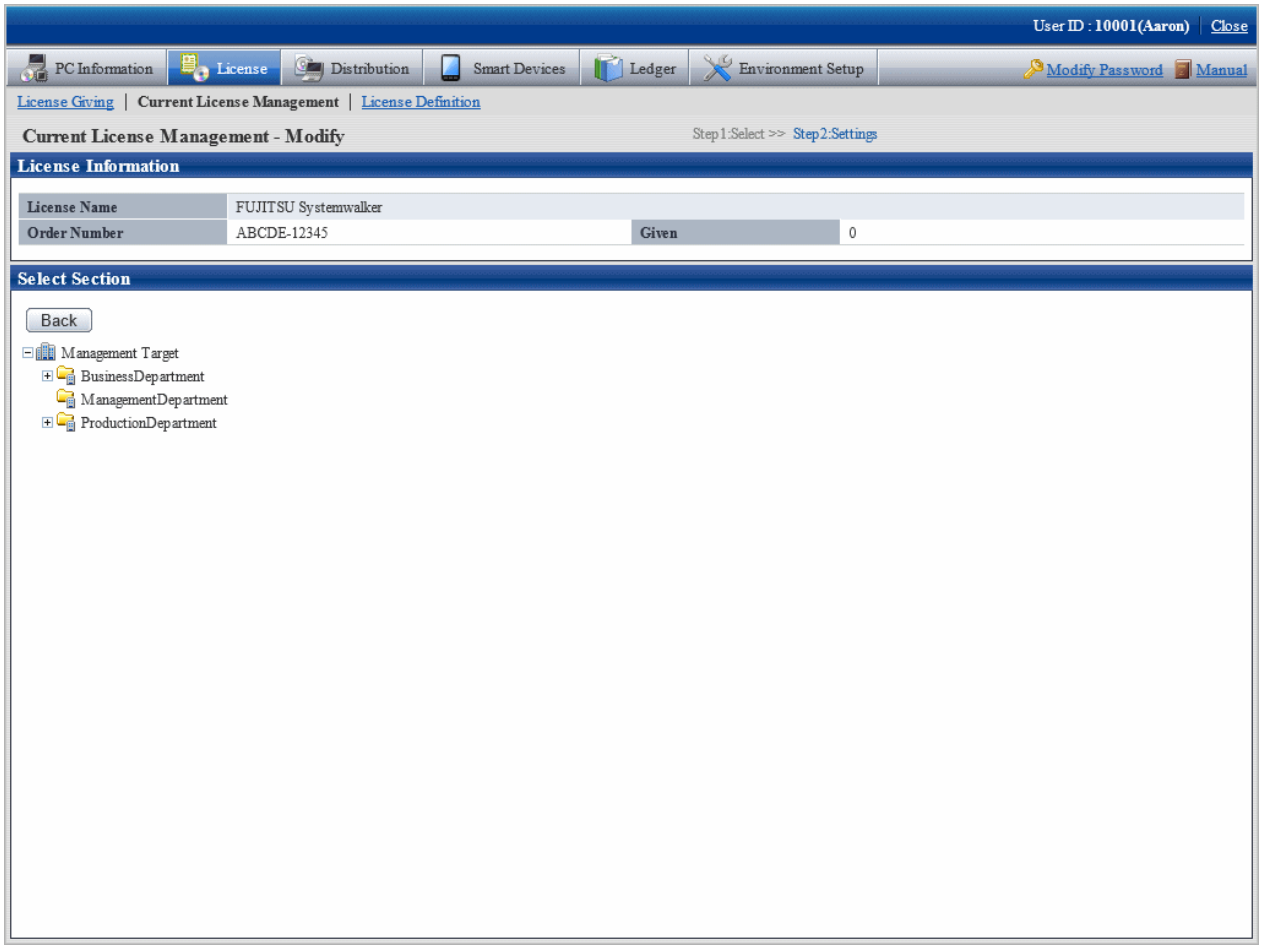
   The **Current License Management - Modify** window will be displayed.



6. Perform the following operations to modify the section to purchase License. If not to modify, proceed to the next step.

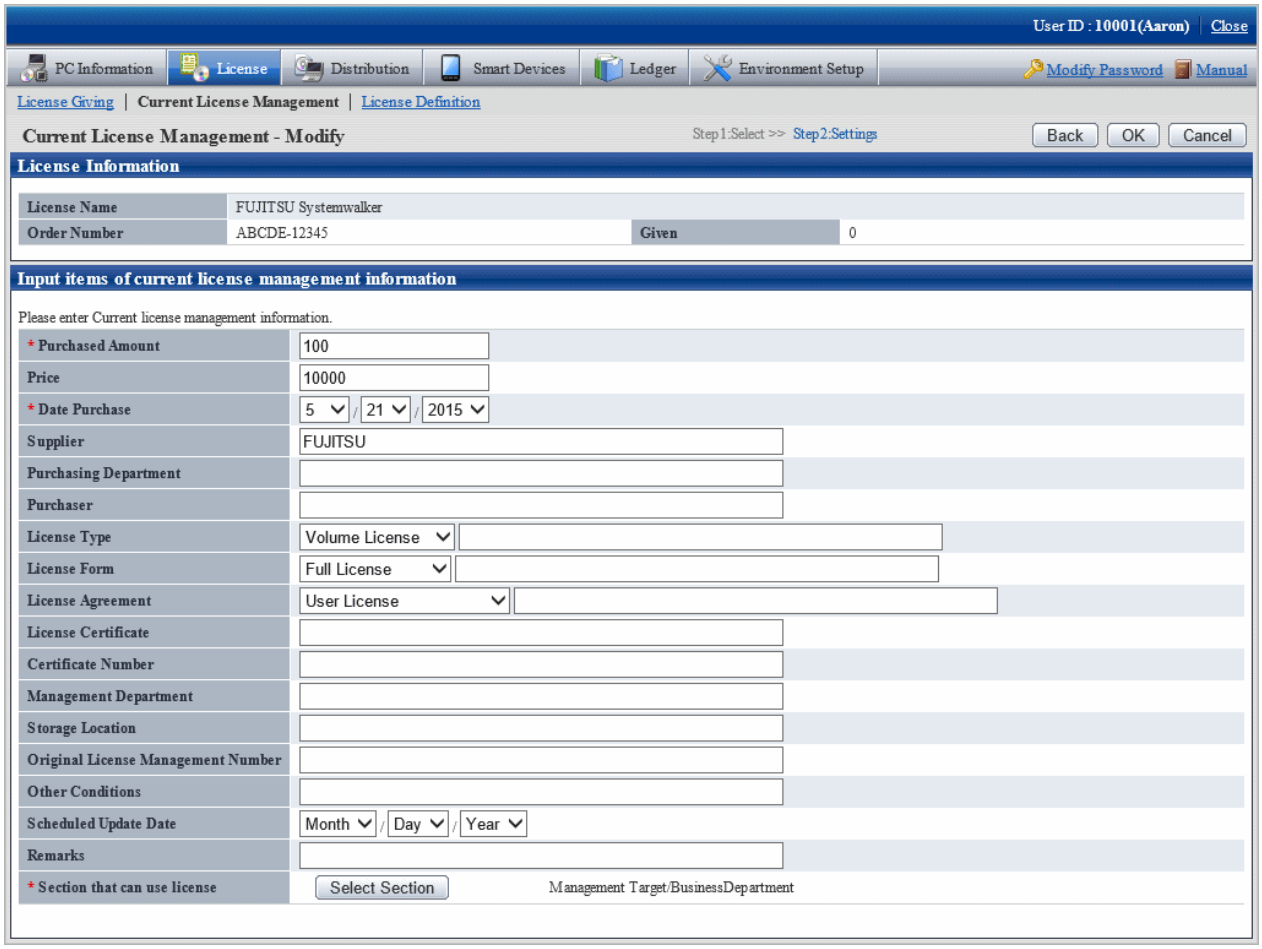
   a. Click the **Select Section** button.

      The following window will be displayed.



b. Select the section to be modified.

The following window will be displayed.



7. Click the **OK** button.

   The information of purchased License will be modified.

5.3.1.3 Delete Current License

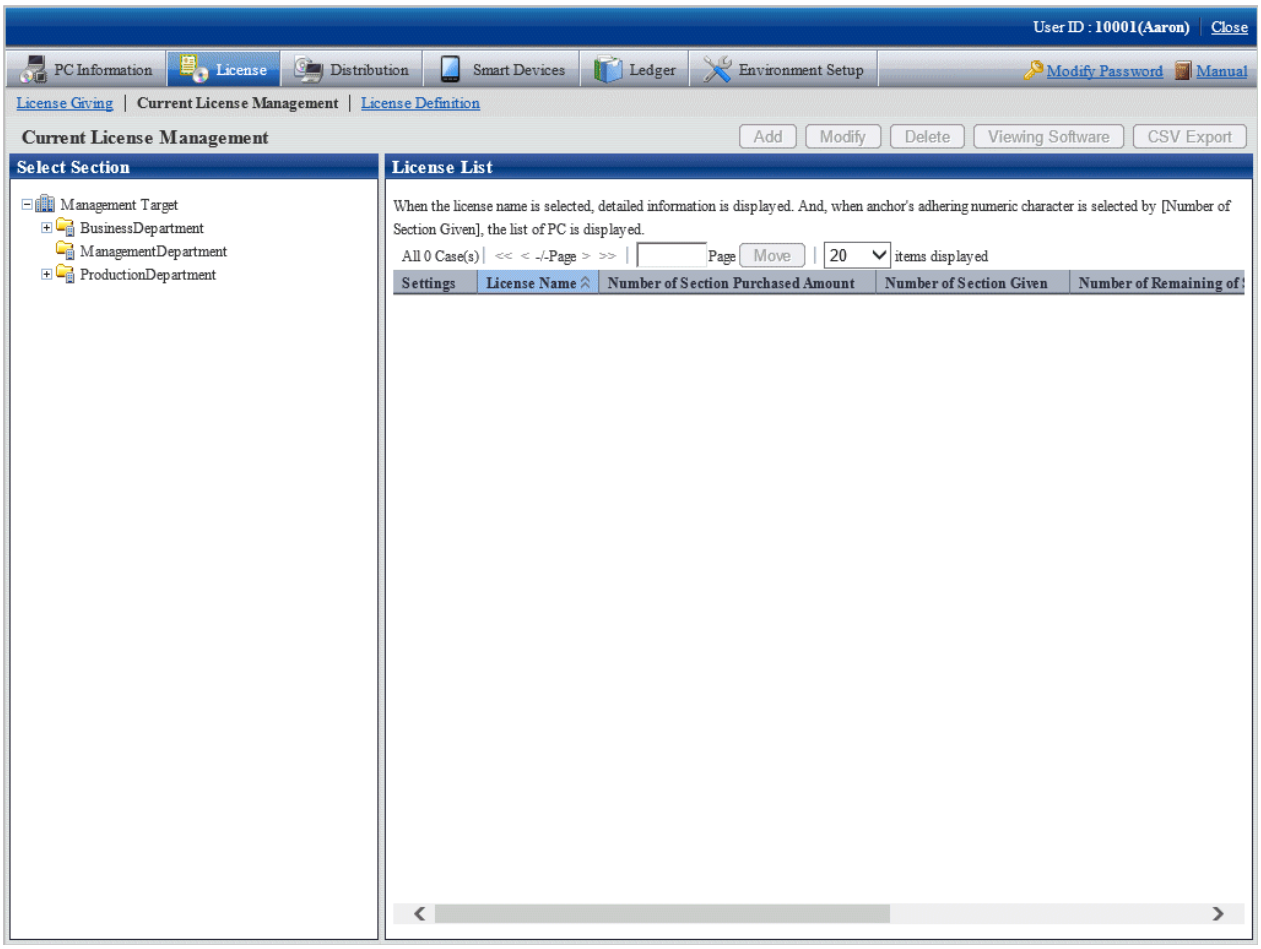
Unwanted License can be deleted. The procedure is as follows.

1. Log in to the main menu, and click **License**.

   The **License** window will be displayed.

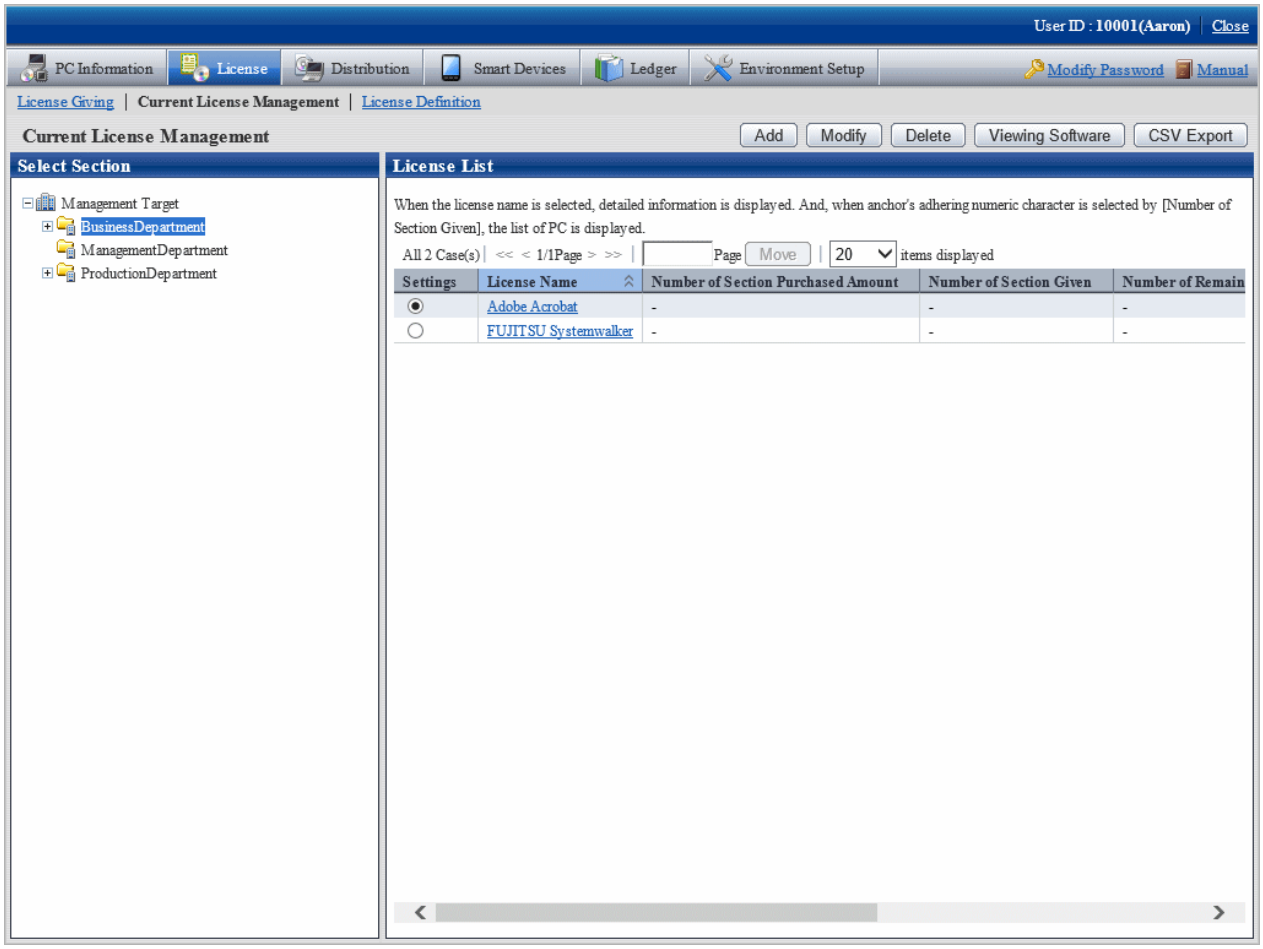
2. Click **Current License Management**.

   The following window will be displayed.



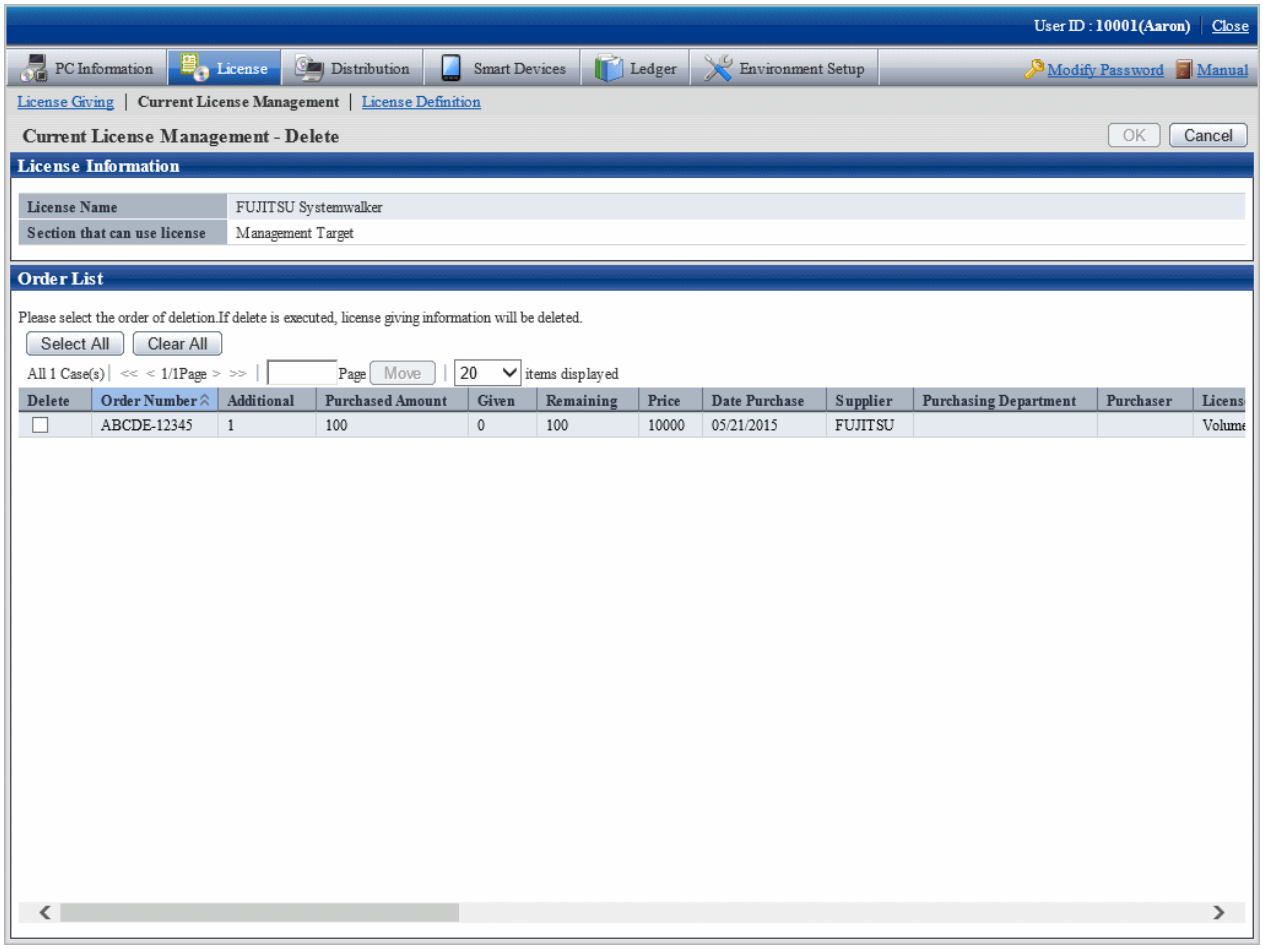
3. Select a section from the section tree in the field on the left.

   The License status of the selected section will be displayed in the field on the right.



4. Select the radio button of License name to be deleted from **License List** in the field on the right, and click **Delete** button.

   The following window will be displayed. This window is for selecting the License to be deleted by the registered order number.



5. Select the check box of order number to be deleted, and click the **OK** button.

   The License will be deleted.

5.3.1.4 View the Registered Software in Current License

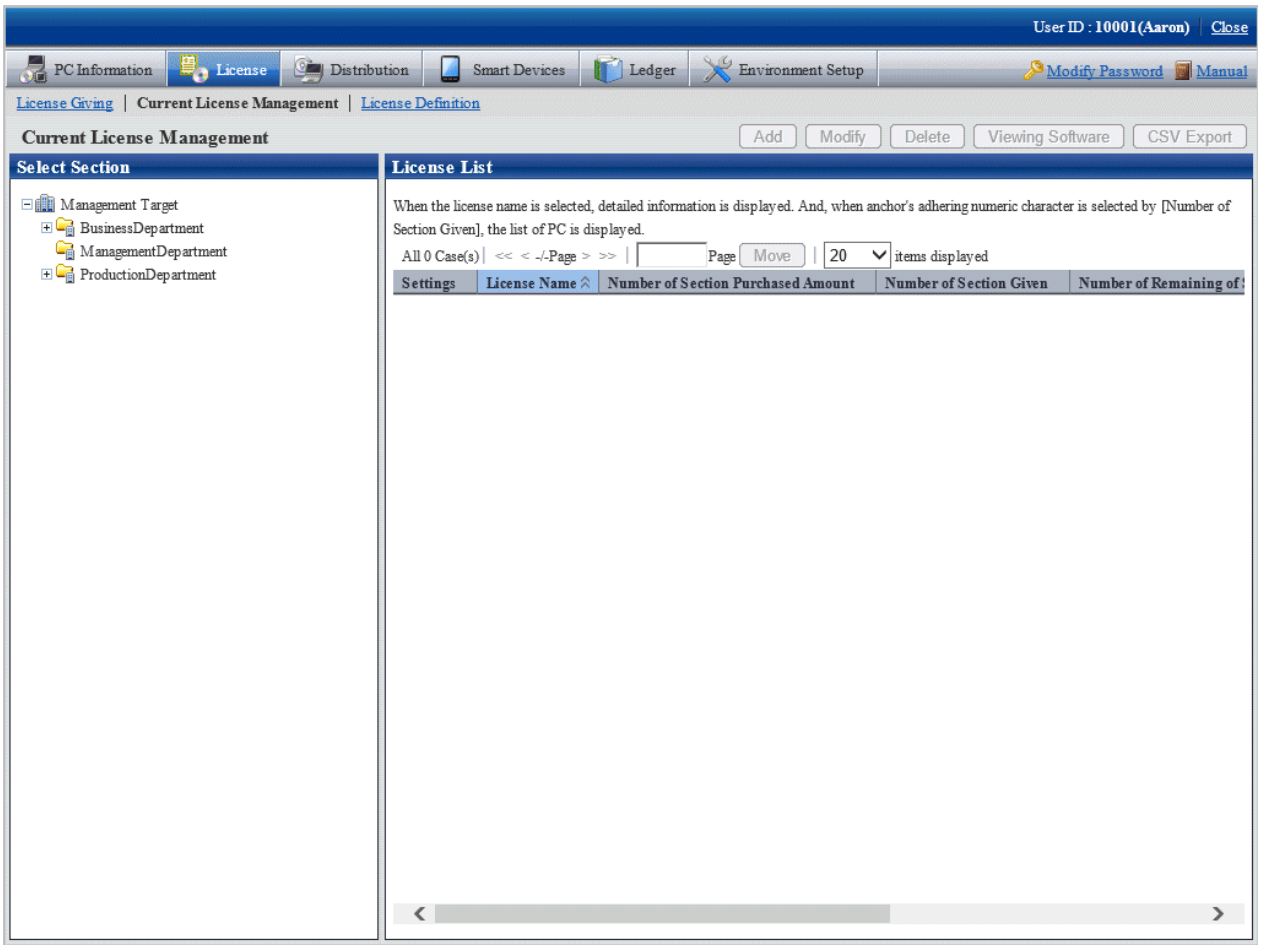
Software registered in License can be viewed. The procedure is as follows.

1. Log in to the main menu, and click **License**.

   The **License** window will be displayed.

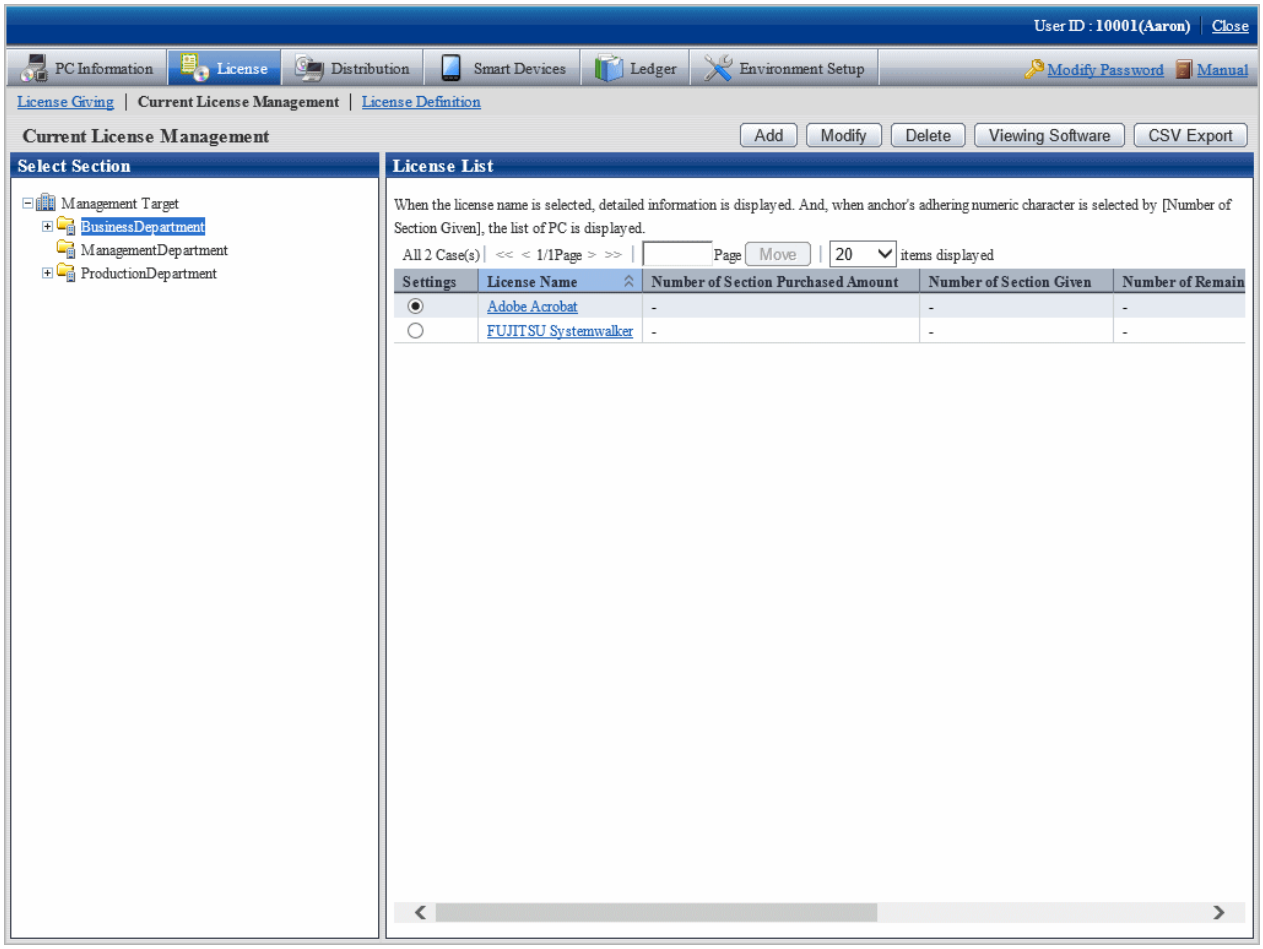
2. Click **Current License Management**.

   The following window will be displayed.



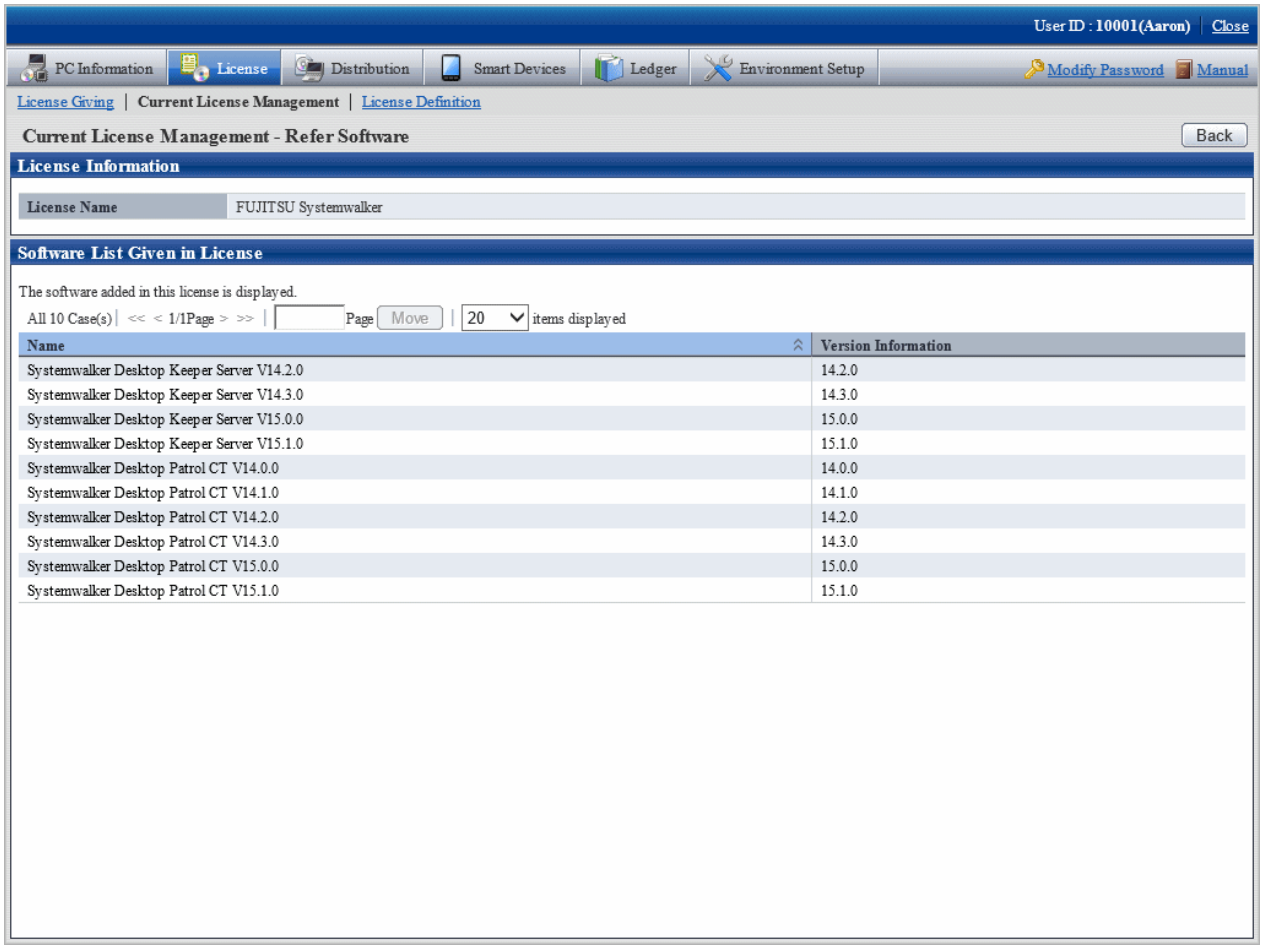
3. Select a section from the section tree in the field on the left.

   License status of the selected section will be displayed in the field on the right.



4. Select the radio button of the License name to be viewed from **License List** in the field on the right, and click the **View Software** button.

   The following window will be displayed.



5. Click **License Definition** to confirm the selected License Giving software.

5.3.2 Allocate License

To manage and operate License, It is necessary to allocate License registered in "5.3.1.1 Register Current License Information".

This chapter describes how to allocate License and cancel the unwanted License.

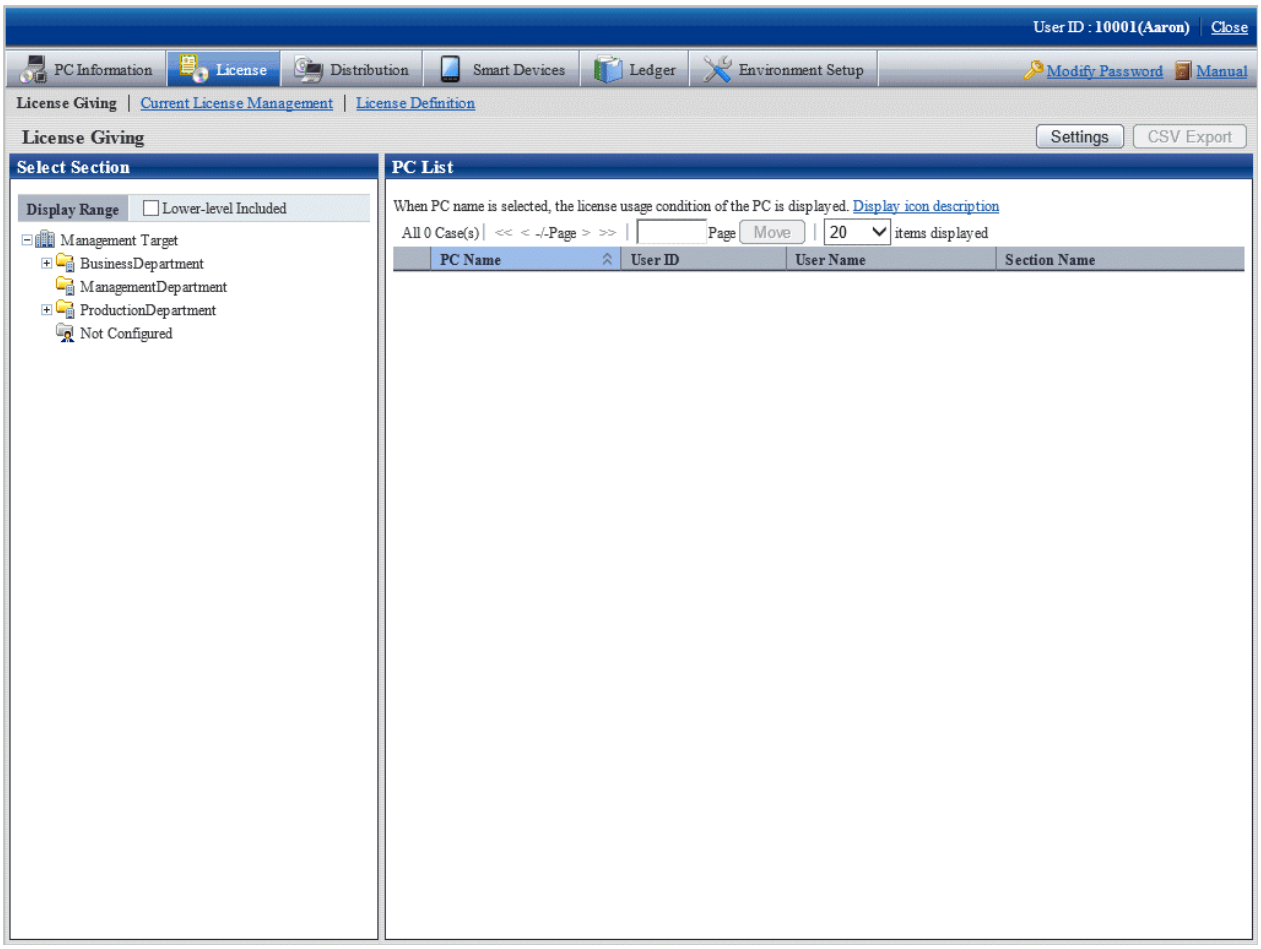
The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

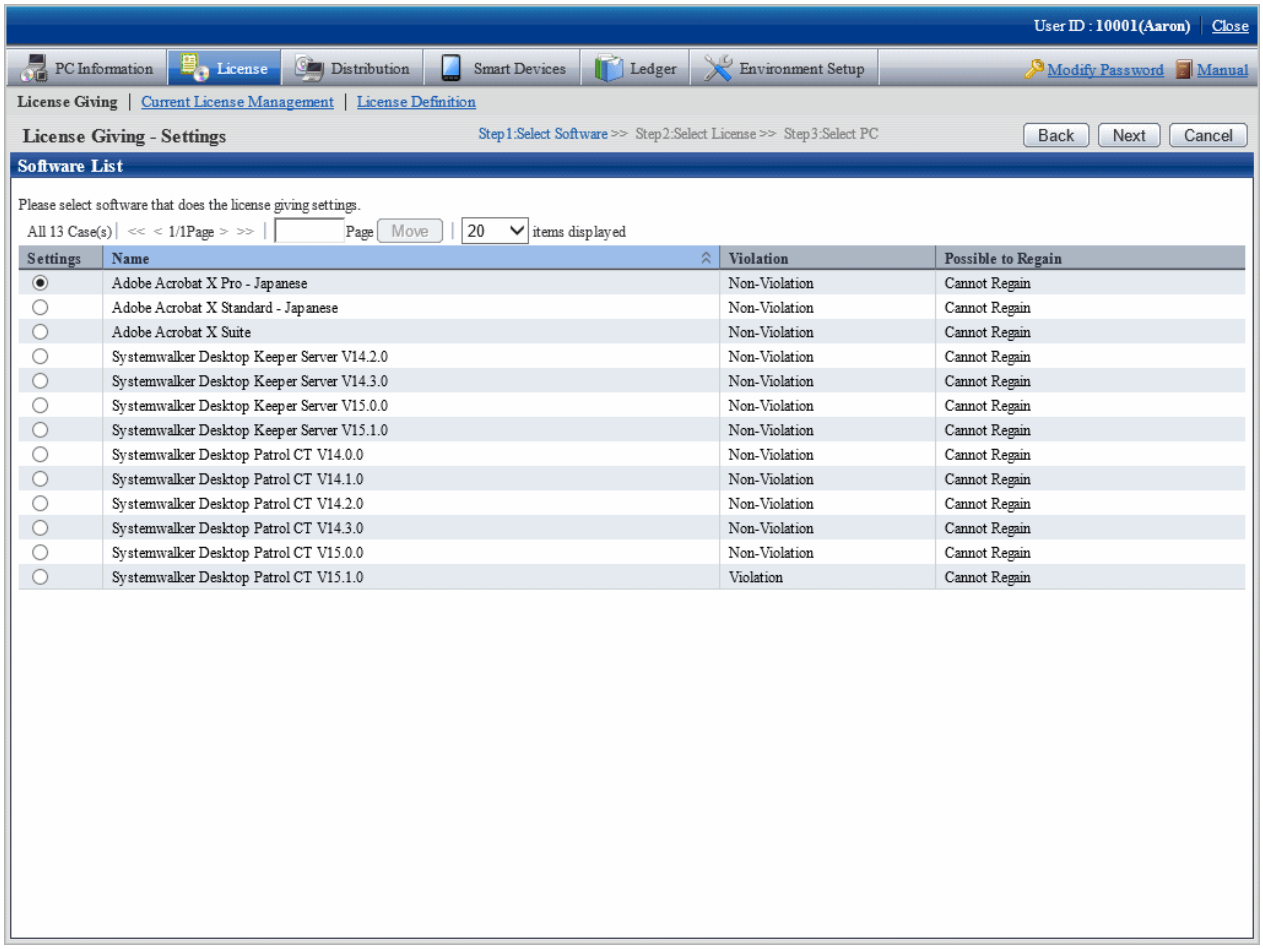
2. Click the **License Giving**.

   The following window will be displayed.



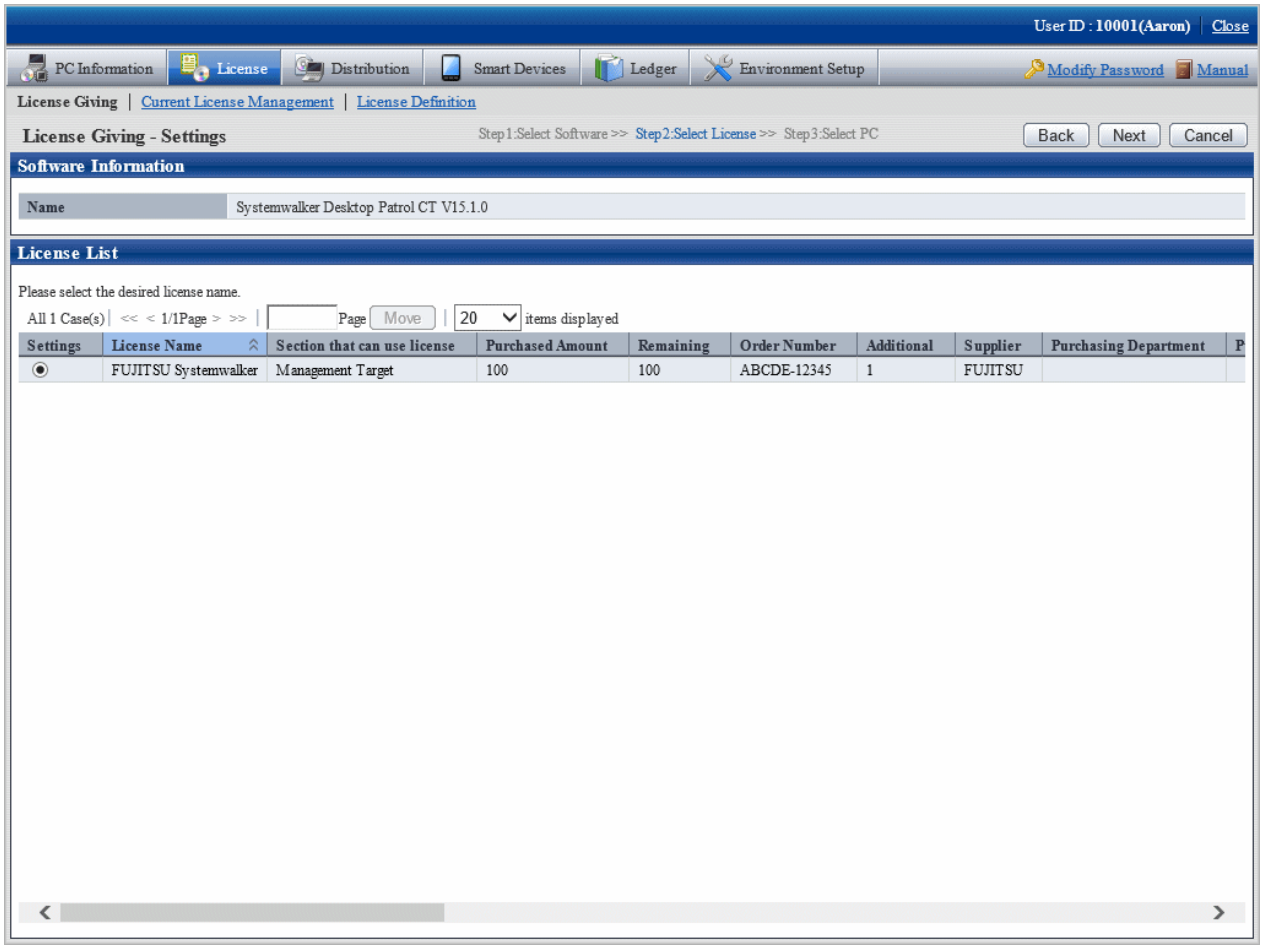
3. Click the **Settings** button.

   The following window will be displayed.



4. Select the radio button of software name to be allocated from the software list, and click the **Next** button.

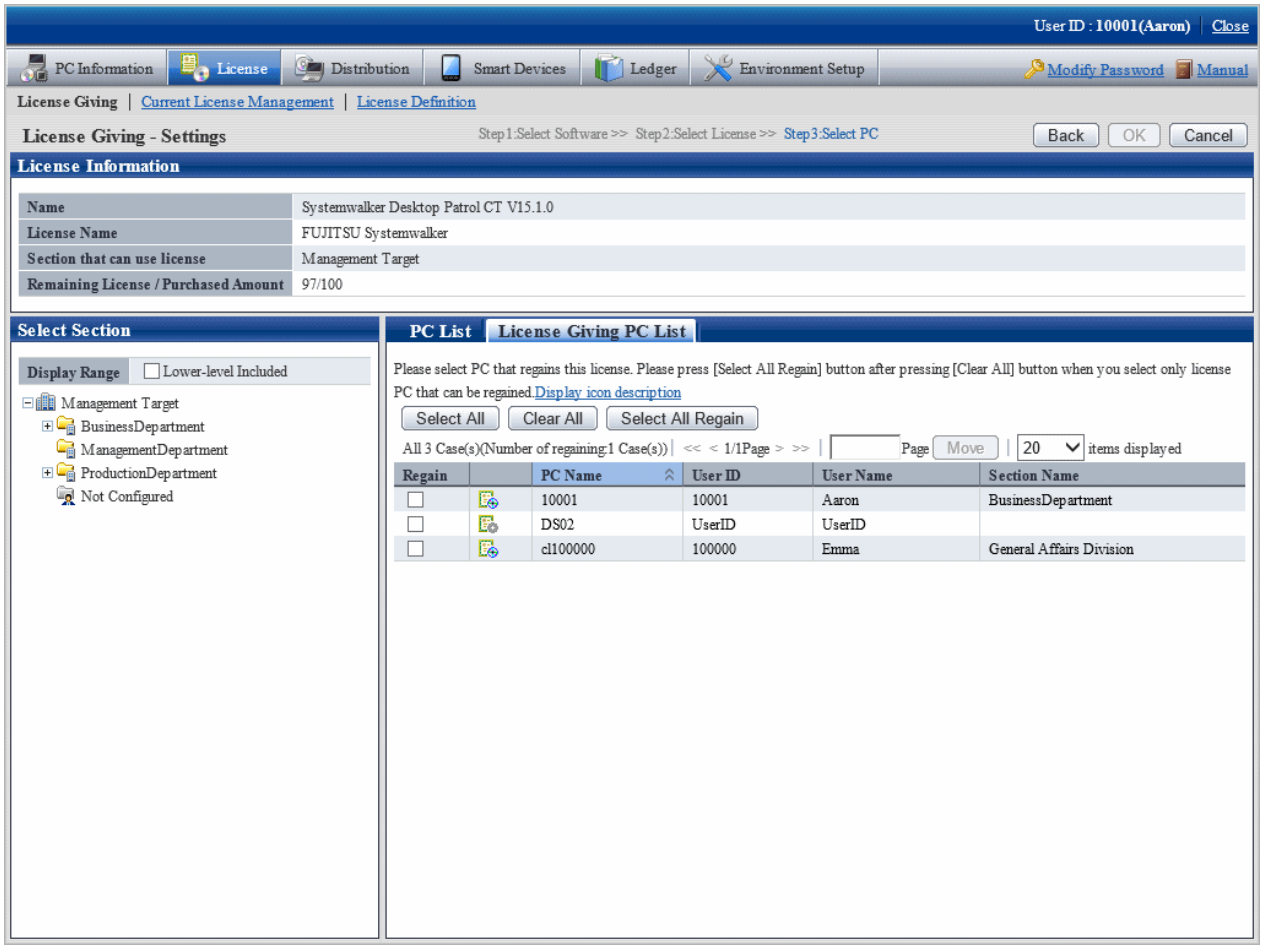
   The License List will be displayed.



   The higher purchasing section to which the user belongs to will be displayed when logging in with the section management account.

5. Select the radio button of License name to be allocated, click **Next** button.

   The following window will be displayed.



6. Select the section as object for allocation from the section tree in the field on the left.

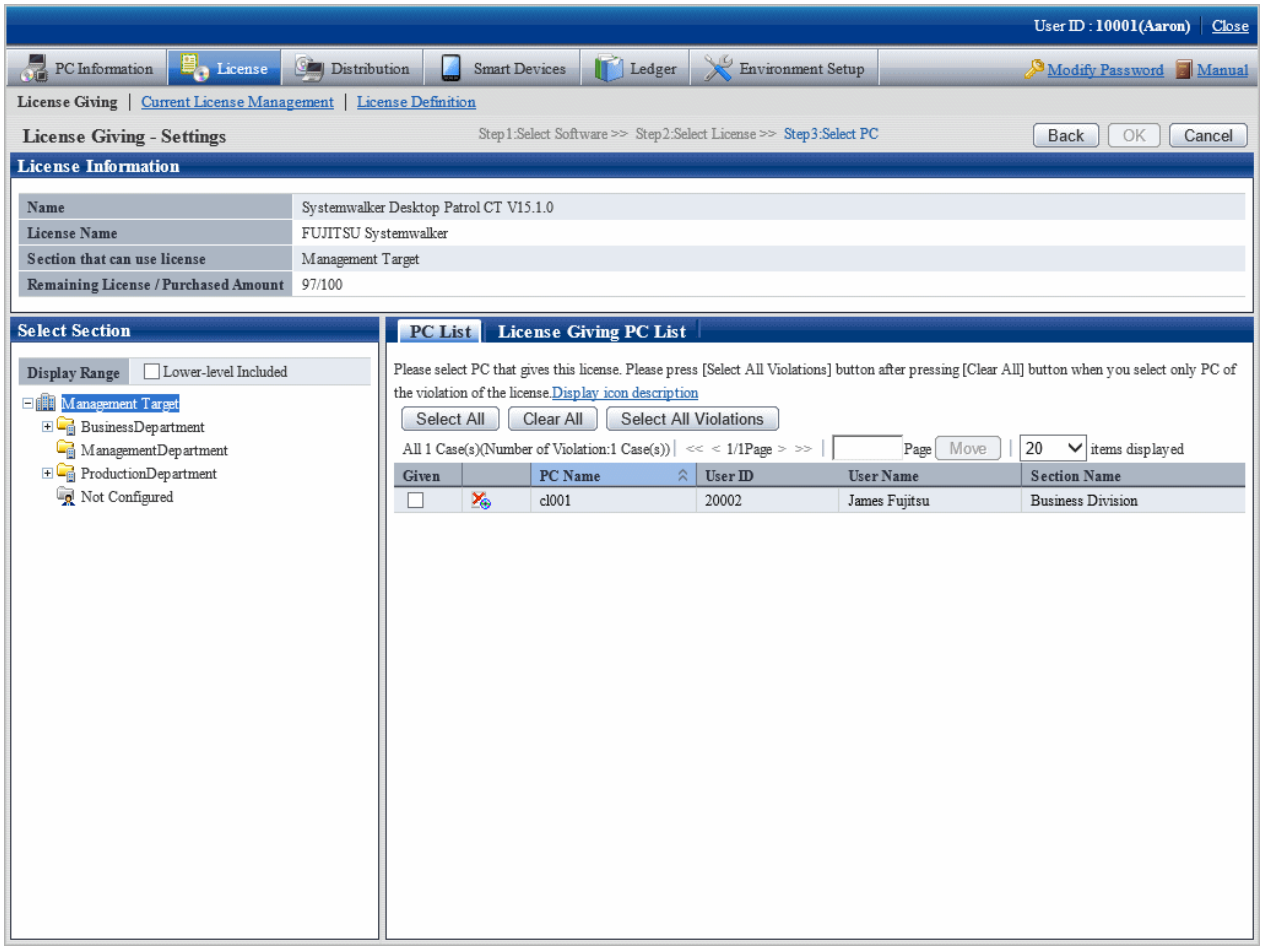
   PCs under the selected section will be displayed in the field on the right.

   PCs displayed in the section tree are all the ones belonging to the purchasing section specified in step "5.".

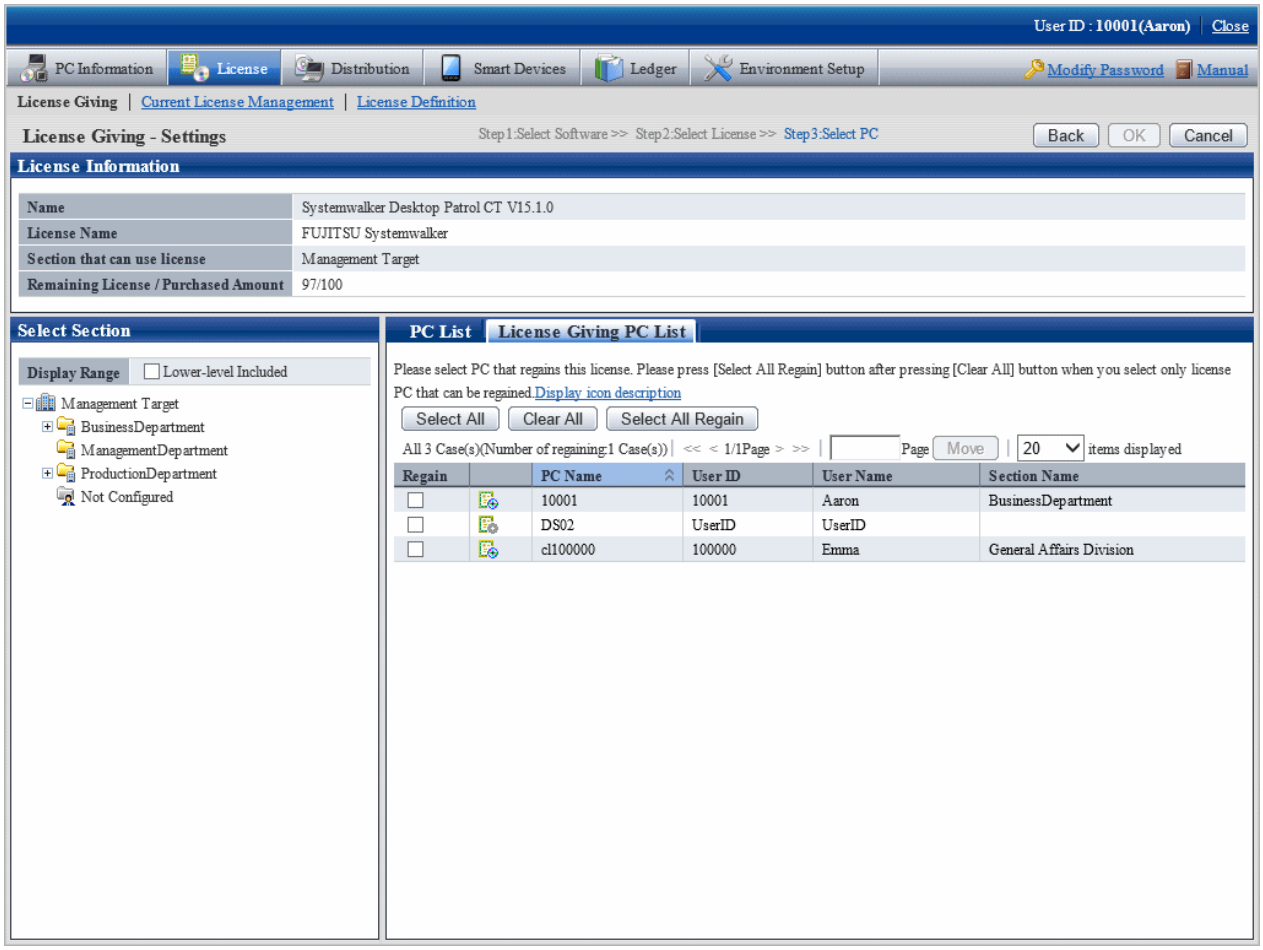
   Only all the PCs of the section to which the login user belongs will be displayed even it is the higher purchasing section specified in step "5." when logging in with the section management account.

7. Select the check box of PC to be allocated with License from the PC list, click the **OK** button.

   When the License violation PC is to be selected, click the **Select All Violations** button. All the check boxes of License violation PC will be selected.



8. To return License, click the **License Giving PC List** tab, and click the **Select All Regain** button. The check box of all PCs with License given but not imported will be selected.



5.3.3 Set as Needed

Perform the following operations as needed after confirming the License violation PC.

- When purchasing software
- When purchasing license
- When discarding license

5.3.3.1 When Purchasing Software

It's necessary to register the newly defined License or register the purchased software to the defined License when purchasing software. Perform the operations of **Add** or **Modify** in **License** > **License Definition** in main menu.

Consult "System Administrator" to register software.

5.3.3.2 When Purchasing License

Change License purchased number in **License** > **Current License Management** in main menu when purchasing License.

Refer to "5.3.1.2 Modify Information of Current License" for correction method.

5.3.3.3 When Discarding License

Instruct the client using the discarded License to uninstall the software allocated in License. Then discard this License from **License** > **License definition** in main menu.

Consult "System administrator" when discarding License.

5.3.4 Operation

Perform the following operation during operation after confirmation of settings of License violation PC.

- Confirmation of License violation PC
- Processing during confirmation of License violation PC

5.3.4.1 Confirm License Violation PC

Confirm from **License** > **License Giving** in main menu for License violation PC. Confirm the following in the **License Giving** window.

- Confirmation of License violation PC
- Confirmation of License violation software

In addition, operation condition of current License can be saved as CSV format file.

Method to confirm license violation PC

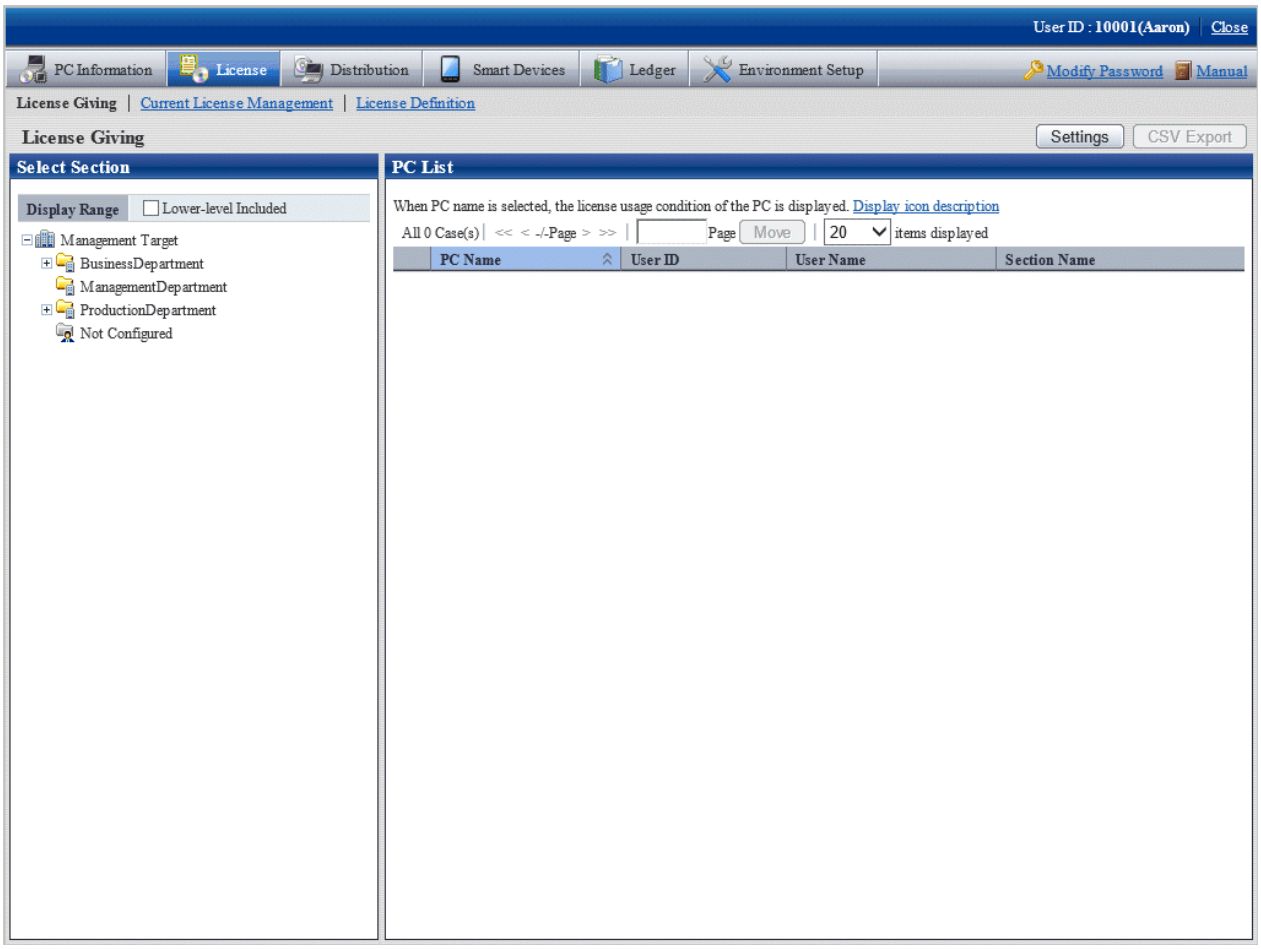
The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

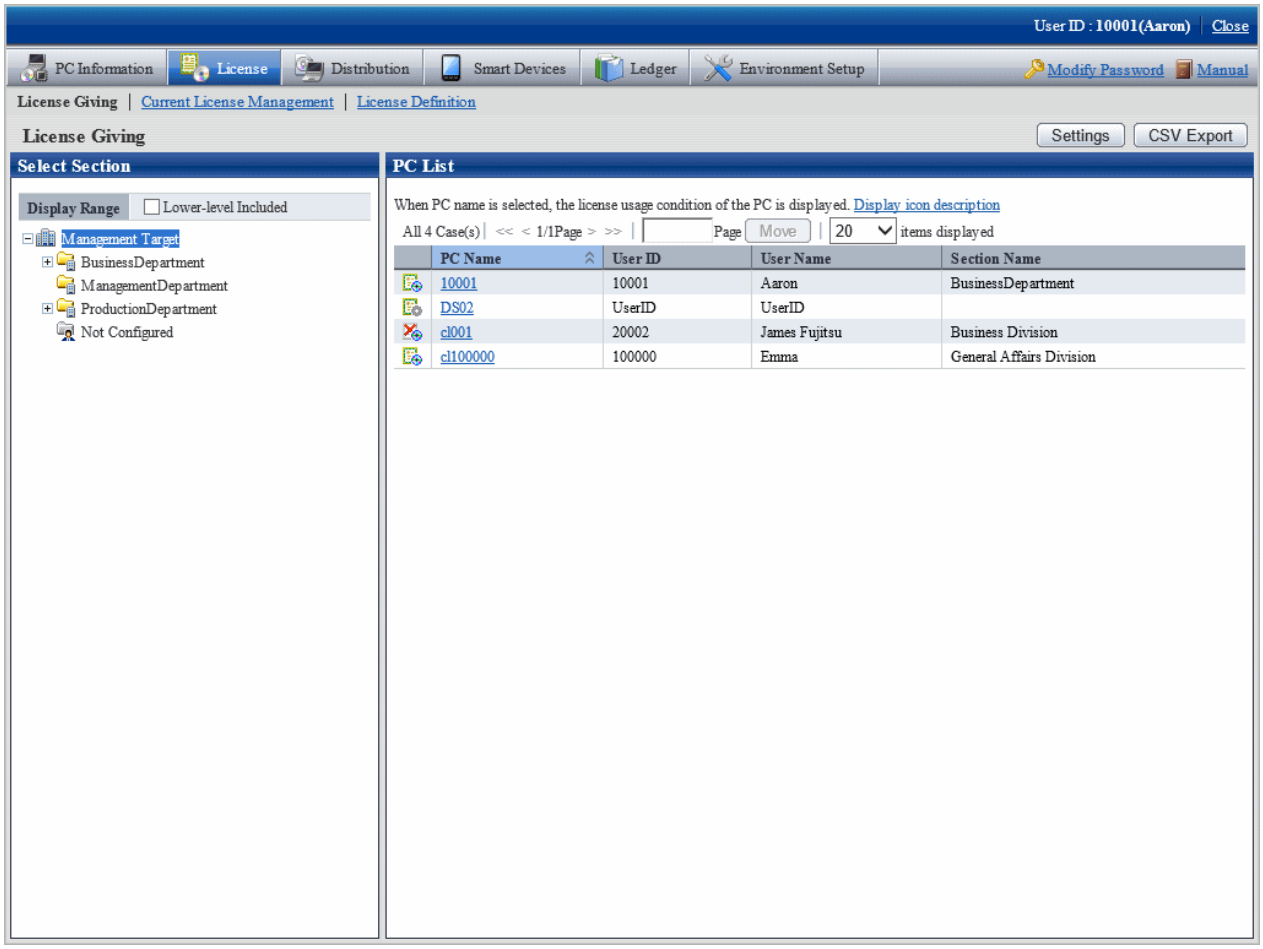
2. Click **License Giving**.

   The following window will be displayed.



3. Select section from the section tree in the field on the left.

   PC under the selected section will show in the field on the right.



4. Perform the following operations to export License Giving status of PC displayed in the field on the right as CSV format file. If not to export, proceed to the next step.

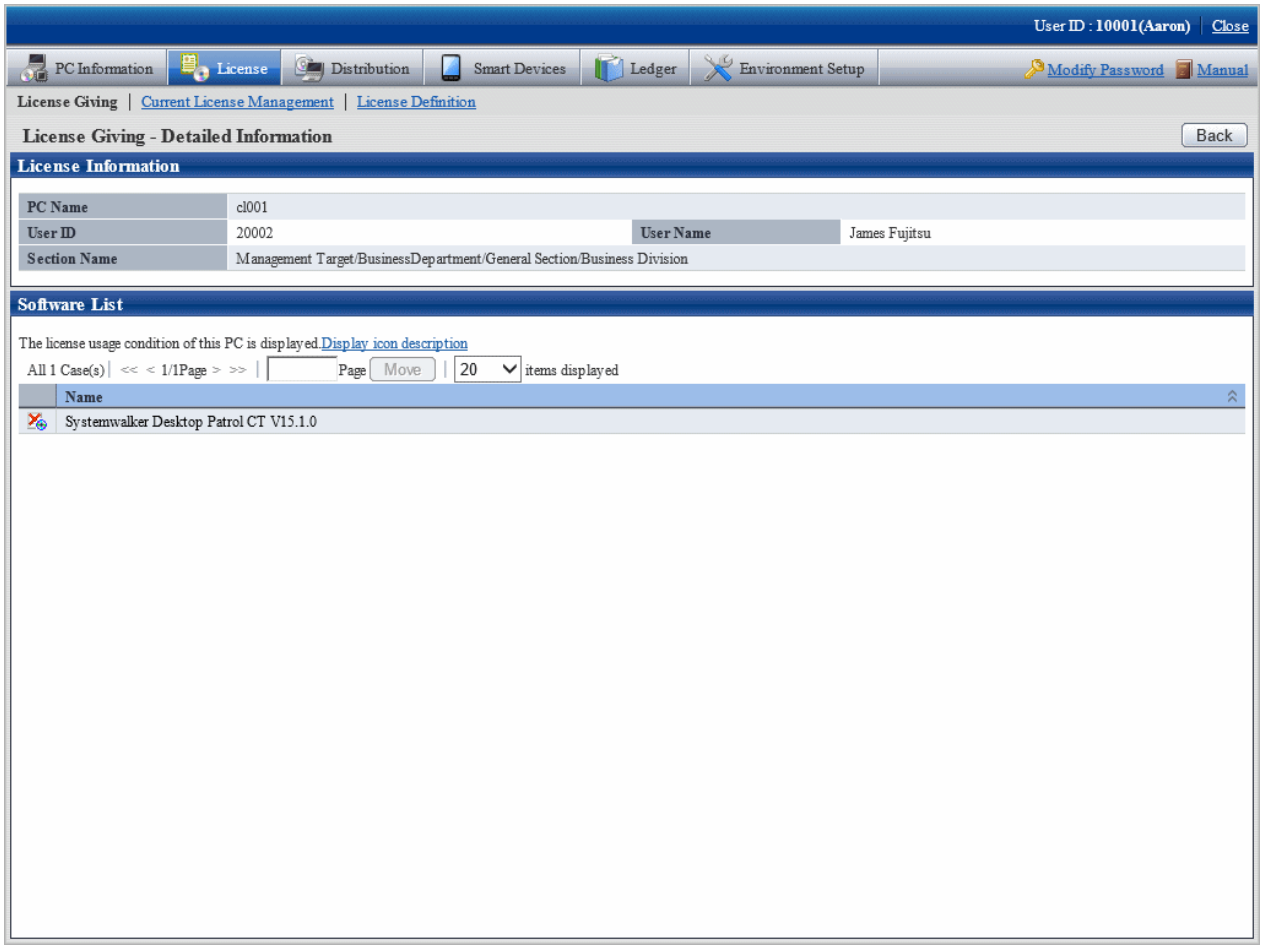
   a. Select name of PC to have CSV export, click the **CSV Export** button.

      The download window will be displayed.

   b. Export License information as CSV format file according to the window.

5. Click the PC name to confirm License Giving status by unit of PC.

   The following window will be displayed.



   Meanings of the icons are as below.

	Indicates that the software installed on the PC violated the Licensing Policy.
	Indicates that the software may become an idle asset but the license has been given.
	Indicates that the PC has permitted to install the software and to use the license.
	Indicates that the PC has no given license and the software has not been installed.

5.3.4.2 Processing at Confirmation of License Violation PC

After confirmation of License violation PC, confirm PC and violation software, decide if the "client" needs the License violation software. After confirmation, perform the following operations.

- License violation software is needed

  Allocate License when there are remaining ones. Or purchase License and then allocate to client.

- License violation software is not needed

  Instruct "Client" to unload the License violation software.

In addition, refer to "5.3.2 Allocate License " for License Giving.

5.4 Confirm Idle Assets

The software installed in CT that has been allocated with License but not in use can be confirmed.

5.4.1 Settings

Method of setting varies with method of confirming idle assets. The method to confirm idle assets is as follows.

- License Giving status
- Software Operation Status

Set separately according to the method of confirmation.

License giving status

Perform the same settings as **Confirmation of License violation PC** when confirming idle assets from **License** > **License Giving** in the main menu.

Additionally, refer to "5.3 Confirm PC of License Violation" when confirming setup of License violation PC.

Software operation status

When confirming idle asset from **PC information** > **Software Operation Status** of the main menu, perform the following setting.

1. Settings of software operation condition

   Refer to "2.2.2 Create User Definition" to confirm the software to be "User Definition", and set **Software Operation Condition** in the **Software Auditing - detailed information** window.

2. Settings of collection of software operation condition

   Confirm in the main menu if the collection of software operation condition has been set.

   > **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** tab > **Settings of Collection Items** in the **Inventory information** tab of the main menu.

3. Application of client policy

   The client policy is applied according to the schedule set in the main menu. Confirm the schedule in the main menu.

   > **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic Operation Policy** tab > **Settings of Collection Schedule** in **Inventory information** tab of the main menu.

4. Re-logon of CT

   In the above mentioned "Set Collection of Software Operation Status", after the client policy is applied to CT, it is necessary to re-logon to PC to take effect. Re-logon each PC before starting operation.

5.4.2 Use

Perform the following operations in using after the confirmation setting of idle asset is finished.

- Confirmation of idle asset
- Processing of idle assets confirmation

5.4.2.1 Confirm Idle Asset

Take the following steps to confirm idle asset.

- License Giving status
- Software operation status

License giving status

Confirm the idle assets through **License** > **License Giving** in main menu according to License Giving status.

In the **License Giving** window, the software that has been allocated a License but not installed can be confirmed for each PC.

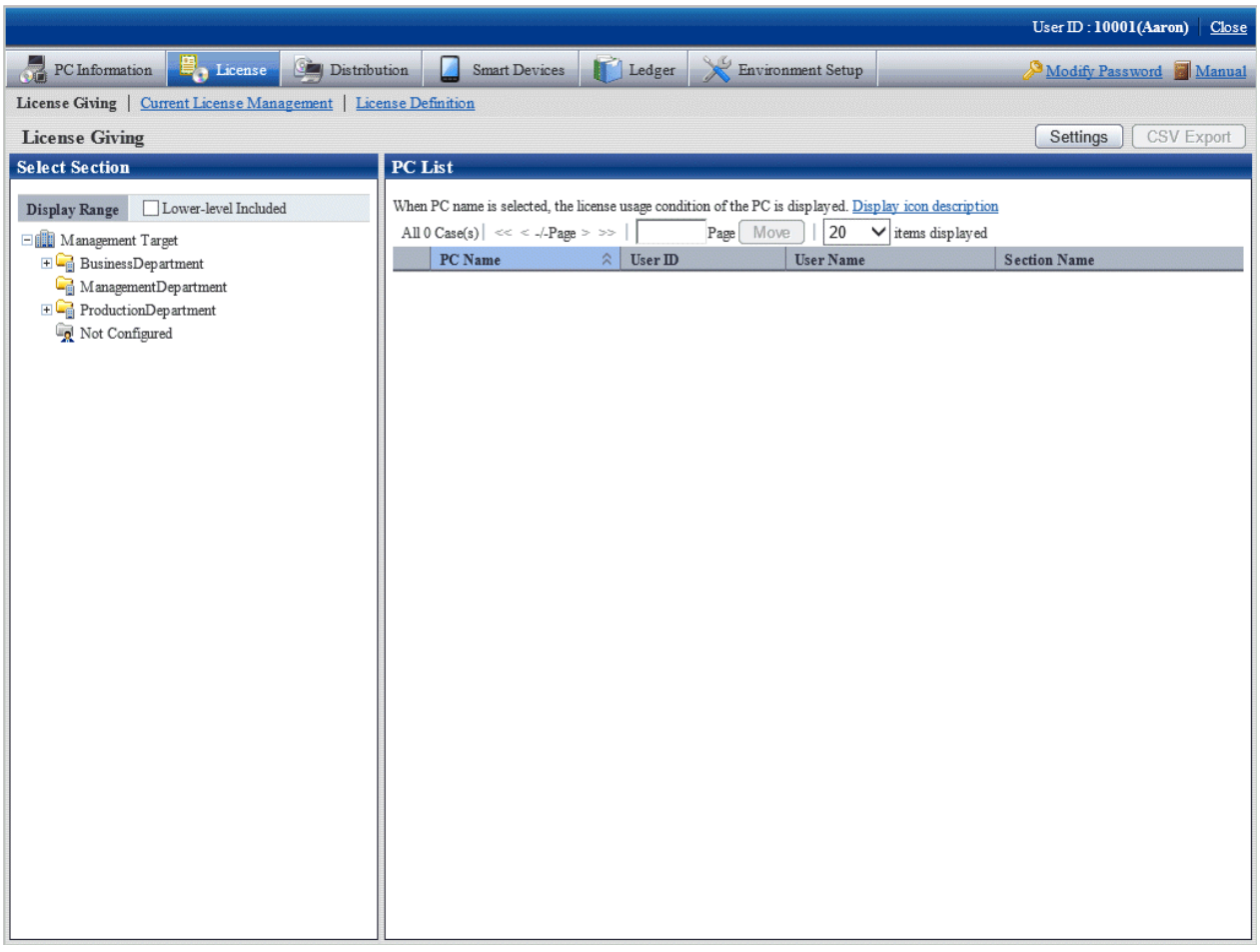
The procedure is as follows.

1. Log in to the main menu, click **License**.

   The **License** window will be displayed.

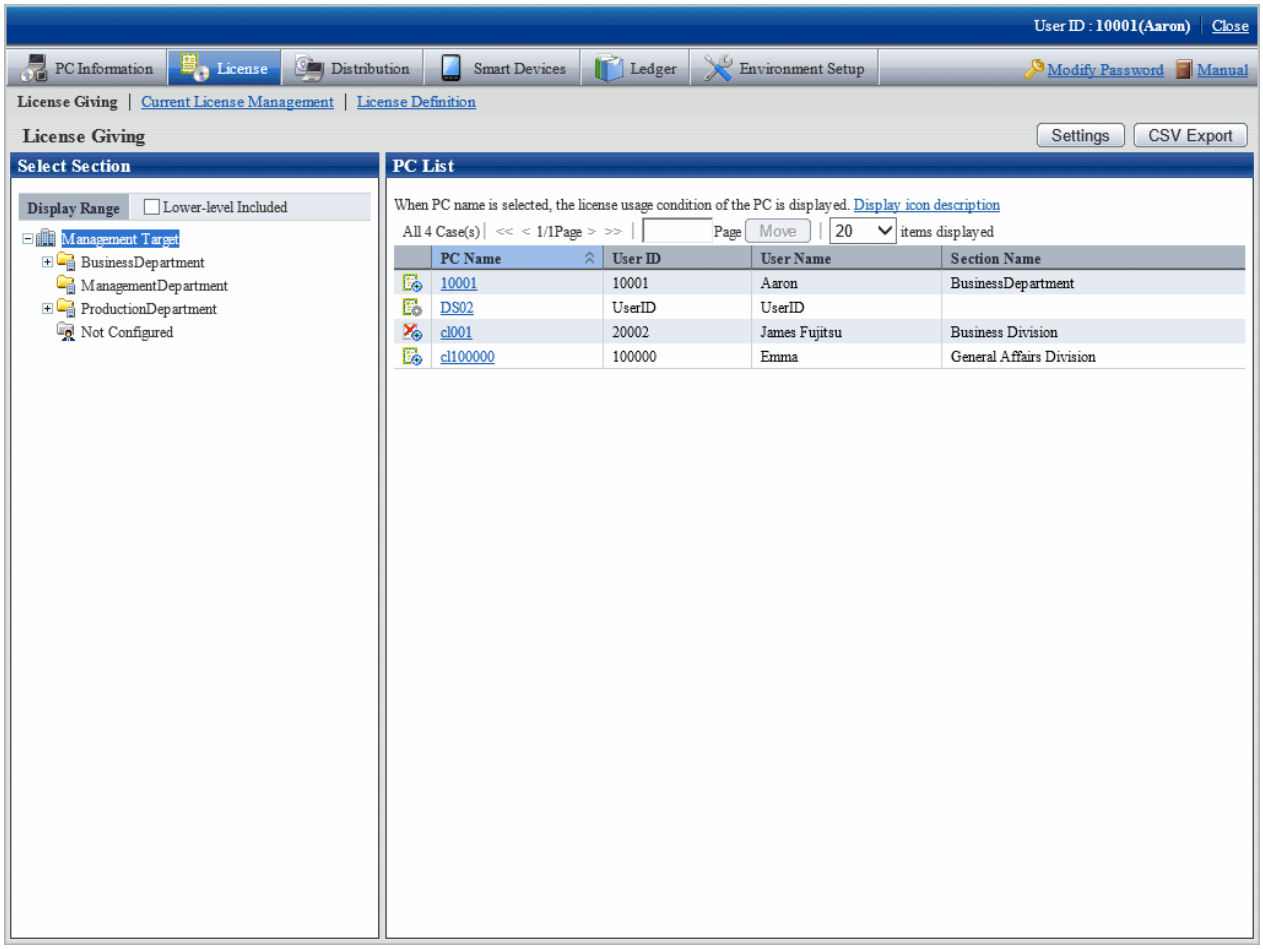
2. Click **License Giving**.

   The following window will be displayed.



3. Select a section from the section tree in the field on the left.

   PCs of the selected section will be displayed in the field on the right.



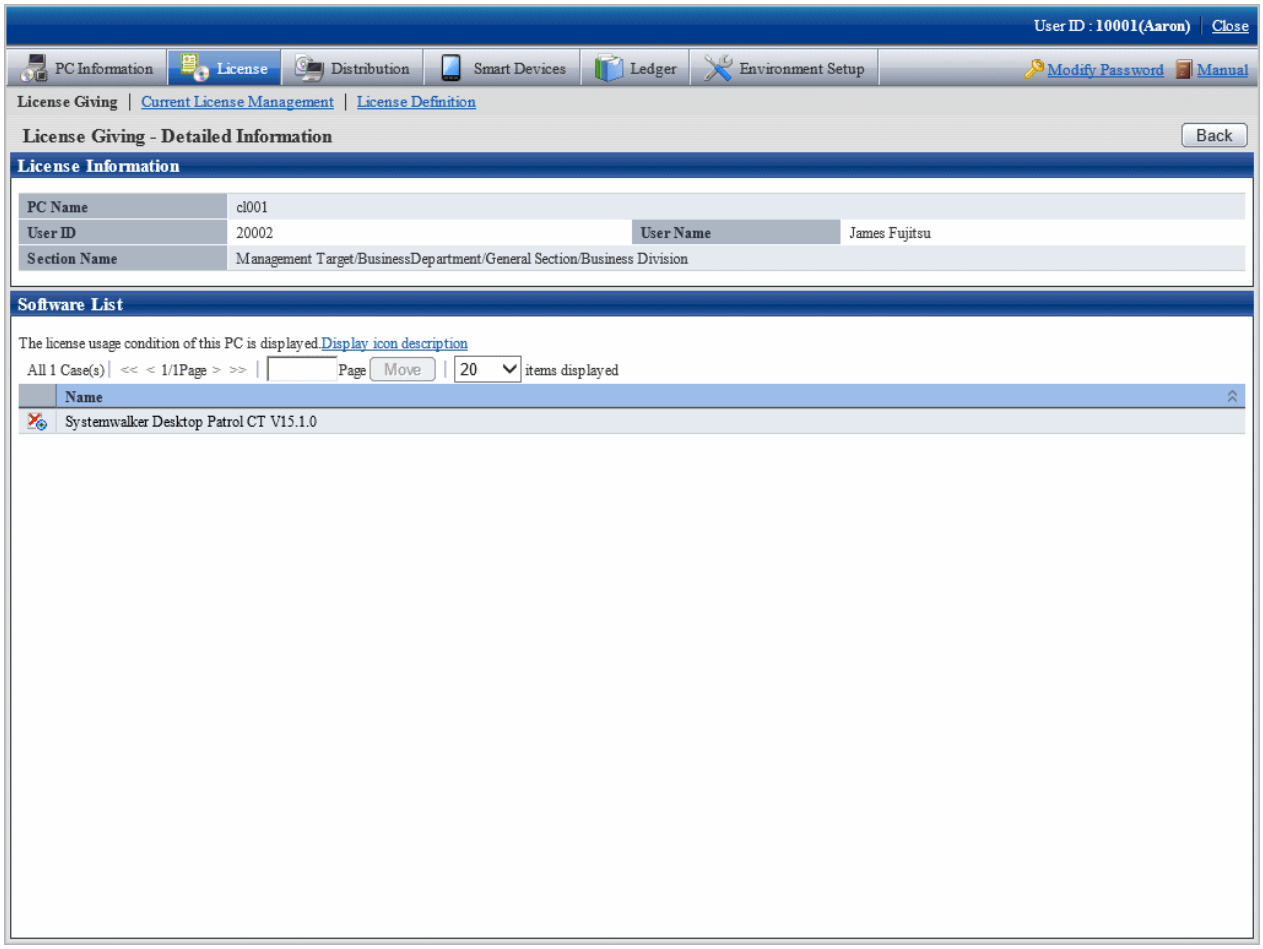
4. Perform the following operations to export License Giving status of PC displayed in the field on the right as a file in CSV format. If not to export, proceed to the next step.

   a. Select the name of the PC to export in CSV format, and click the **CSV Export** button.

      The download window will be displayed.

5. Click the name of the PC to confirm License Giving status by unit of PC.

   The following window will be displayed.



   Emphasize on viewing the icon of **Software List** in above window.

   The software with License has been allocated but not installed to PC will become idle asset.

Software operation status

Operate from **PC Information** > **Software Operation Status** in the main menu to confirm idle asset through software operation status.

In the **Software Operation Status** window, confirm the PC that does not use the software by referring to the software operation status collected as Inventory information. In addition, operation status of the current software can be saved as file in CSV format.

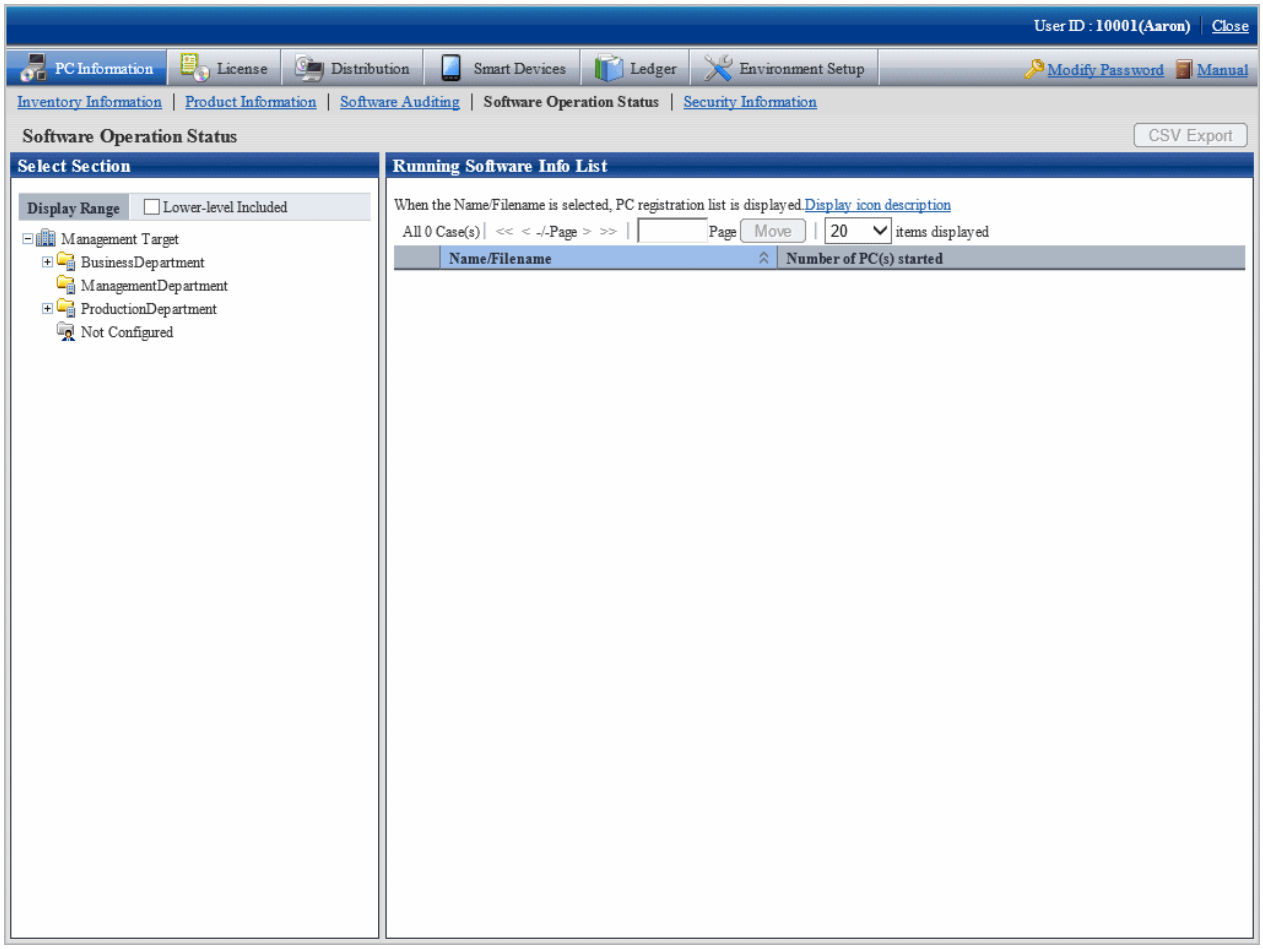
The procedure is as follows.

1. Log in to the main menu, click **PC information**.

   The **PC Information** window will be displayed.

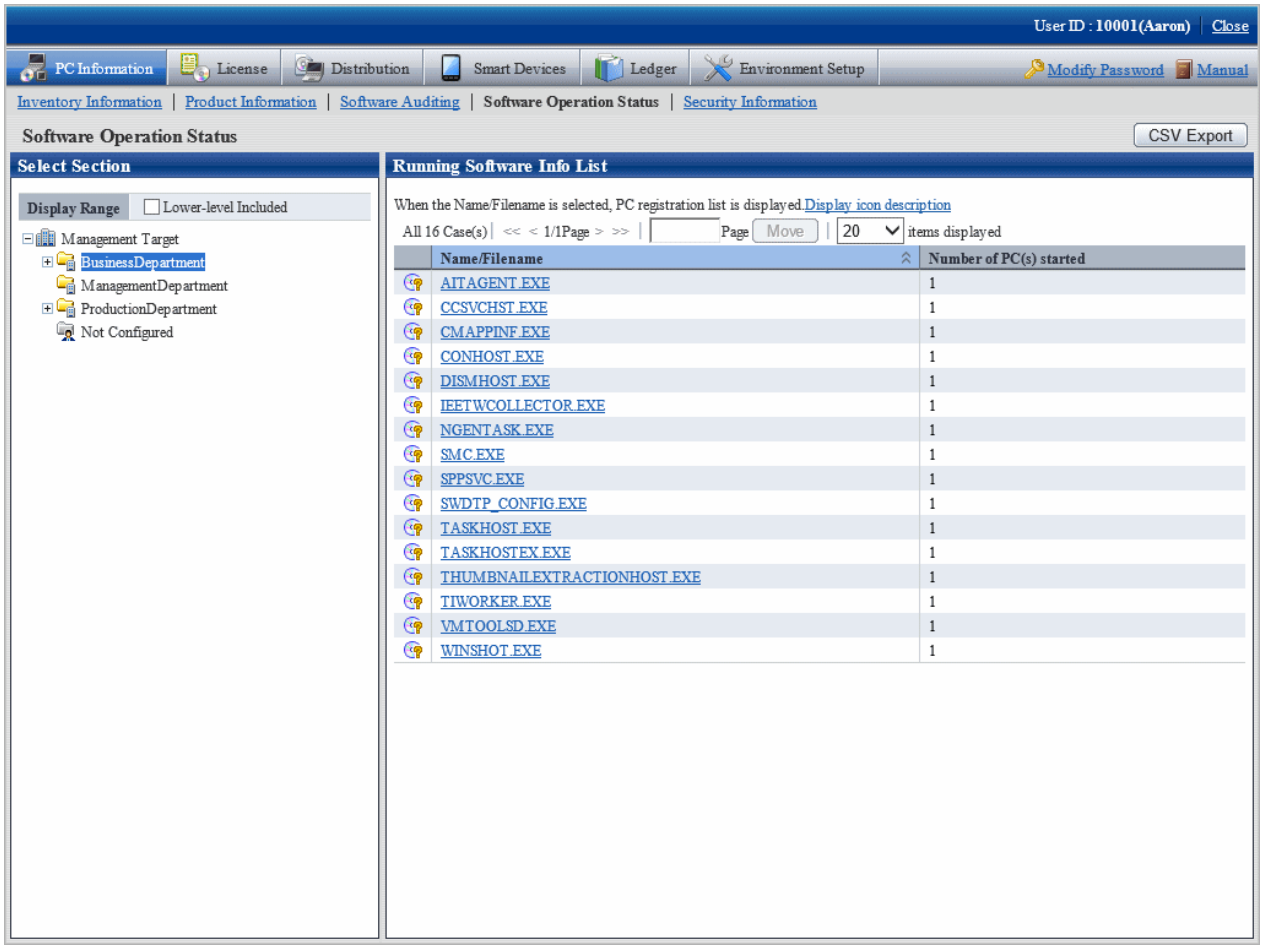
2. Click **Software Operation Status**.

   The following window will be displayed.



3. Select section from the section tree in the field on the left.

   The Software Information used by the selected section will be displayed in the field on the right.



Item	Description
Number of PC(s) started	Number of PCs in which the software has been started

4. Perform the following operations when the PC software operation status shown in the field on the right is exported as a file in CSV format. If not to export, proceed to the next step.

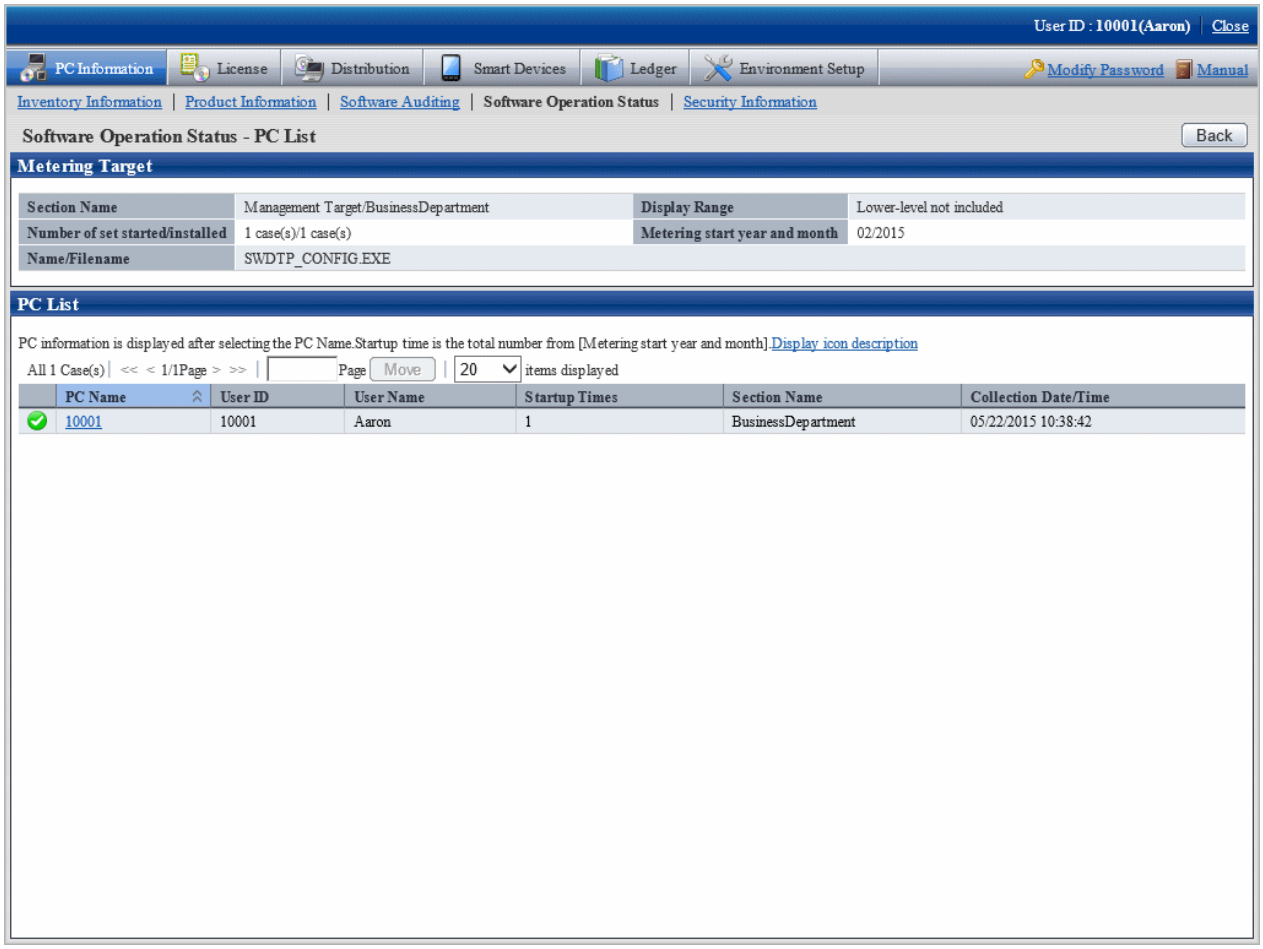
   a. Click the **CSV Export** button.

      The download window will be displayed.

   b. Export software operation status as file in CSV format according to the window.

5. Click the software name in the field on the right when confirming the details including the user of software.

   The following window will be displayed.



   Pay attention to PC shown with the icon of in the above window. The software selected in step "4." on the PC displayed as icon of is idle assets.

6. After confirmation of idle asset has completed, close all the Web browsers and exit processing.

5.4.2.2 Processing at Confirmation of Idle Assets

Processing at confirmation of idle assets varies according to the above mention confirmation method of idle assets. Take the corresponding processing according to situations.

License giving status

When confirming idle assets by confirming License Giving status, identify PC and software and perform the decommissioning operation of License Giving. Therefore, it's able to allocate License to other PC.

As to decommissioning of License Giving, refer to "5.3.2 Allocate License ".

Software operation status

When confirming idle assets through the software operation status, confirm the PC and software and confirm whether this software as idle asset is required in "Client". After confirmation, perform the following processing.

- When it is necessary to put asset software in idle

- Take no action.
- When it is not necessary to put asset software in idle

  Instruct the "Client" to uninstall this software which is idle assets and remove License Giving.

Based on the above processing, the license can be allocated to other PC. In addition, refer to "5.3.2 Allocate License" for removal of License Giving.

Chapter 6 Distribute/Install Security Patches

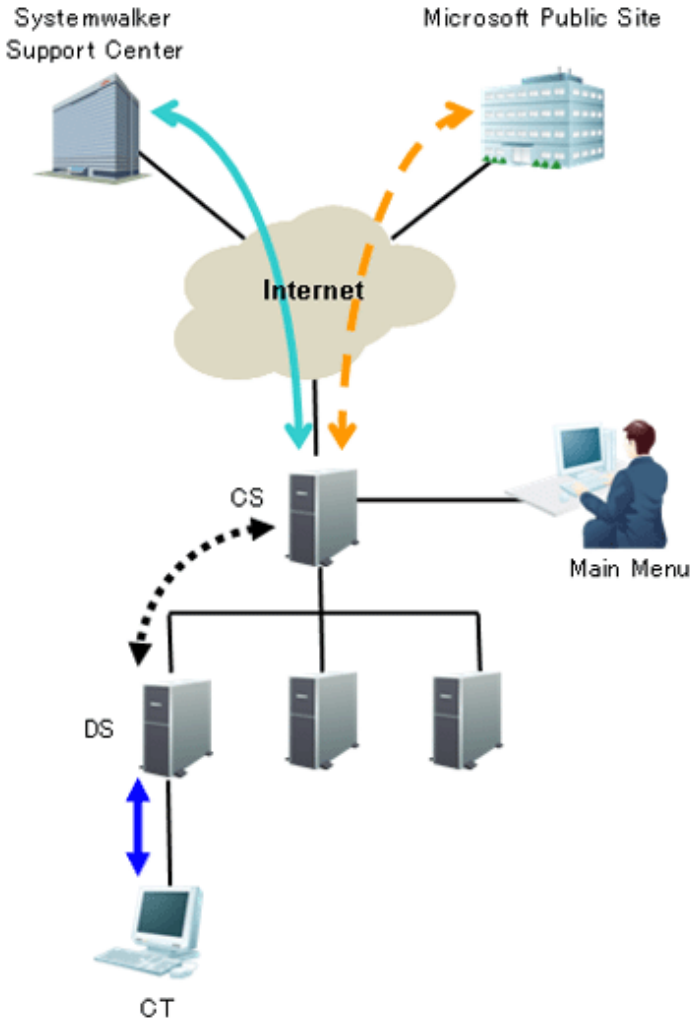
This chapter describes how to obtain security patches from Microsoft company and install them to CT.

6.1 Operation Steps

The security patches distributed by Microsoft can be obtained automatically to CS and installed automatically to CT.

As to the security patches to be installed, detect the ones not installed based on the Inventory information collected from CT, only the necessary security patches will be distributed and installed to PC. After installation, identify the installed security patches and PC from the main menu through the Inventory information, the administrator's workload can be reduced in this way.

Flow of data in automatic installation of security patches in the 3-level model is shown as follows.



See the table below for information required for installation of the security patches and the time point (original value) when the information is sent.

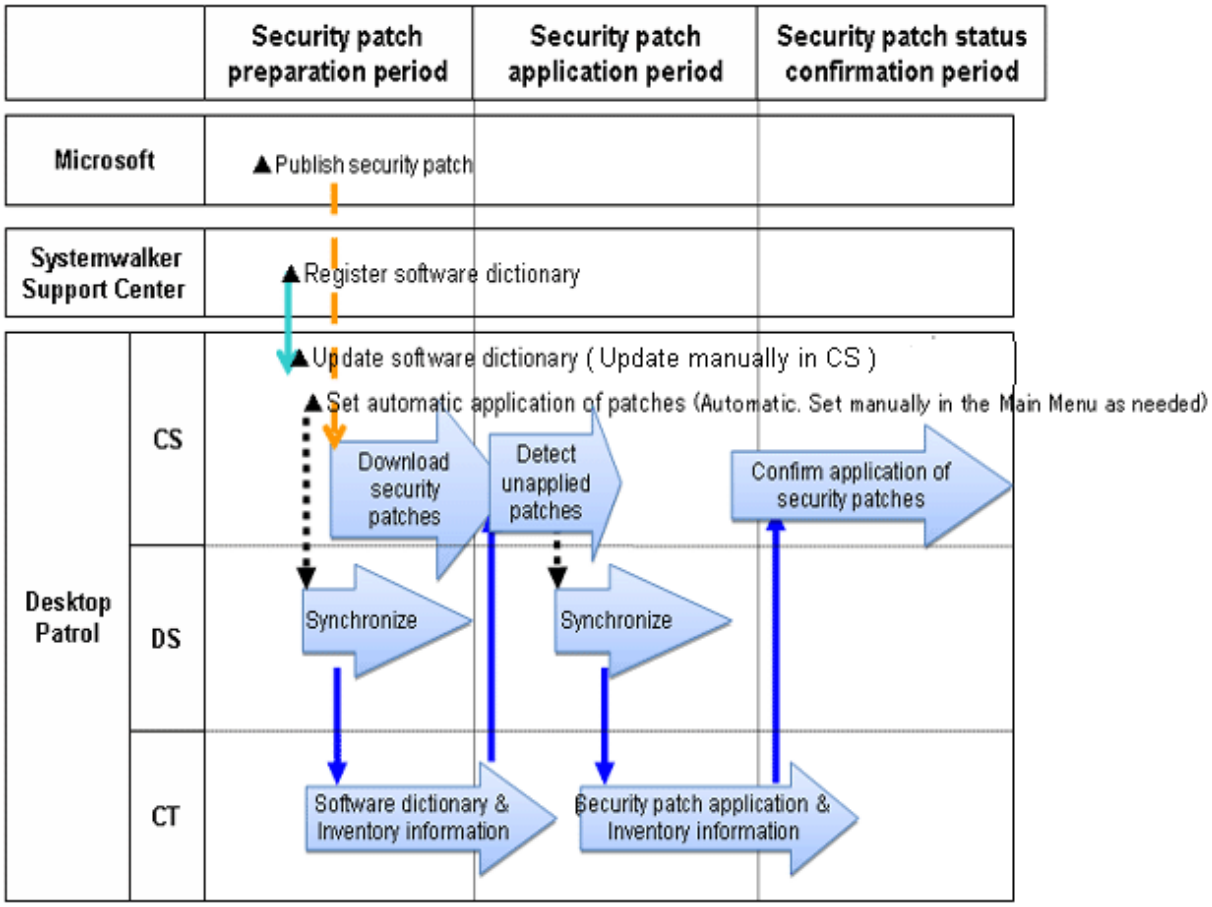
Type of line	Operation	Operation time
⟷	Update Software Dictionary	Install by E-Mail (Note 1)
← →	Download security patches	Start to download at 3:00 each day(Note 2)

Type of line	Operation	Operation time
		Setup in **Environment Setup** > **Option** in the main menu
◀····▶	Synchronize Software Dictionary Synchronize security patches	Confirm in every 30 minutes Setup by selecting DS name in "**Environment Setup** > **CS/DS Settings and Status** in the main menu
◀——▶	Download Software Dictionary Upload of Inventory information Installation of security patches	Confirm in every 3 hours Setup in **Environment Setup** > **Policy Groups** in the main menu

Note 1) The contract of SupportDesk and the registration operation of Systemwalker Support Center are required in advance.

Note 2) Set to be disabled during installation. Therefore, it is necessary to enable setup.

See below for sequence chart up to installation of security patches to CT.



Operation	Operation time
Patches not installed	Confirm in every 1 hour
Confirmation of installation of security patches	Anytime Status confirmation from the main menu.

The sequence chart will be described in 3 stages.

Preparation stage of security patches

Automation of preparation of the security patches published by Microsoft can be achieved through the following settings on CS in advance. This kind of setup shall begin after CS is installed but it is not necessary to set for each time.

- Update of Software Dictionary

  Regular update of software dictionary to keep it up to date.

  Refer to relevant contents of "6.2.2 Update of Software Dictionary" for update method of software dictionary.

- Setting of automatic installation of patches

  Automatically download the security patches defined in the software dictionary from Microsoft company.

  Refer to relevant contents of "6.2.4 Select Security Patches" and "6.2.5 Acquisition of Security Patches" for setup method.

Installation stage of security patches

No need for special setup. The operations will be performed according to the setting of the product installation.

Refer to relevant contents of "6.2.6 Settings of Installation & Distribution Intervals of Security Patches" for setting modification.

Status confirmation stage of security patches

No need for special setup. The operations will be as per Settings of the product installation.

Refer to relevant contents of "6.4.3 Confirmation of Installation of Security Patches" for confirmation method.

6.2 Setup

It explains herein about use Settings of automatic acquisition/automatic installation of modification of security patches.

6.2.1 Confirm and Publish Server Connection

Under the circumstance that CS is connected to Microsoft company's public server through proxy, it is necessary to click the CS name in **Environment Setup** > **CS/DS Settings and Status** in the main menu for proxy settings. Refer to relevant contents in *Systemwalker Desktop Patrol Installation Guide* for setup method.

In addition, it is no need for proxy settings under the circumstance without connection with Microsoft's public server through proxy.

Processing when download of security patches failed

It will not be possible to download security patches from Microsoft's public server under the following circumstances. Take the following measures as instructed.

- Can visit Microsoft company's public server through proxy, but without proxy settings of server attribution.

  "Process"

  Carry out proxy settings in server attribution.

- Insufficient disk space of the specified software saving directory in installation.

  "Process"

  - Extended directory not specified during installation, specify a disk of sufficient available capacity as the extended directory.
  - Extended directory specified during installation, delete the unwanted files in the directory to increase the available capacity.

- In Microsoft company's public server, the URL information of security patches download has been changed, or the security patches themselves are not provided anymore.

  "Process"

  Update to the latest software dictionary.

- Necessity of manual download of security patches from Microsoft company's public server.
  "Process"

  Refer to "6.2.5.2 Obtain Security Patches Manually" to register the security patches to be downloaded manually.

6.2.2 Update of Software Dictionary

It is necessary to update the software dictionary to acquire and install the latest security patches.

The method to update the software dictionary is update manually according to the mail receive from Systemwalker Support Center.

Refer to relevant contents in *Systemwalker Desktop Patrol Installation Guide* for update of software dictionary.

6.2.3 Select security Patches to be Installed to Special PC

This section explains how to select and apply security patches to a specific PC.

Usually, the security patches you select at "6.2.4 Select Security Patches" are distributed and applied. Therefore, you do not need to select a patch application policy for a policy group whose **Group Type** is **CS** or **DS** in **Policy Group List** of **Policy Groups**.

However, you need to select security patches for PCs whose operation is affected when specific security patches are applied.

You can select a patch application policy for a policy group whose **Group Type** is **Policy Group** in **Policy Group List** of **Policy Groups**.

Exceptional operation of patches installation can be performed for the PC having had problems in operation after installation of the specific security patches. This kind of exceptional operation works for both the security patches of automatic installation and manual installation (install patches from software download window by clicking **Start** or **Apps** > **Patch Application**).

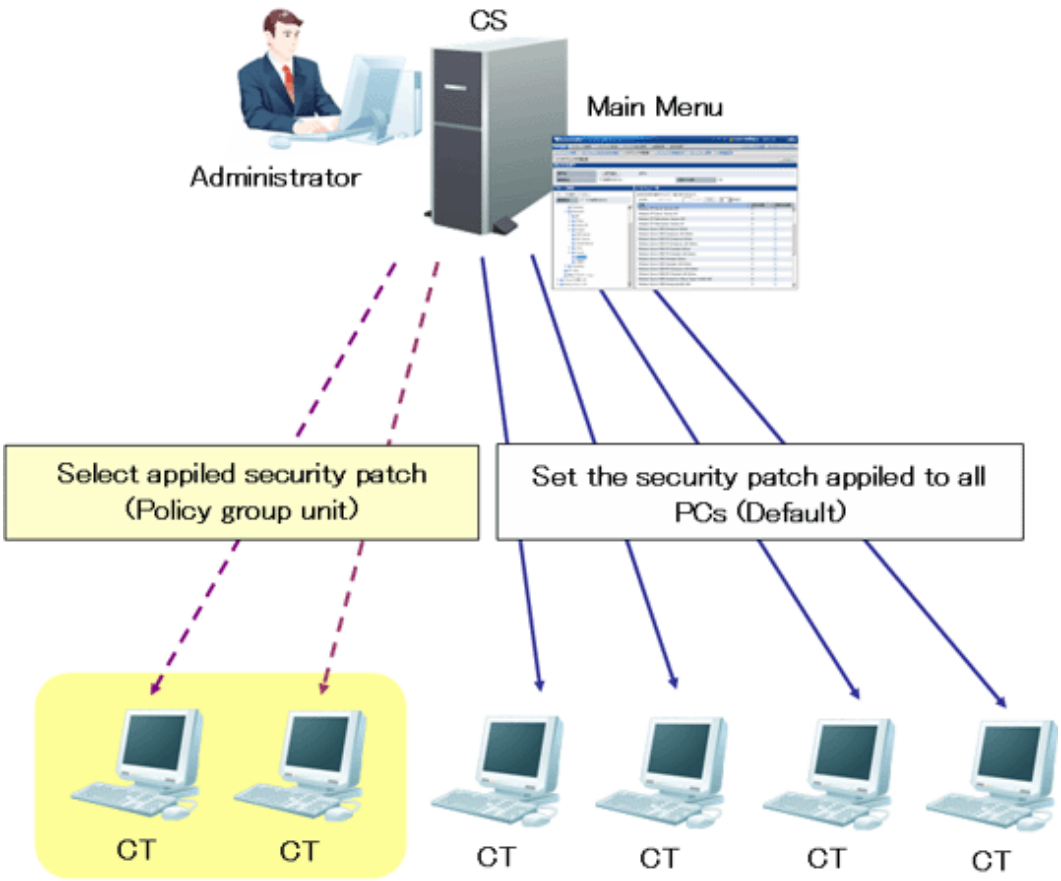
Complete the following setup to select the security patches to be installed.

- For the specific PC, select Settings of the security patches to be installed
- For the specific PC, Settings of security patches provided in future not to be installed

The above setups can also be installed in combination.

Operation graph

See below for operation graph of the security patches selected and installed to the specific PC.



CT that does not belong to policy group can adopt the patches according to the setup contents of the security patches selected in window of **Security Patches Distribution** in **Distribution** in the main menu.

As to the security patches to be selected and installed to specific PC, select the security patches not to be used in of the **Patch installation Policy** tab in **Customize Various Policies** in **Policy Groups** in **Environment Setup** in the main menu.

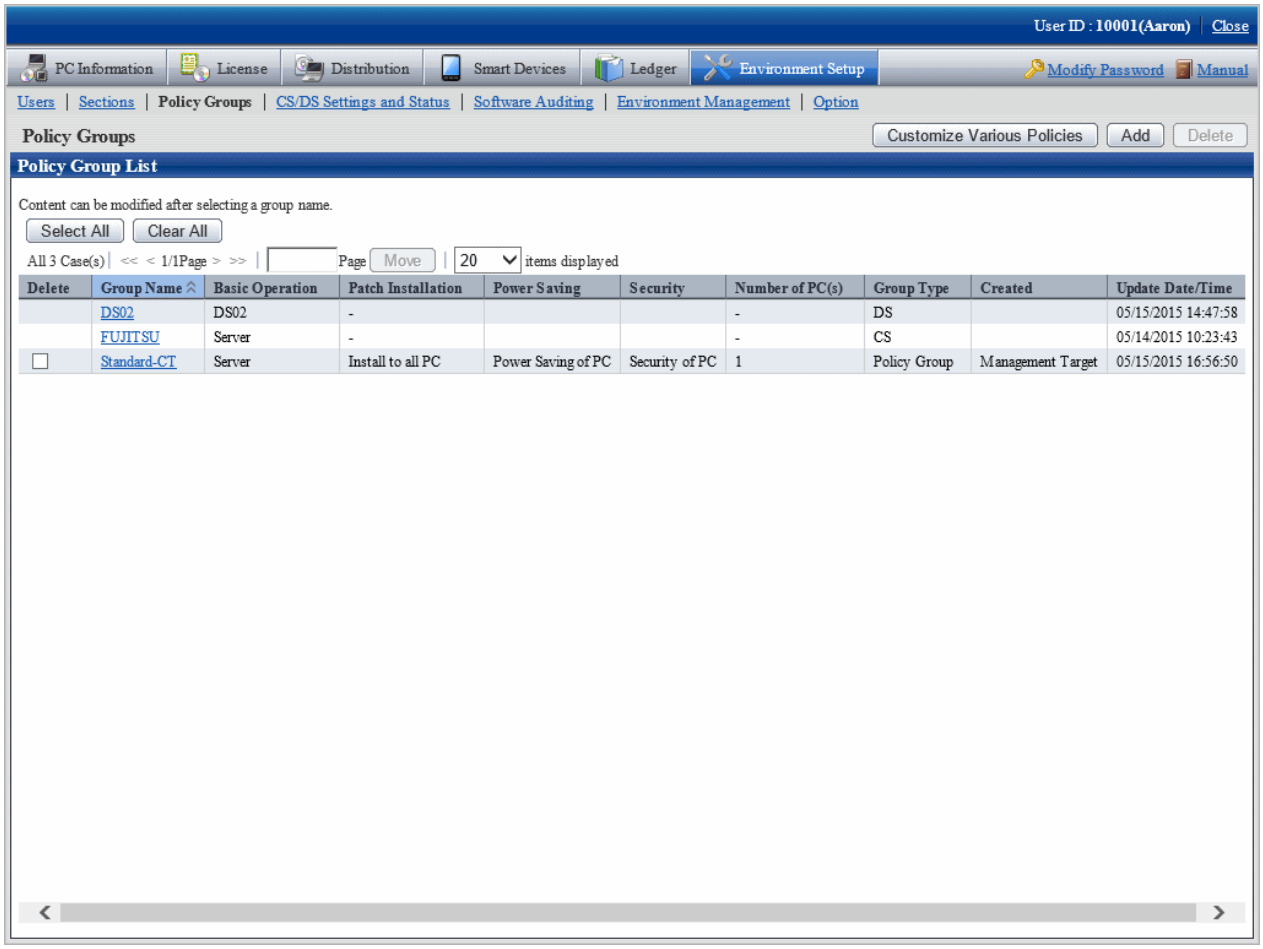
Now you can select and install the security patches to PC belonging to the policy group.

Setup steps

Take the following steps.

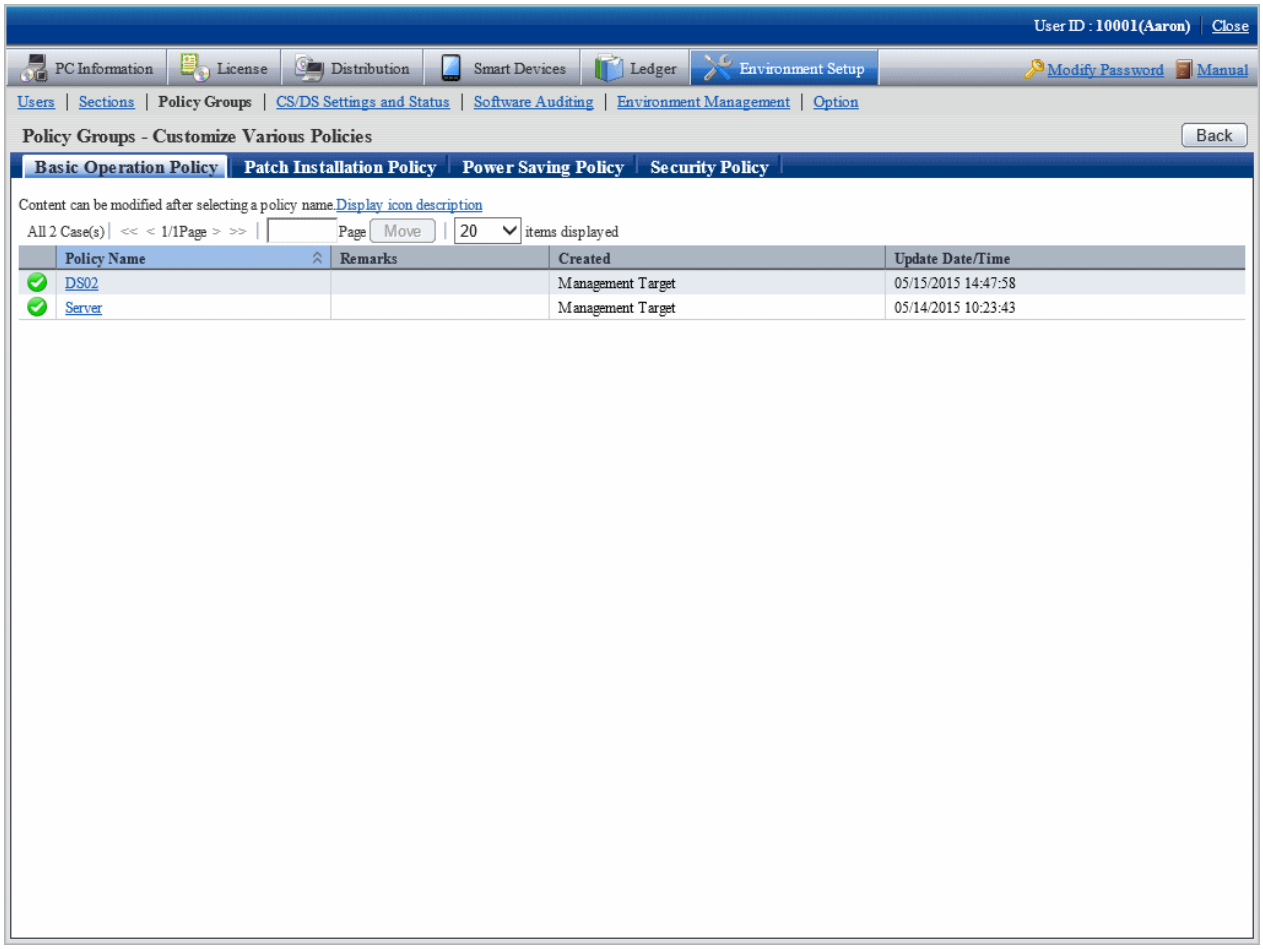
1. Click **Policy Groups** in **Environment Setup**.

   The following window will be displayed.



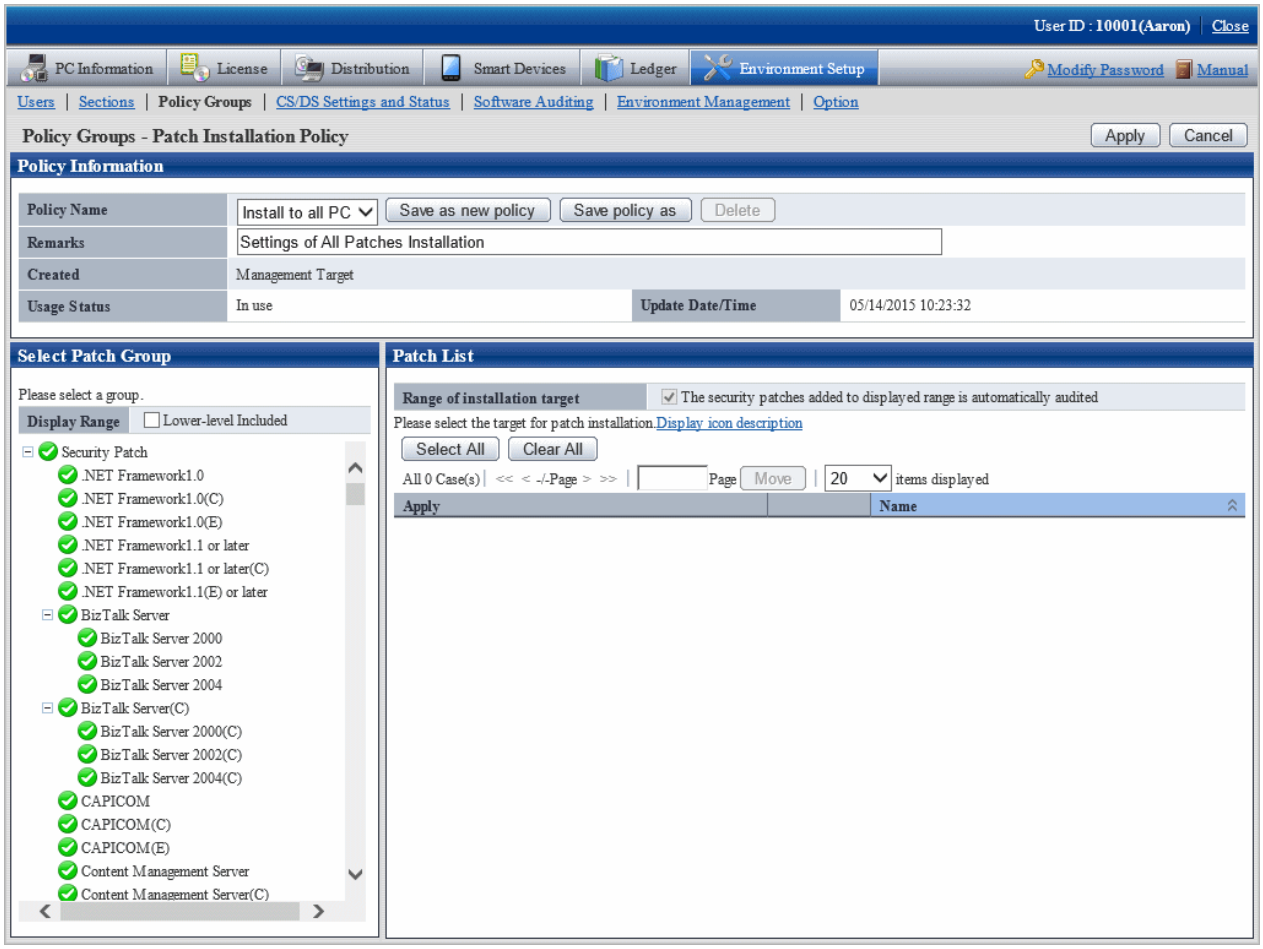
2. Click the **Customize Various Policies** button.

   The following window will be displayed.



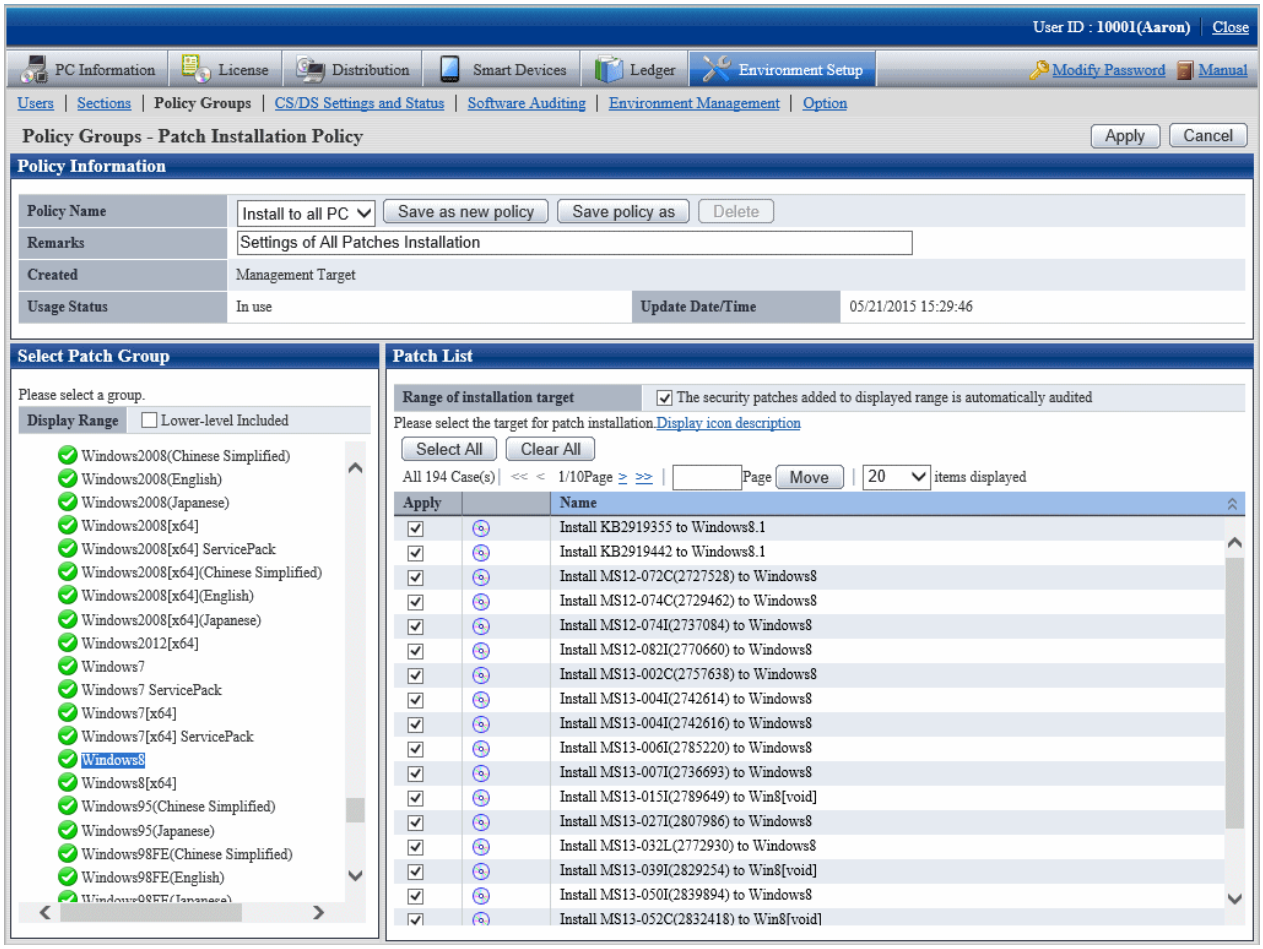
3. Click the **Patch Installation Policy** tab.

   Click the link of the policy name, the following window will be displayed.



4. Select the patch group to have the security patches setup modified and installed from the tree on the left field.

   The security patches under the selected patches group will be displayed in the field on the right.



5. Delete the Select Security Patches not to be installed from the security patches in the field on the right. Finish the following setup as well.

   - **The security patches added to displayed range is automatically audited**

     Delete the selected check box if the security patches under the selected patch group added in future will not be regarded as objects.

     After deleting selection of check box, none of the security patches will be regarded as installation object for the ones whose definition is added to the software dictionary in future, or the security patches are selected under its own patches group from window of **Distribution** > **Security Patches Distribution**.

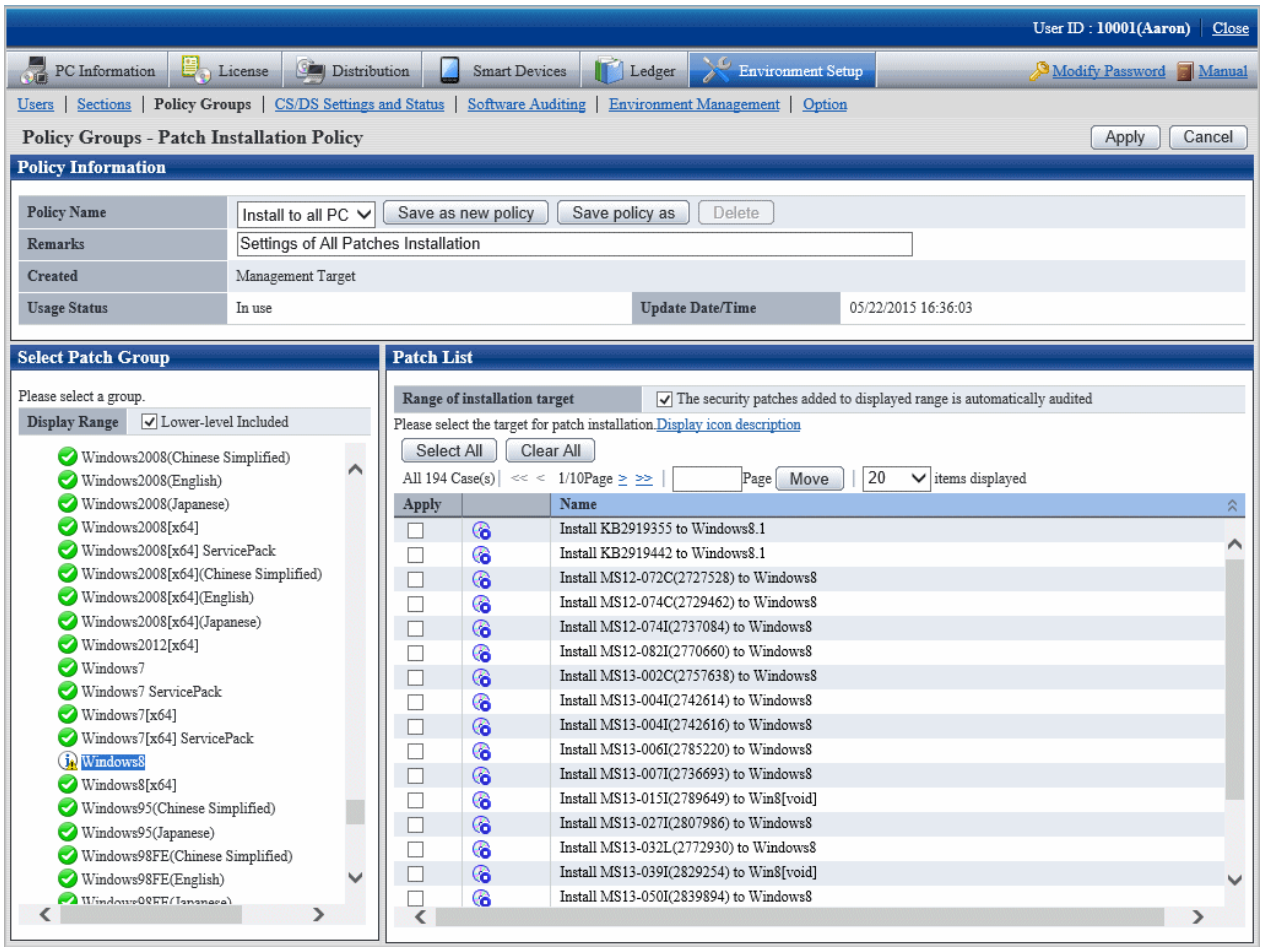
6. Click **Apply** button to save the setup.

7. Repeat step "3." to "7." for modification of Settings of multiple patches groups.

8. To confirm contents of setup modification, repeat step "3.", select the patches group and confirm.

   Icon of patches group having had the installation security patches setup modified will change as below.

Icon	Description
	All the security patches are installation objects.
	Security patches of non-installation objects exist.



The patches groups shown in the tree are the whole patches groups. Delete the selected patches group in window of **Distribution** > **Security Patches Distribution**, the installation will be disabled even it is selected in Patch installation policy.

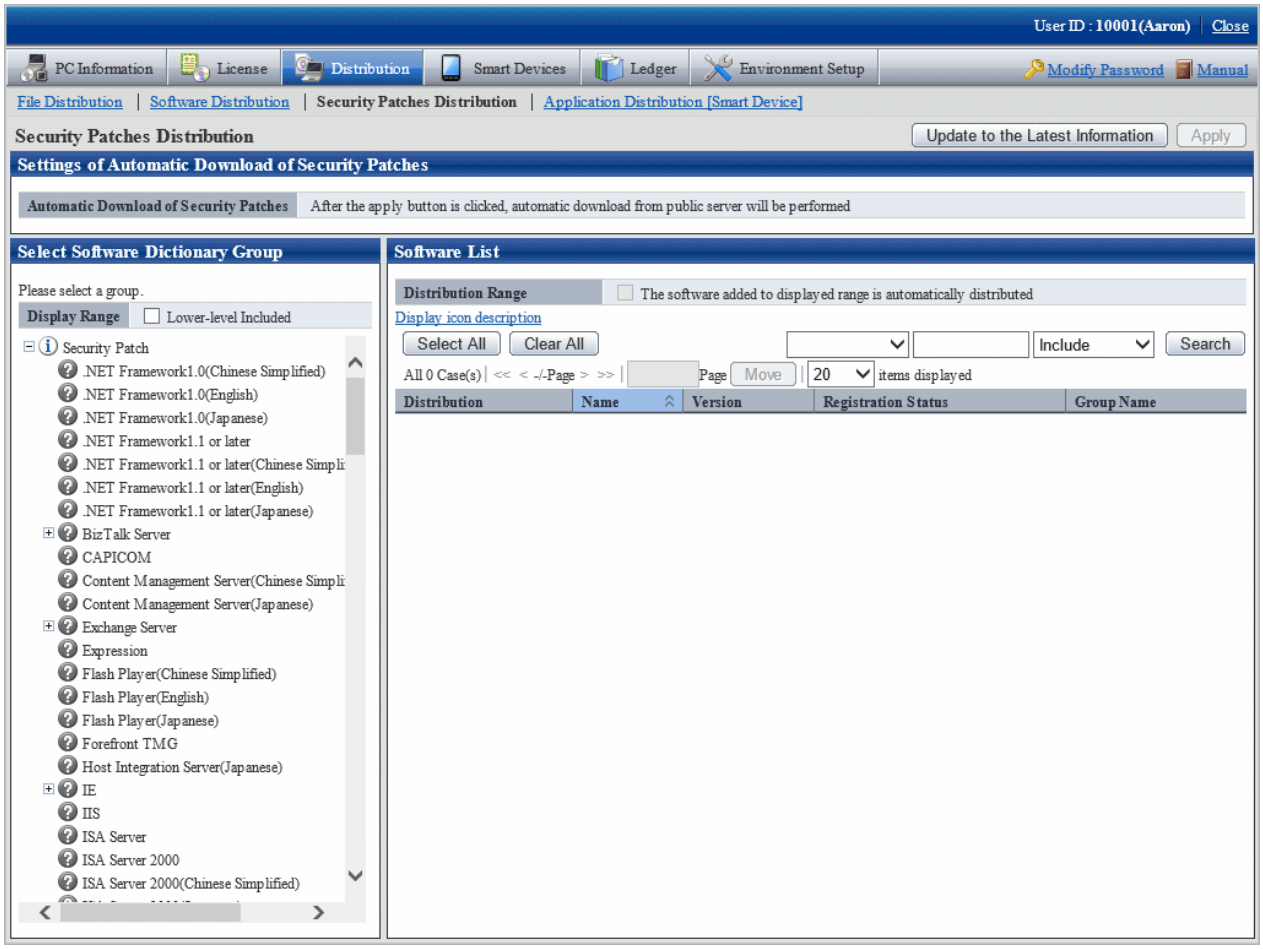
6.2.4 Select Security Patches

Select the security patches from the software dictionary that are acquired from Microsoft company to CS. Only the selected security patches will become the objects of automatic or manual acquisition.

Take the following steps.

1. Log on to the main menu, click **Distribution**, then click **Security Patches Distribution**.

   The following window will be displayed.

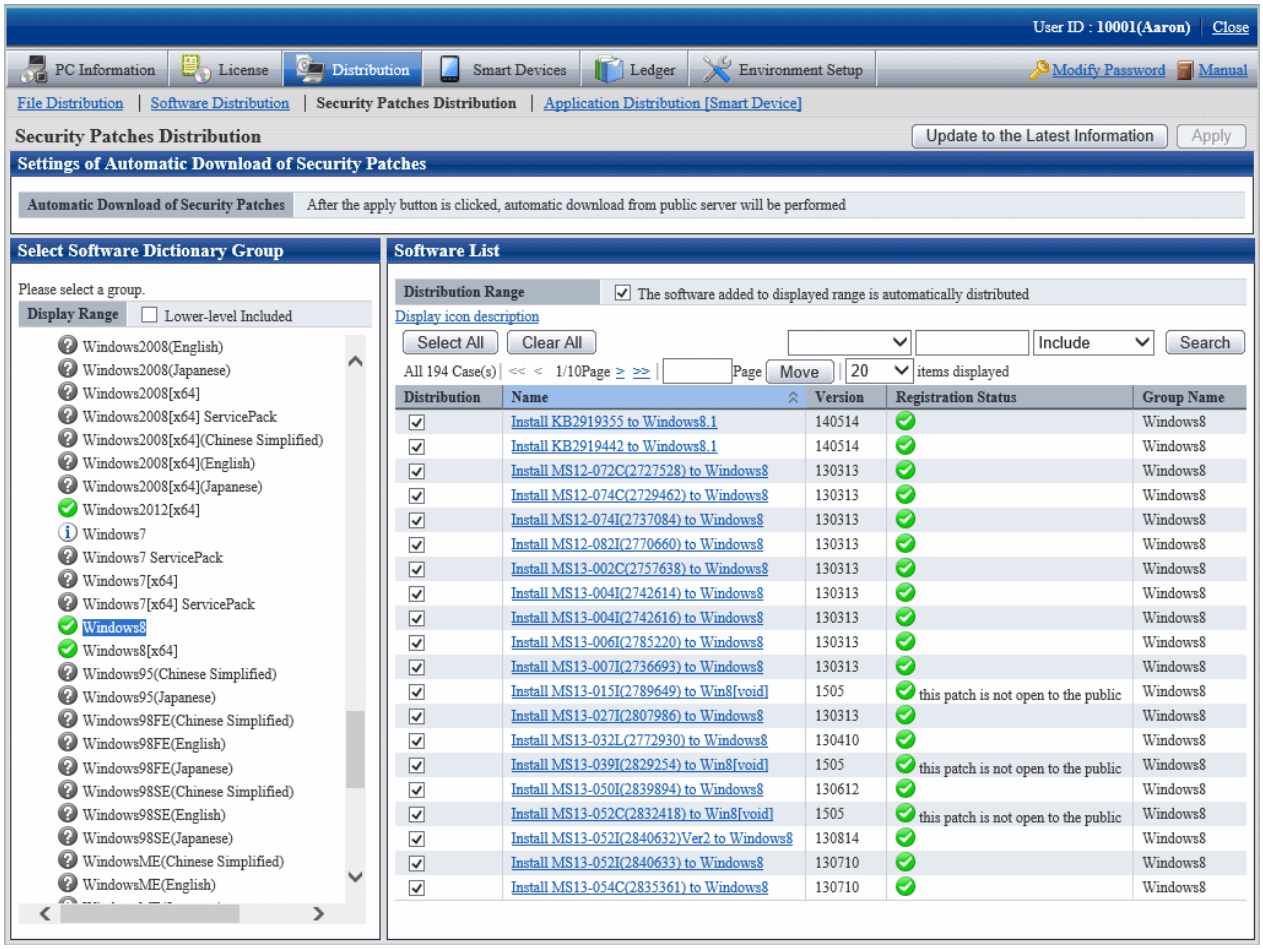


The following information will be displayed in the area of S**ettings of Automatic Download of Security Patches**.

Item	Description
Automatic Download of Security Patches	As to when the setup downloads the security patches from the public server will be shown as the following(Set value in **Settings of Security Patches** in **Option** in **Environment Setup**): - Click the **Apply** button for automatic download from the public server. - Click the **Apply** button, then download from the public server automatically by plan.

2. Select the directory under the security patches from the left field of the window.

   List of the selected security patches will show in the field on the right..

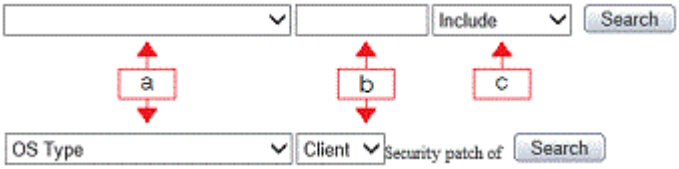


Meanings of the icons of the selected area in the software dictionary group are as below.

Icon	Description
	All software is distribution object.
	Part of the software is not distribution object.
	None of the software is distribution object.

See below for Description about the fields in **Software List**.

Item	Description
The software added to displayed range is automatically distributed	Check box only shown when the security patches are shown. After this item is selected, even the security patches are automatically added to the group selected in **Select Software Dictionary Group** can also be distribution objects.
Distribution	Select the security patches to be distribution objects. - When selecting Select **Download from public server** from **Settings of distributed software - Detailed Settings** in the main menu, click this button, download will proceed automatically or by plan from the public server (Web site of Microsoft company). - When not selecting

Item	Description
	Delete the security patches downloaded from the public server. **Note** Pay attention to the following when setting up the security patches automatically downloaded from the public server by plan. - After the registered security patches have been deleted from the main menu, the deleted security patches won't be objects for automatic acquisition.
Search button	Display contents of screening software list.  Select the objects to be screened from "a". The selection objects are the item names, **OS name** and **OS type** respectively. In addition, only specified security patches for OS type. Conditions of the specified screening objects in "a" will be specified in "b" and "c". - When selecting each item name or **OS name** in "a" - The screening character string will be specified in "b". The character string can be specified as partially consistent. In addition, when "a" is **OS name**, specify a character string in "b" excluding **Windows** and Edition. (can't specify **Windows** and screen Edition) - Select **Included** or **Excluding** in "c". - When selecting **OS type** in "a" Select **Client end** or **Server** in "b".

" Table 6.1 Message of registration status of security patches" will be displayed when errors occur in registration status of the security patches.

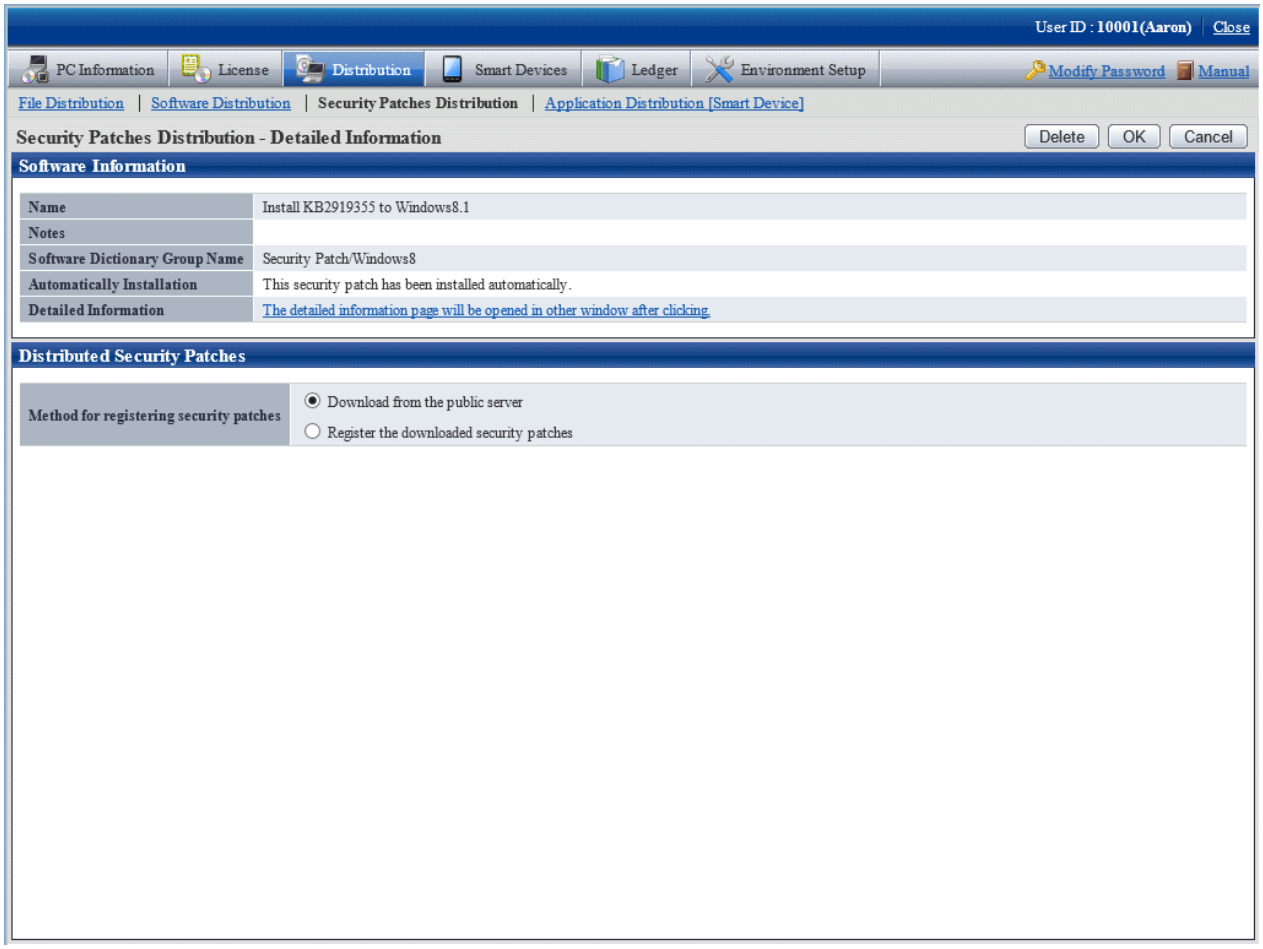
Table 6.1 Message of registration status of security patches

Messages	Description	Process
failed to delete patch file	Failed to delete patches	Delete the error patches, then download the security patches from the public server or register the downloaded patches. If the same message stays, collect the log and contact the technicians.
failed to download	Failed to download patches	Confirm the following contents. - Are there any problems in CS proxy settings(**Use proxy** in window of **CS/DS Settings and Status**) - Are there any problems in IP address settings - Is system virtual memory sufficient - Is system in high load state - Is disk remaining space sufficient - Are there any errors in disk volume

Messages	Description	Process
		After confirmation of the above, operate again from the main menu. If the same message stays, collect the log and contact the technicians.
failed to get patch information from software dictionary	Failed to get detailed patches information from software dictionary	Delete the error patches, then download again from the public server or register the downloaded patches. If the same message stays, collect the log and contact the technicians.
failed to instruct the patch download	Failed to instruct the patches download	Delete the error patches, then download again from the public server. If the same message stays, collect the log and contact the technicians.
network error occurred	Failed to download patches due to abnormal network environment	Confirm the following, check the network environment for any abnormalities. - Any problems in IP address settings - Any problems in CS proxy settings (**Use proxy** in window of **CS/DS setup and operation status**) If the problem can't be solved through the above measures, collect the log and contact the technicians.
patch download was deleted	Interruption of service or change of plan caused interruption of patches download	Interruption of service and modification of plan, causing interruption of patches download. No need for processing as download will be performed by next plan. For immediate download, delete the patches and then start download.
this patch is not open to the public	URL not made public	This patch is included in other patches, or no long public, can't download. No need for Process.
Message displayed in public server for example) response status 404 Not Found	Message displayed in public server	Delete the error patches, then download again from the public server or register the downloaded patches. If the same message stays, collect the log and contact the technicians.

3. Click the link of software name, set detailed information of the security patches.

   the following window will be displayed.



4. Set the following items.

Item	Description
Method for registering security patches	Specify registration method of security patches. - Download from the public server Select this item for automatic download when downloading security patches from the public server(Microsoft company's Website). - Register the downloaded security patches Register the downloaded security patches of manual registration. Specify this item when it is impossible to connect to the public server(Microsoft company's Website).

5. Refer to the following notes and key points, check the check box before the security patches to be installed.

Note

After the security patches are selected, all the selected ones will be acquired when the security patches are being acquired automatically to CS from Microsoft company

Therefore, the acquired security patches will squeeze the disk volume. When selecting from here, only select the necessary security patches.

6. Click **Apply** button to save the selection status of the security patches.

6.2.5 Acquisition of Security Patches

Acquire the security patches selected in "6.2.4 Select Security Patches" from Microsoft company and register to CS settings. There are 2 ways to acquire the security patches.

- Automatic acquisition of security patches
- Manual acquisition of security patches

6.2.5.1 Automatic Acquisition of Security Patches

Carry out automatic acquisition of security patches from Microsoft company and register to CS settings.

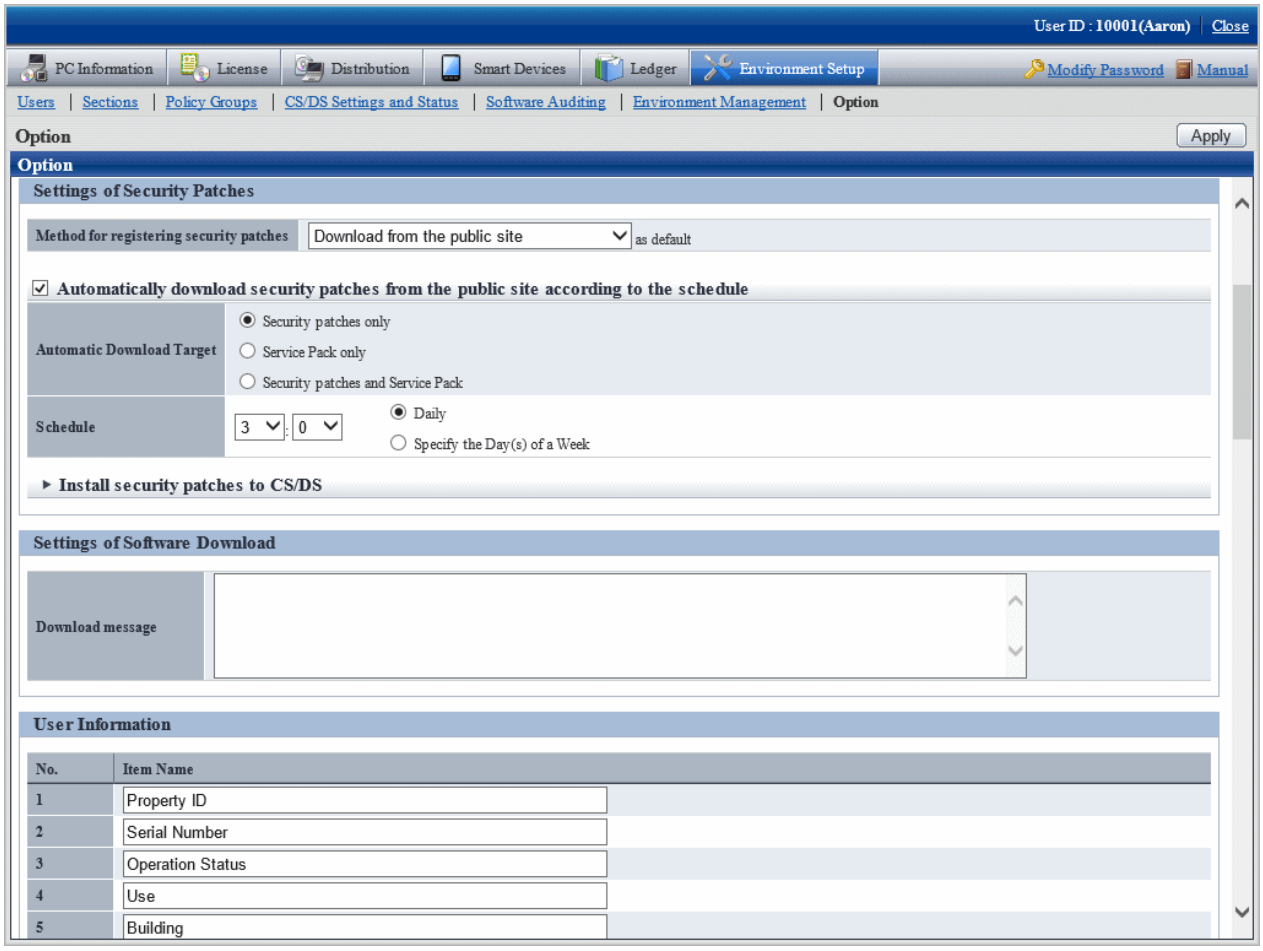
Take the following steps.

1. Log on the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Option**.

   The following window will be displayed.



3. Input the following information to **Settings of Security Patches**.

Item	Description
Method for registering security patches *n* as default	As to the registration method specified in **Security Patches Distribution** of **Settings of Distribution Software - Detailed Settings** in the main menu, select default value from below. - Download from the public sits The security patches automatically downloaded from the public server (Microsoft company's Website) will be set as default. - Specified of the downloaded security patches The downloaded security patches of manual registration will be set as default. Specify this option when the public server (Microsoft company's Website) can't be connected.
Automatically download security patches from the public site according to the schedule	In **Settings of Distribution Software** in the main menu, when the security patches are set as distribution objects, select this item when automatically downloading by the specified plan. Select from below for type of patches can be downloaded automatically. - Security patches only - Service pack only - Security patches and Service Pack Due to the massive module, it will be rather time consuming to download service pack from the public server of Microsoft company. Select **Only security patches** when manually registering and using the service pack provided by CD-ROM.
Schedule	Set up the plan to download from the public server of Microsoft company. The original value is set as 3:00 each day. - Daily Download at the specified time each day. - Specify the Day(s) of a Week Download on the specified day of the week. Outside the specified week, even the **Automatic patches installation** group in the software dictionary has the new Install Patches, download won't be able. Specify more than 1 day of the week.
Install security patches to CS/DS	Select when installing the security patches to CS and DS. Select more than 1 server to be installed when selecting.

4. Click the **Apply** button.

When service pack is selected for patch selection, sometimes it will take excessive time to acquire due to network conditions. Therefore it is suggested to register manually from CD-ROM or other. Refer to relevant contents in "6.2.5.2 Obtain Security Patches Manually" for manual registration.

6.2.5.2 Obtain Security Patches Manually

Manually obtain security patches from Microsoft and register to CS settings. Take the following steps.

- Manually obtain from Windows Update directory and log on the security patches
- Register and obtain the security patches from CD-ROM and other.

Manually obtain from windows update directory and register security patches

Take the following steps to manually obtain from Windows Update directory and register the security patches.

Early Preparations

It is necessary to connect to Microsoft company's website setup via network to download.

In addition, decide in advance if it is necessary to create a destination folder to save the downloaded security patches. At this time, also pay attention to remaining disk capacity.

Start IE and Connect to Microsoft Update Catalog

Start IE, and display the Microsoft Update Catalog page:

http://catalog.update.microsoft.com/

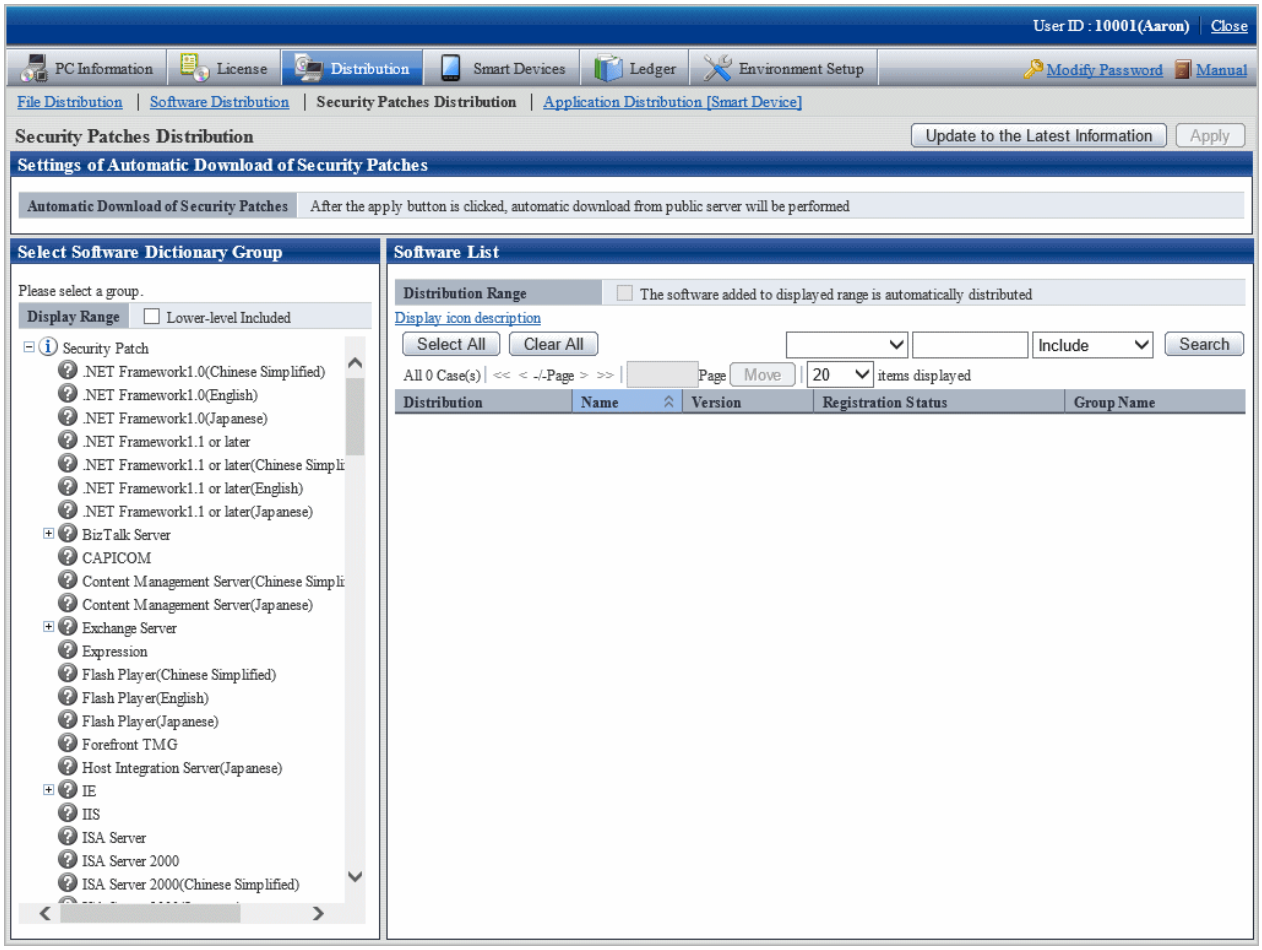
About the latest steps, confirm from Microsoft company's home page.

Settings of Security Patches

Take the following steps.

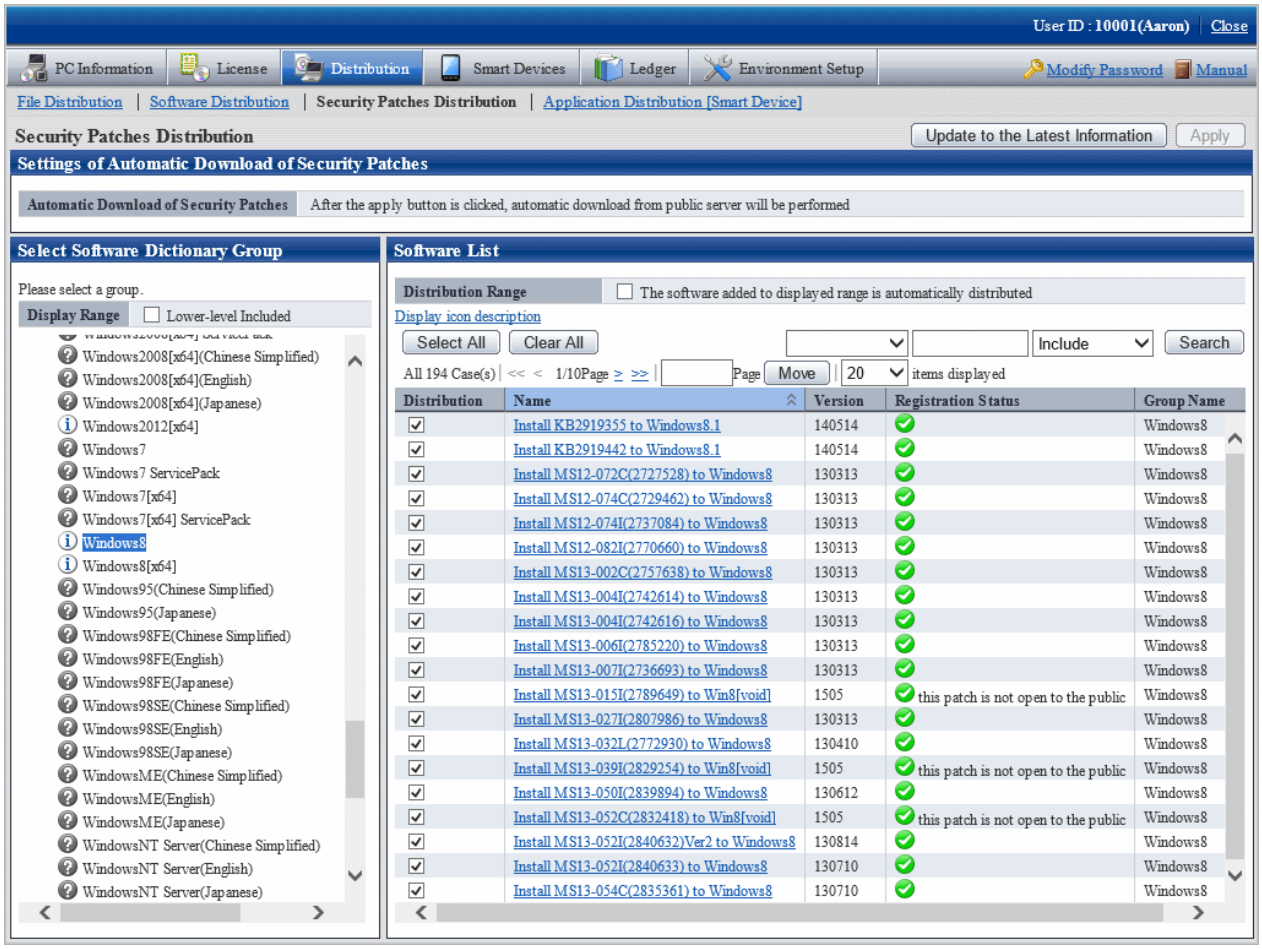
1. Log on the main menu, click **Distribution** and then click **Security Patches Distribution**.

   The following window will be displayed.



2. Select the directory under the security patches on left field of the window.

   List of the selected security patches will be displayed on right side of the window.

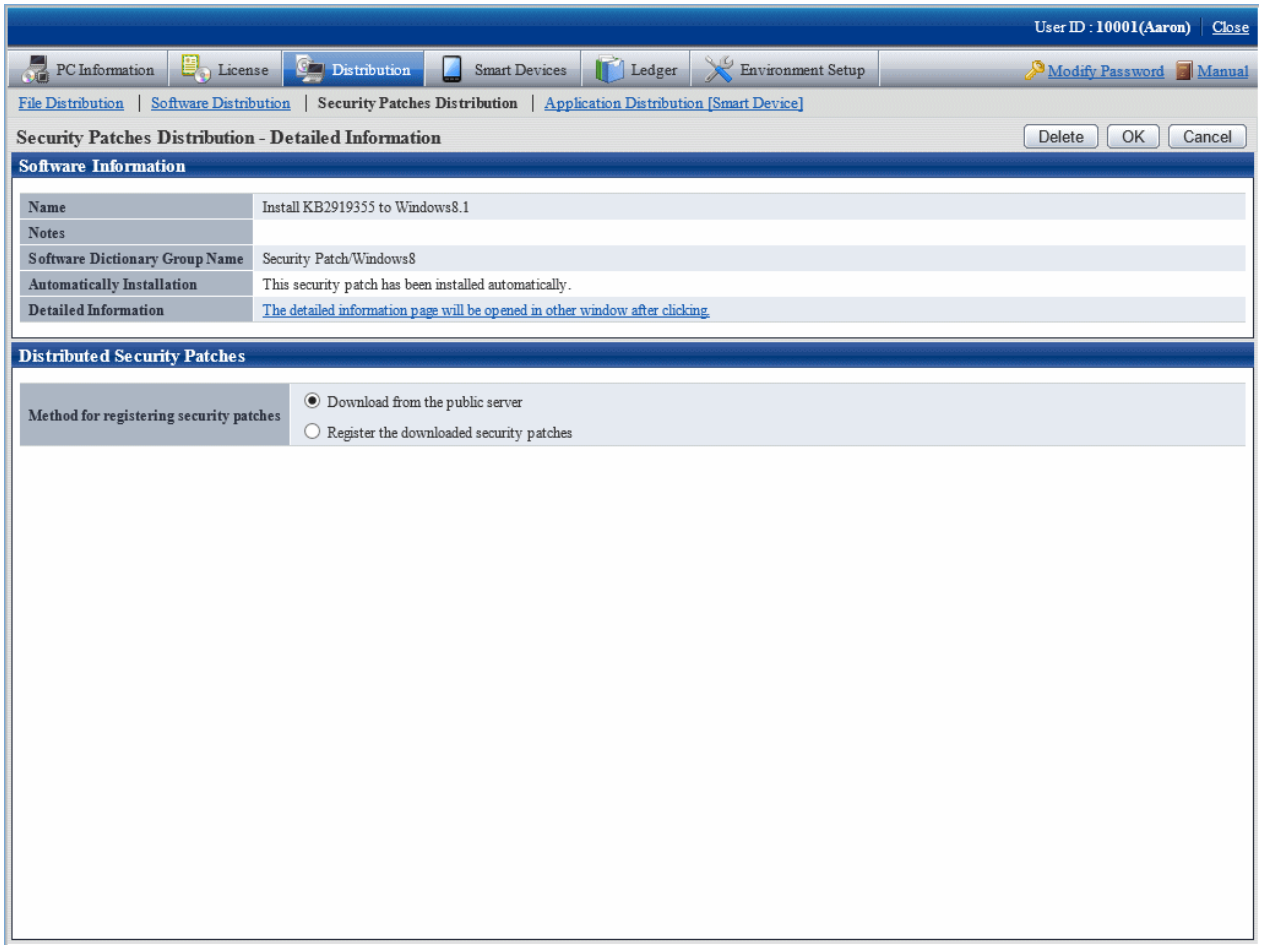


   Select security patches from the tree view on left field of the window, then confirm the KB number recorded in ( ) of patches list on right side of the window.

   The KB number shall correspond to file name of the downloaded security patches.

3. Click link of the target security patches.

   The following window will be displayed.



4. Select the single choice button of **Register the downloaded security patches** to specify the security patches to be downloaded manually.

5. Click **OK** button then register the security patches.

   The folder name varies depending on each security patch. Do not mess up the formatted file of execution of the security patches during registration.

   Basically, all the file names are attached with a KB number to correspond to the KB number recorded in ( ) in patches list in the main menu.

   After confirmation of the file name, click **OK** button.

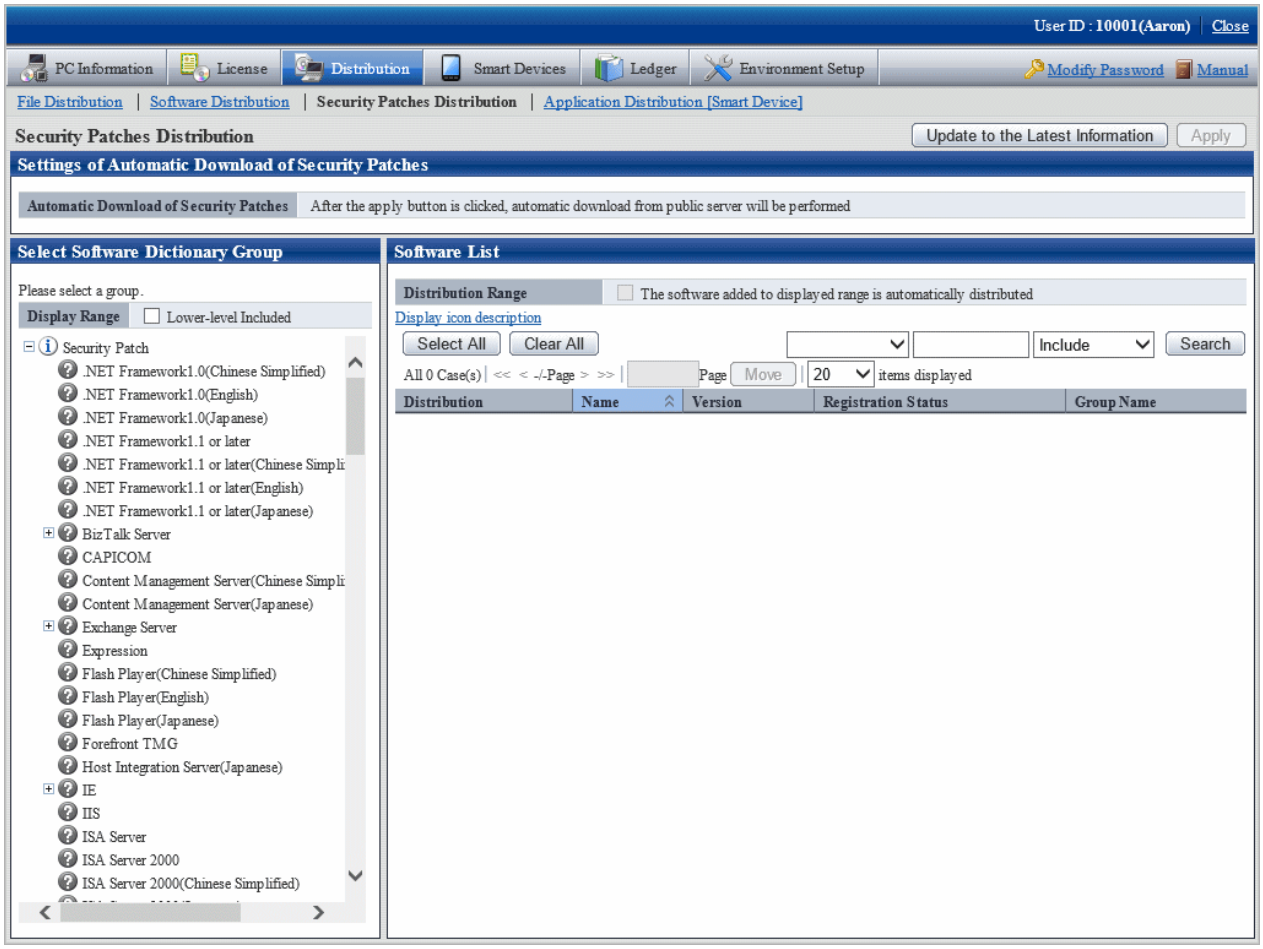
6. Repeat the operations according to number of the target security patches.

Obtaining of security patches through registration of CD-ROM and other

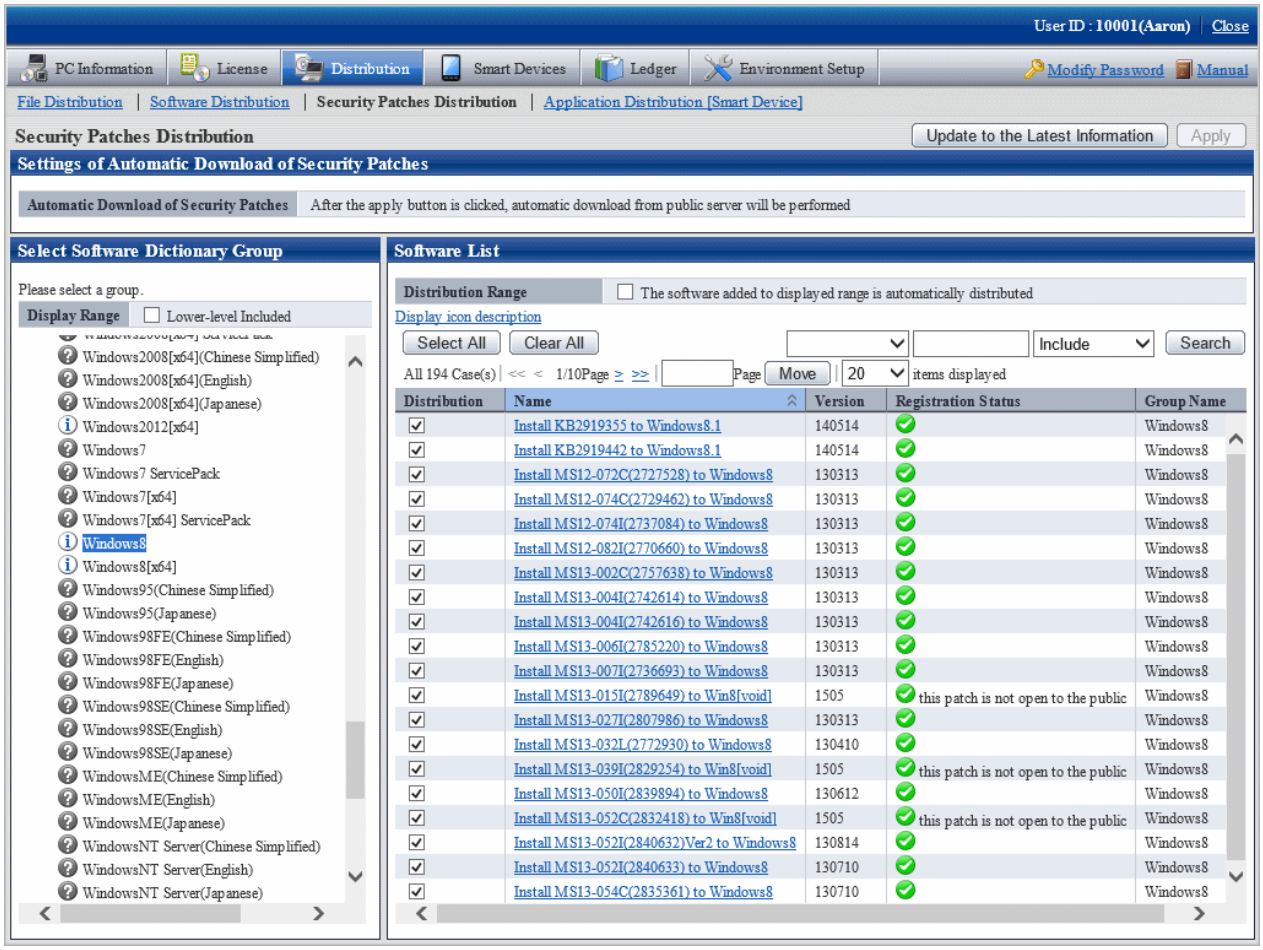
Take the following steps to obtain security patches through registering and passing CD-ROM and other.

1. Log on the main menu, click **Distribution**, and then click **Security Patches Distribution**.

   The following window will be displayed.



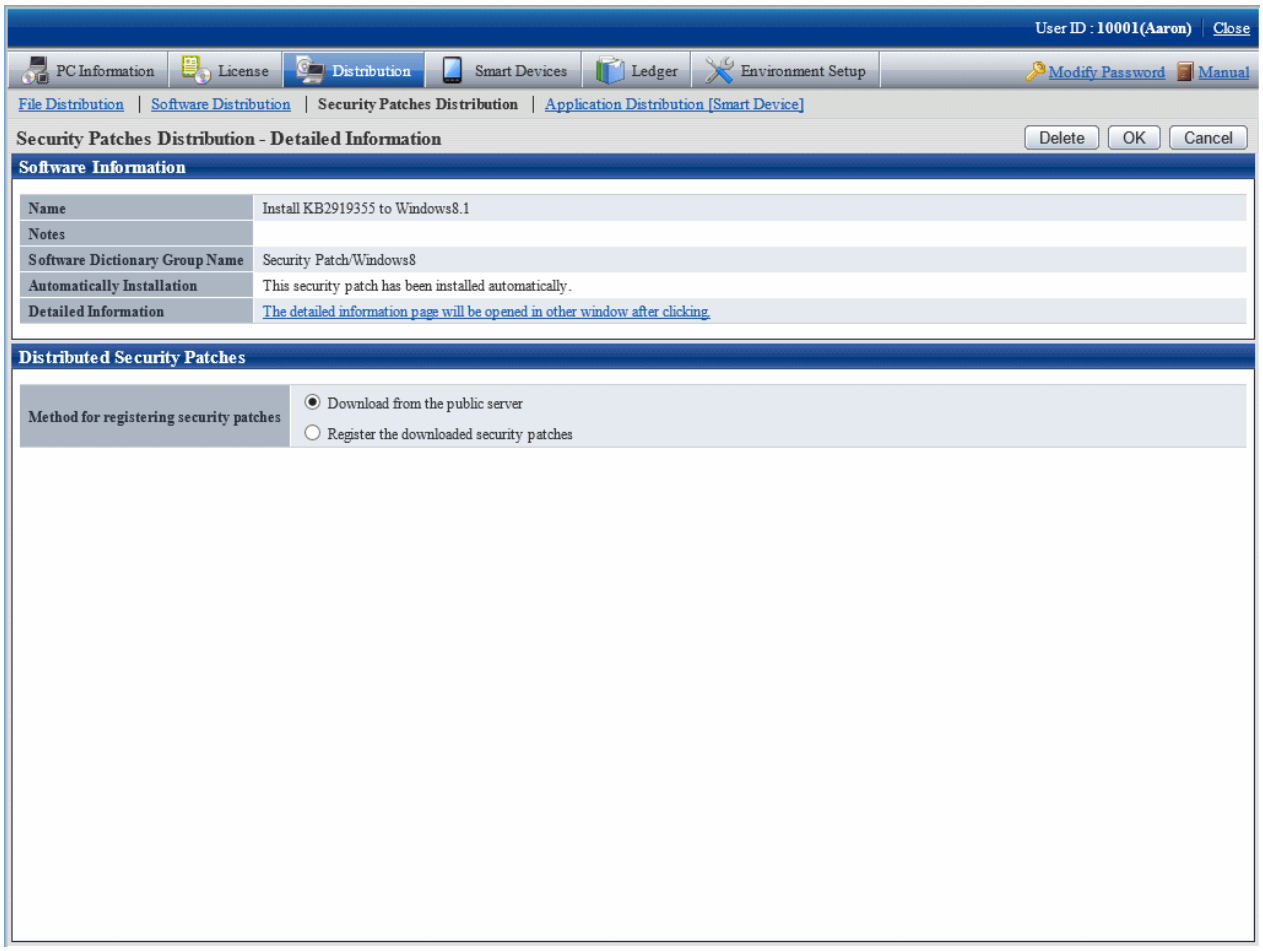
2. Click the link of security patches to be registered on right side of the window.



When the security patches to be registered are not shown, select the directory under the security patches from the tree view on left field of the window to show the security patches to be registered.

Refer to "6.2.4 Select Security Patches" for selection of the security patches.

The following window will be displayed.



3. Select the single choice button of **Register the downloaded security patches** to specify the destination path to save the security patches obtained from CD-ROM and other.
4. Click **OK** button to register the security patches.

6.2.6 Settings of Installation & Distribution Intervals of Security Patches

Set the interval of automatic installation of the security patches. In addition, interval of security patches distribution from CS to DS, and settings of the new message displayed on CT will also be set.

For more information about installation of the security patches, refer to relevant contents of "Note" in "6.5 Type of Use".

Note

When installing the security patches of Microsoft's Office, sometimes the CD-ROM of Office installation is installed. The security patches requiring the CD-ROM won't be installed to CT automatically.

Instruct to manually install the security patches from the software download window on the Client using CT.

Note

Under the following circumstances, the security patches can't be installed automatically.

Operate from the main menu again as per steps of "6.2.4 Select Security Patches" and "6.2.5 Acquisition of Security Patches".

- The new security patches are selected in the main menu, but the download operation is not performed.
- Fail to download the selected security patches.

Installation interval of security patches

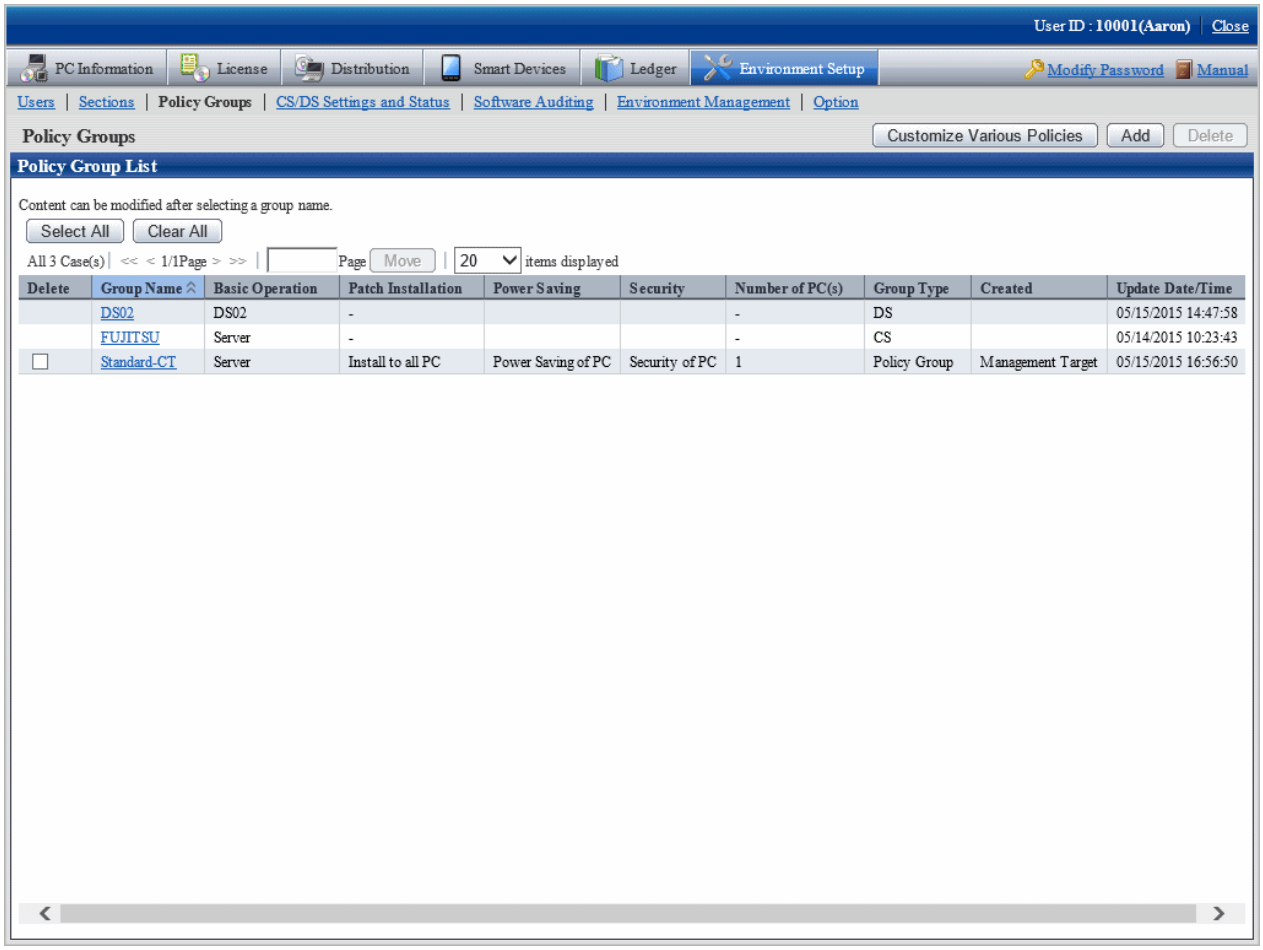
Set the interval of security patches not installed to automatic installation to CT.

1. Log on the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

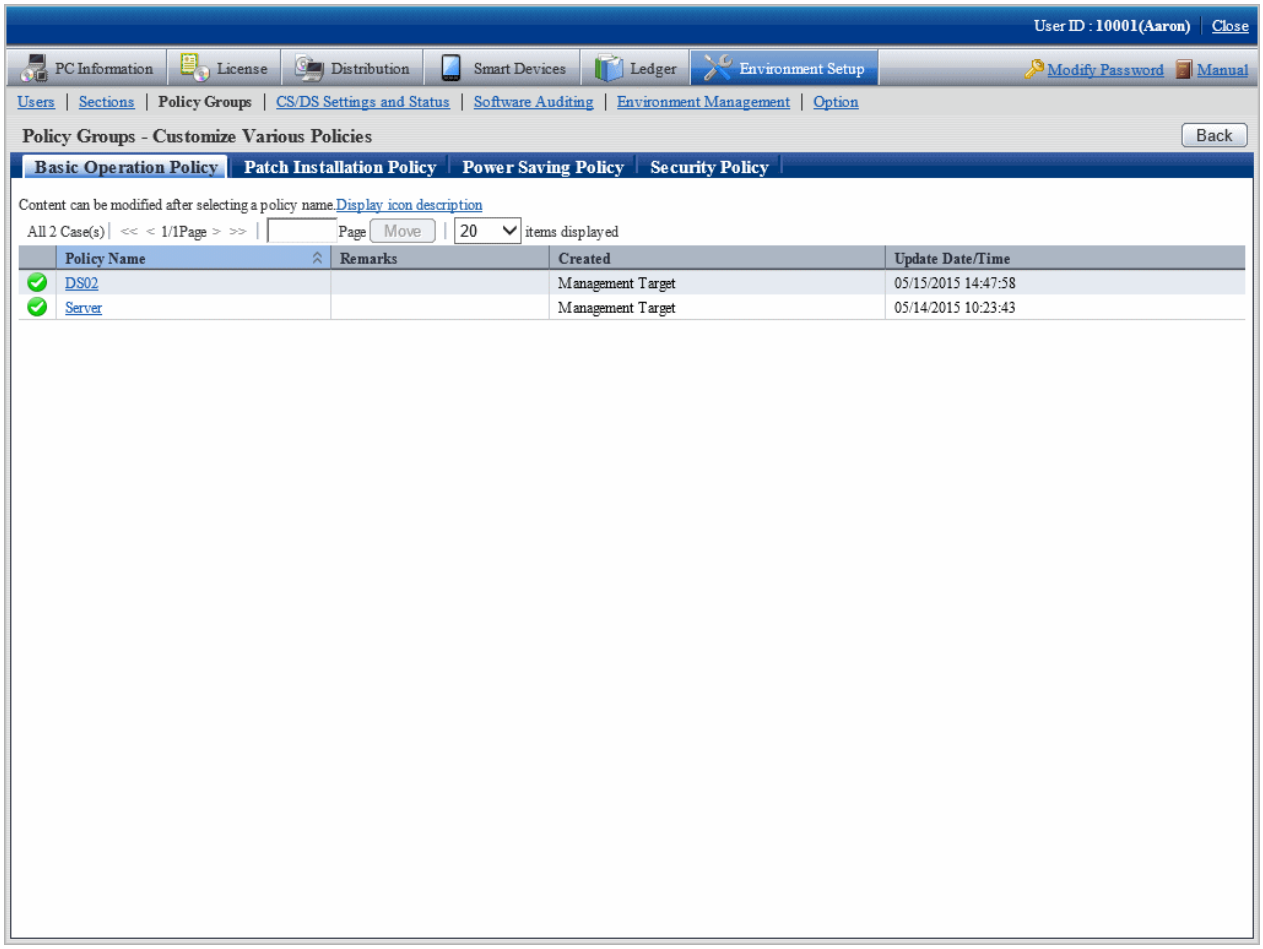
2. Click **Policy Groups** .

   The following window will be displayed.



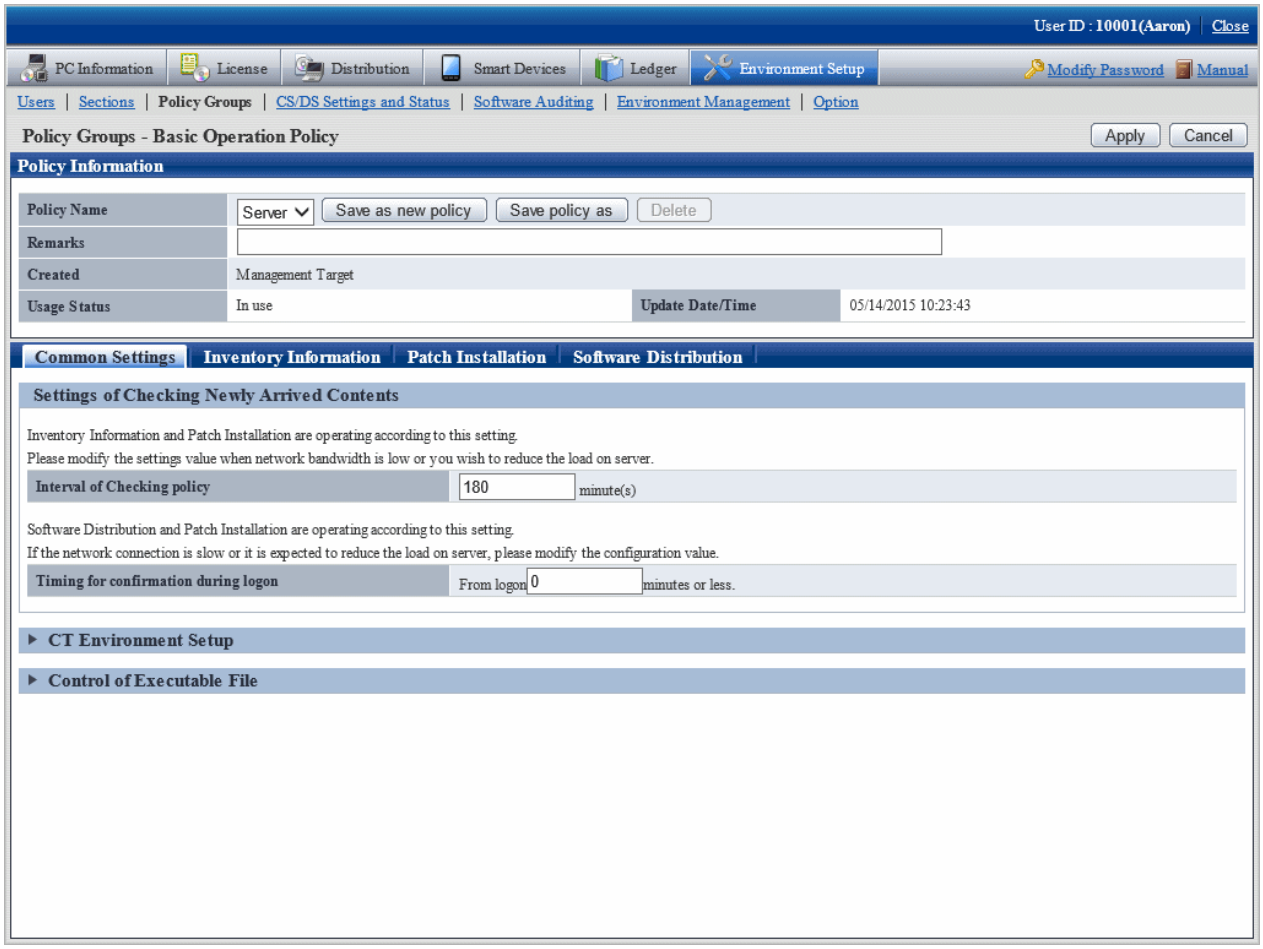
3. Click the **Customize Various Policies** button.

   The following window will be displayed.



4. Click the link of policy name in the tab of **Basic Operation Policy**.

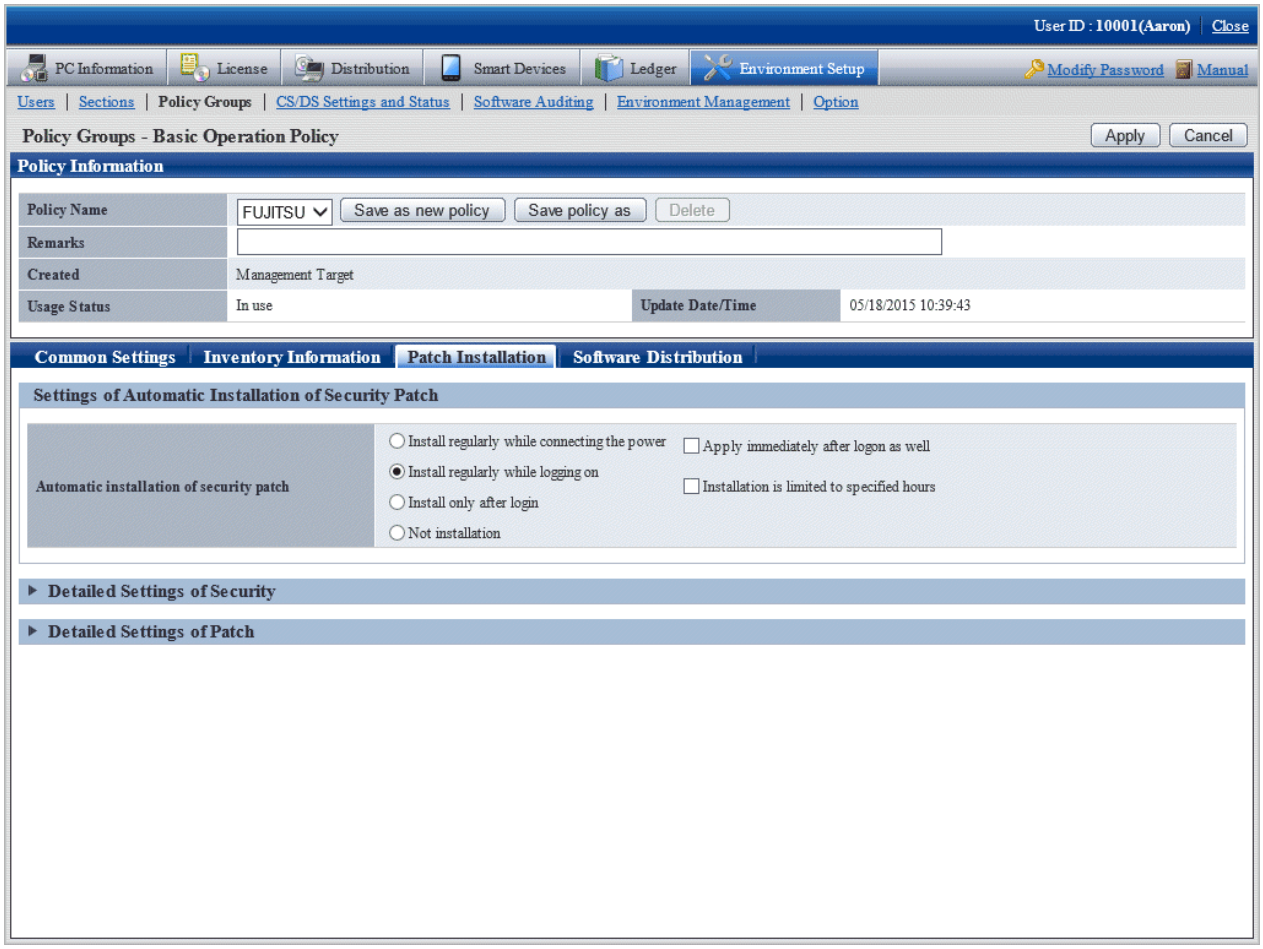
   The following window will be displayed.



   - Confirm with the server if there are patches to be installed according to the interval of set value (minute) of **Interval of Checking policy**.

5. Click the tab of **Patch Installation**.

   The following window will be displayed.



   - Select the operation time point of patches installation according to the set value of **Automatic installation of security patch**.

6. For more Detailed Settings, click the **Detailed Settings of Security** and **Detailed Settings of Patch** in the window for display.

   Refer to relevant contents of "6.5 Type of Use" for setup contents.

Distribution interval of security patches

Set the time interval of security patches distributed from CS to DS. Short installation intervals can be set when important security patches are distributed so that they are distributed to DS and installed to CT as soon as possible.

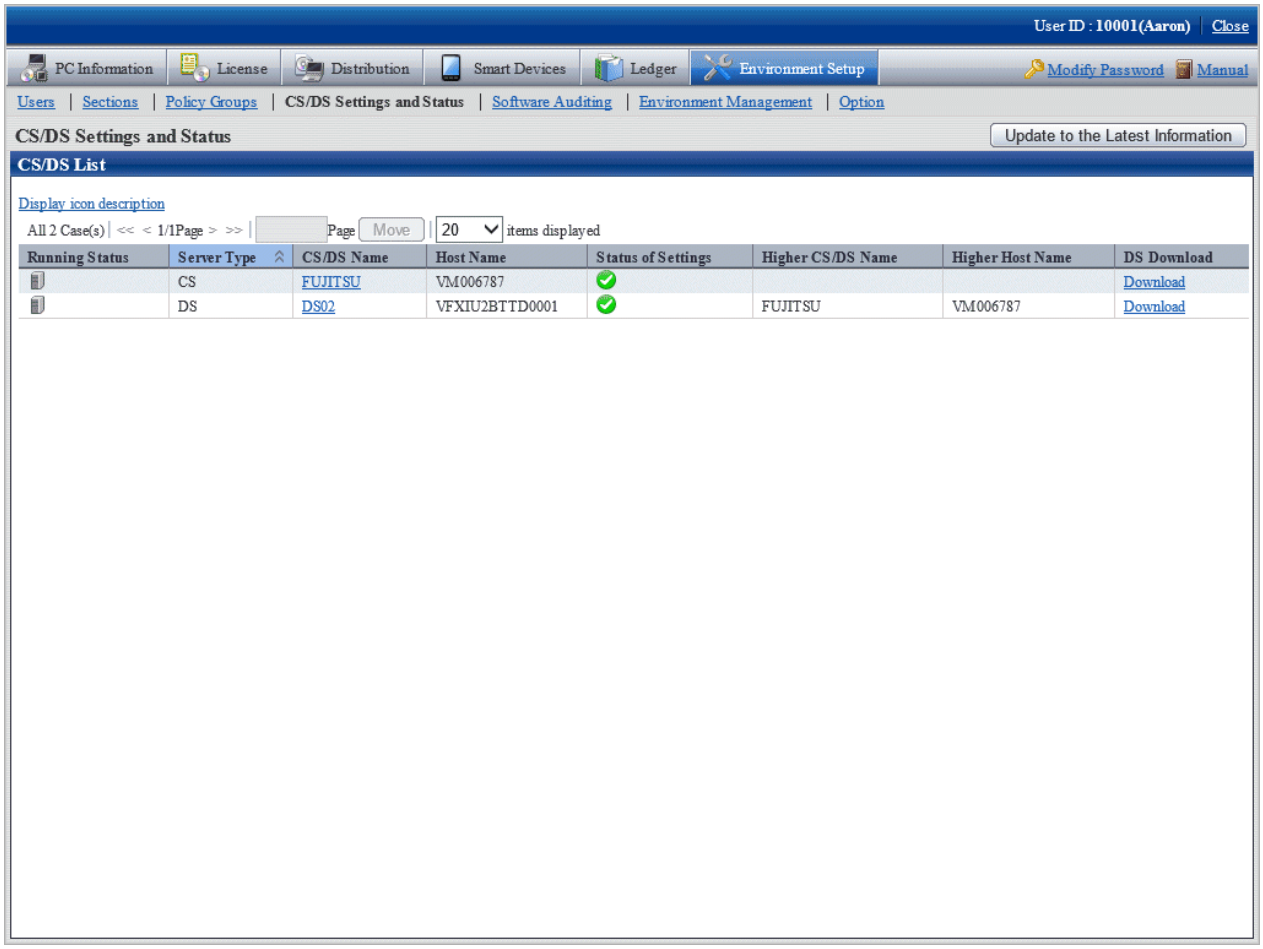
Take the following steps.

1. Log on the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

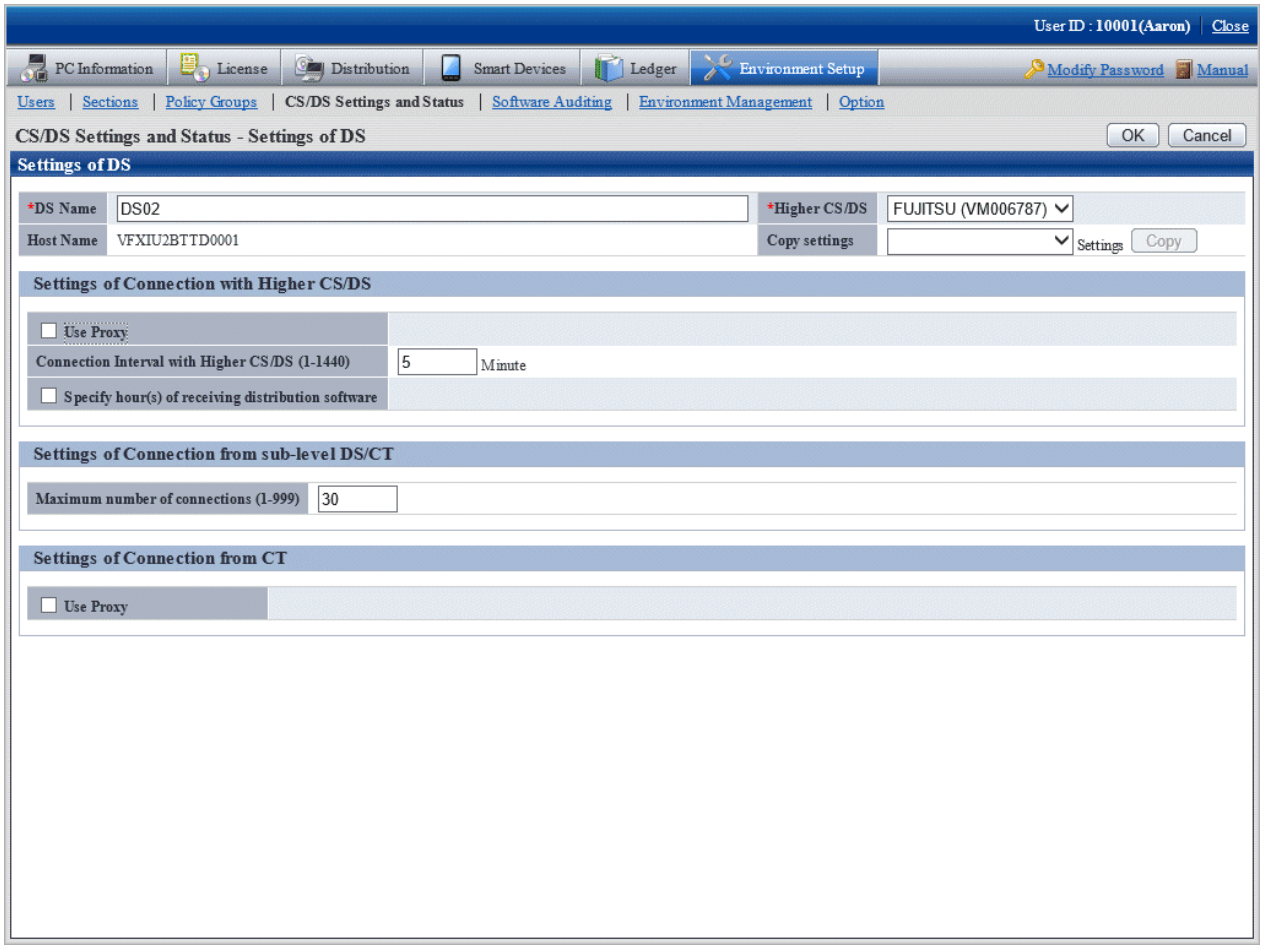
2. Click the **CS/DS Settings and Status**.

   The following window will be displayed.



3. Click the link of DS name.

   The following window will be displayed.



4. Input the item below **Settings of Connection with Higher CS/DS**.

Item	Description
Connection Interval with Higher CS/DS	Specify the period of software download from superior server, a value within 1 - 1,440 minute. Default to 30, not omissible.
Specify hour(s) of receiving distribution software	Select when designating the time period of software download. Specify the time period of software download from superior server. Without selection, the download time period can be any time in 24 hours. The hour unit is specified to be 0 - 23, the minute unit is specified to be 0 - 59. The start time cannot be specified the same as the end time.

5. Input item contents under **Settings of Connection from sub-level DS/CT**.

Item	Description
Maximum number of connections	Total number of inferior DS or CT communicating with CS or DS simultaneously, specify between 1 and 999 (number of pieces). Default to 30, not omissible.

6. Click **OK** button.

6.3 Setup as Needed

In acquisition and installation of the security patches, perform the following operations when necessary.

- Delete the security patches
- When important security patches are made public
- Set retry times and message of security patches installation
- Install security patches to server

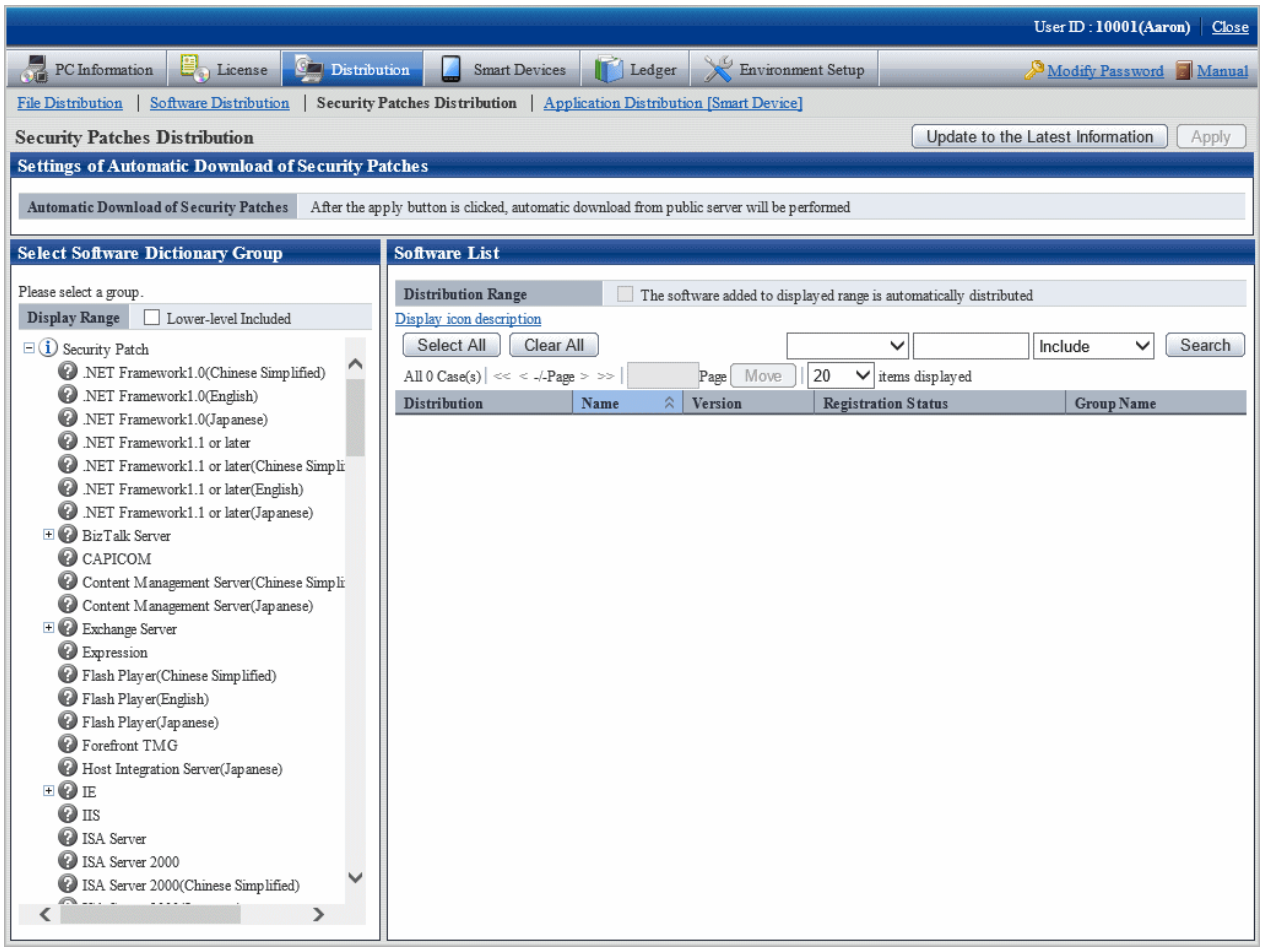
6.3.1 Delete Security Patches

When the downloaded security patches squeeze the disk capacity, delete the security patches judged to be unnecessary.

Take the following steps.

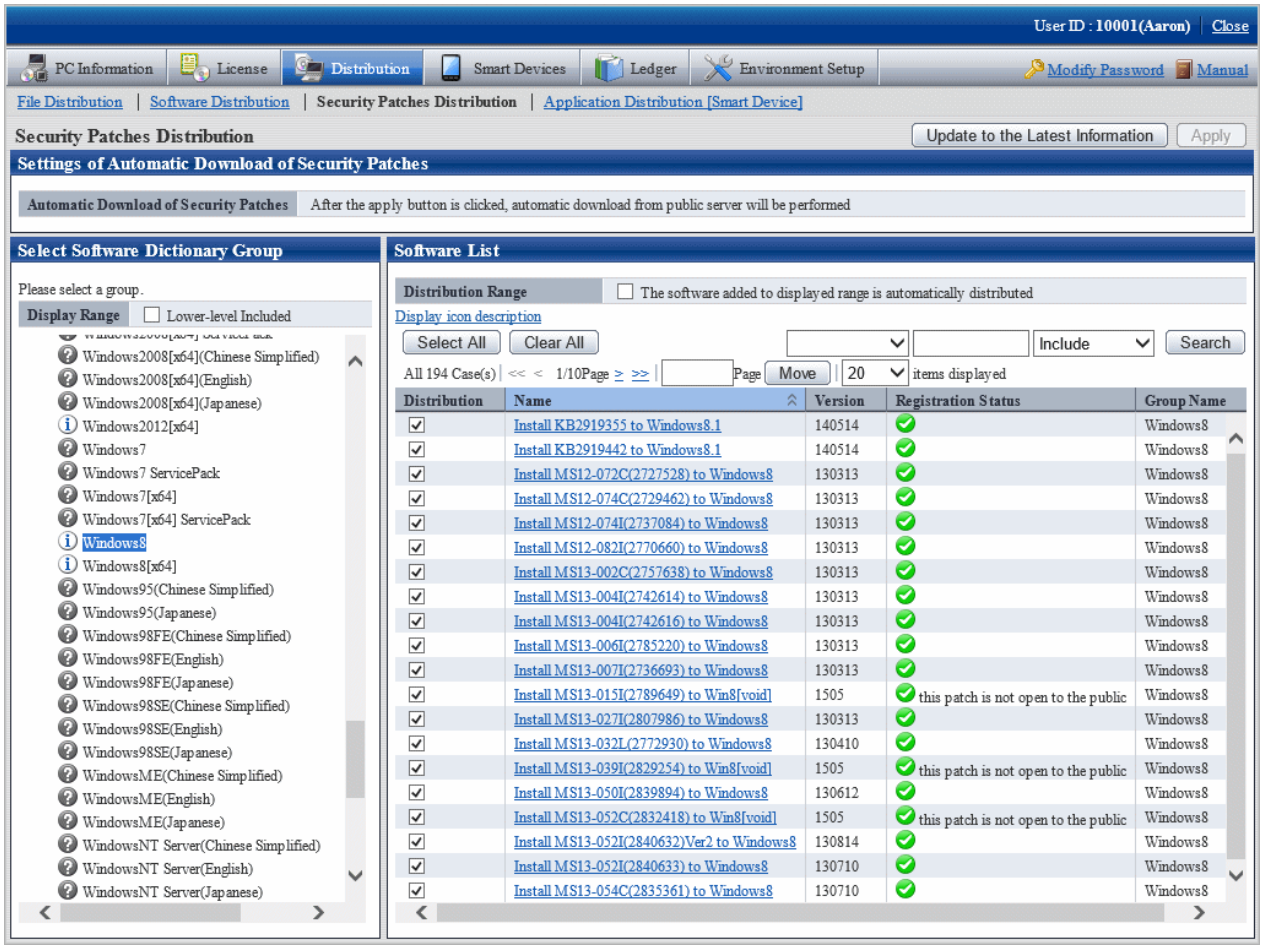
1. Log on the main menu, Click **Distribution**, then click **Security Patches Distribution**.

   The following window will be displayed.



2. Select the directory under the security patches on left field of the window.

   List of the selected security patches will be displayed on right side of the window.



3. Delete the check box of unwanted security patches by judgment.

> **Note**
>
> The security patches with checked check box deleted won't be the automatic installation objects.

6.3.2 When Important Security Patches are Made Public

If the following operations are adopted when important security patches are made public, sometimes the installation to CT will be delayed.

- Automatic acquisition by CS of the security patches distributed by Microsoft company
- Automatic installation to CT of the security patches registered to CS
- Automatic installation to CT after the security patches distributed by Microsoft company are automatically acquired by CS

In the above operations, the security patches are acquired from Microsoft company and installed to CT automatically by plan. When important security patches are made public, installation delay will be caused due to time point of the plan.

Important security patches distributed by Microsoft company shall be installed to CT immediately, or use the Software Distribution function to distribution the security patches to CT when there is not enough time to obtain the software dictionary of the security patches. After that, instruct to install the security patches from the software download window on Client using CT. Refer to relevant contents of "Chapter 8 Distribute Software" for setup contents.

6.3.3 Set Retry Times and Message When Installation of Security Patches Fails

It is necessary to set the retry times and message of security patches installation to treat the failure of automatic installation of the security patches in CT.

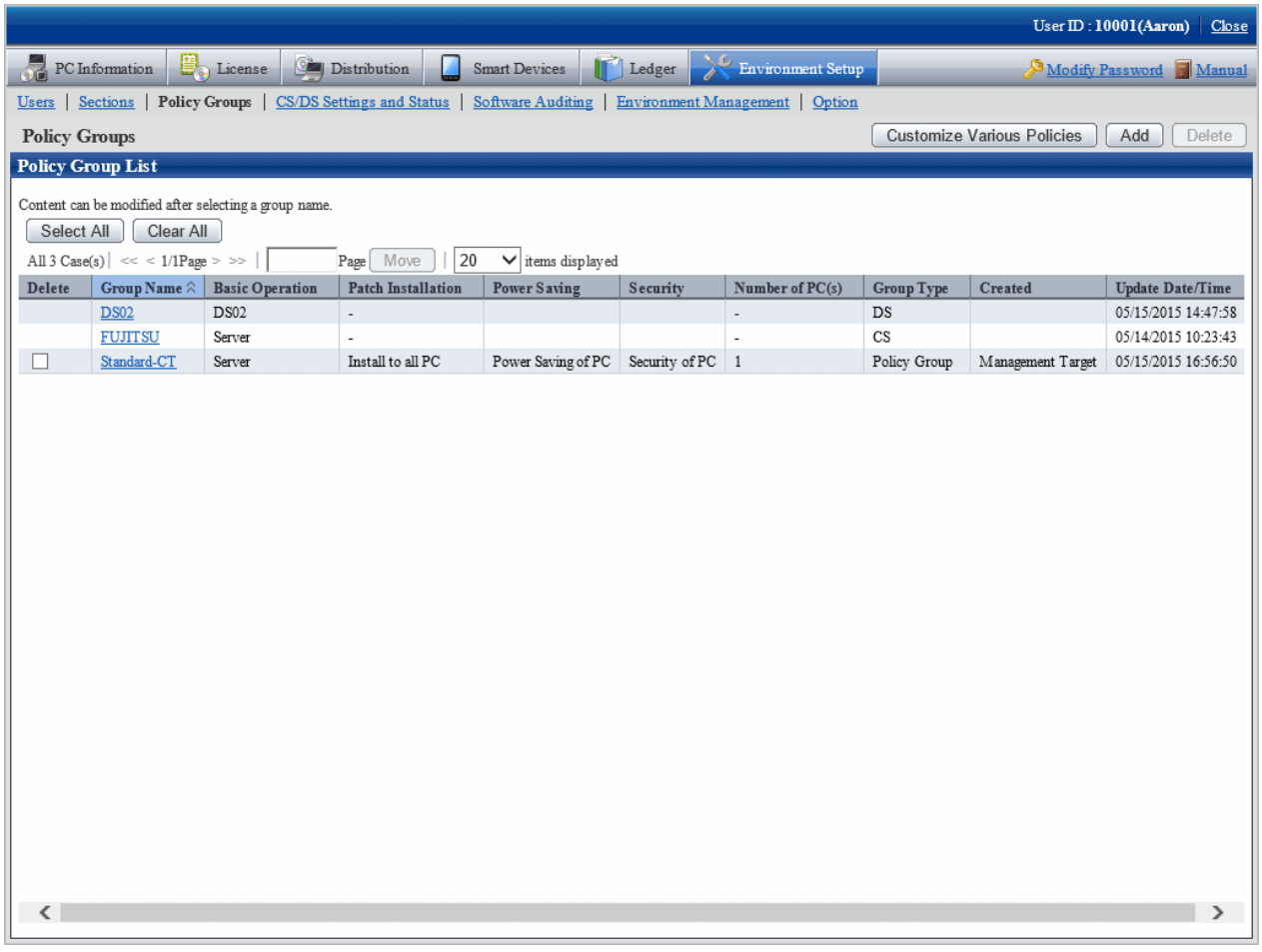
Take the following steps.

1. Long on the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

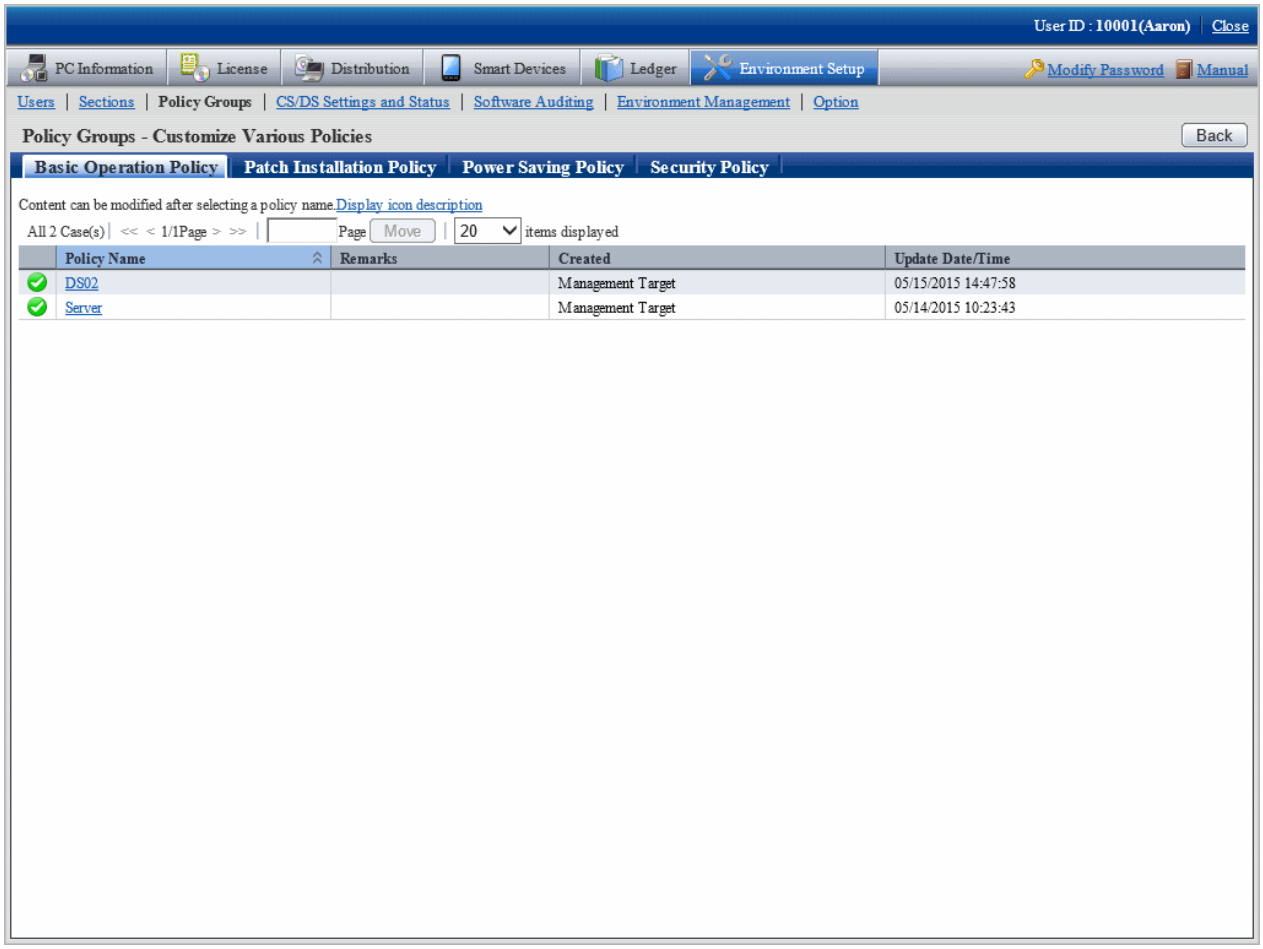
2. Click **Policy Groups** .

   The following window will be displayed.



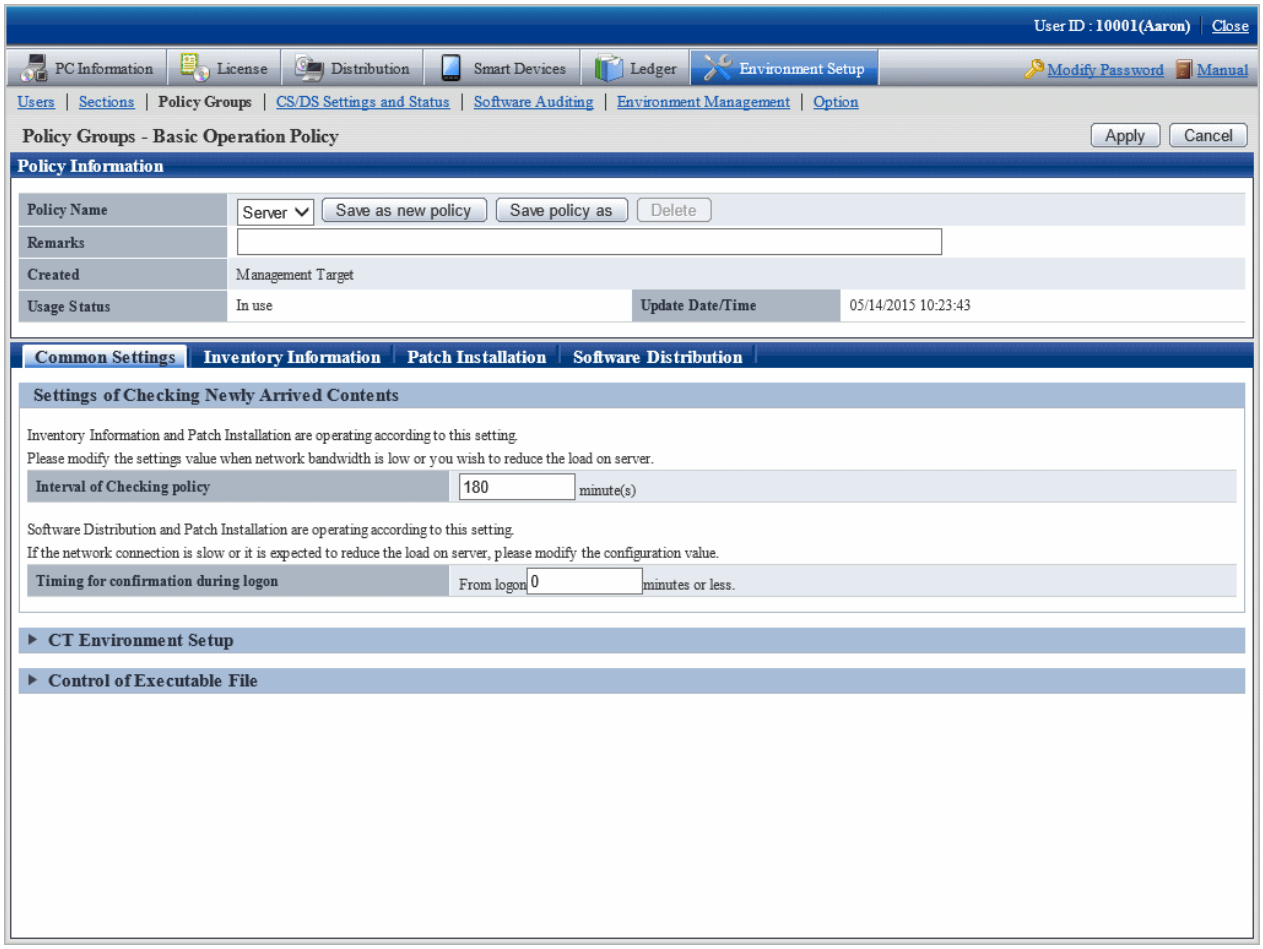
3. Click **Customize Various Policies** button.

   The following window will be displayed.



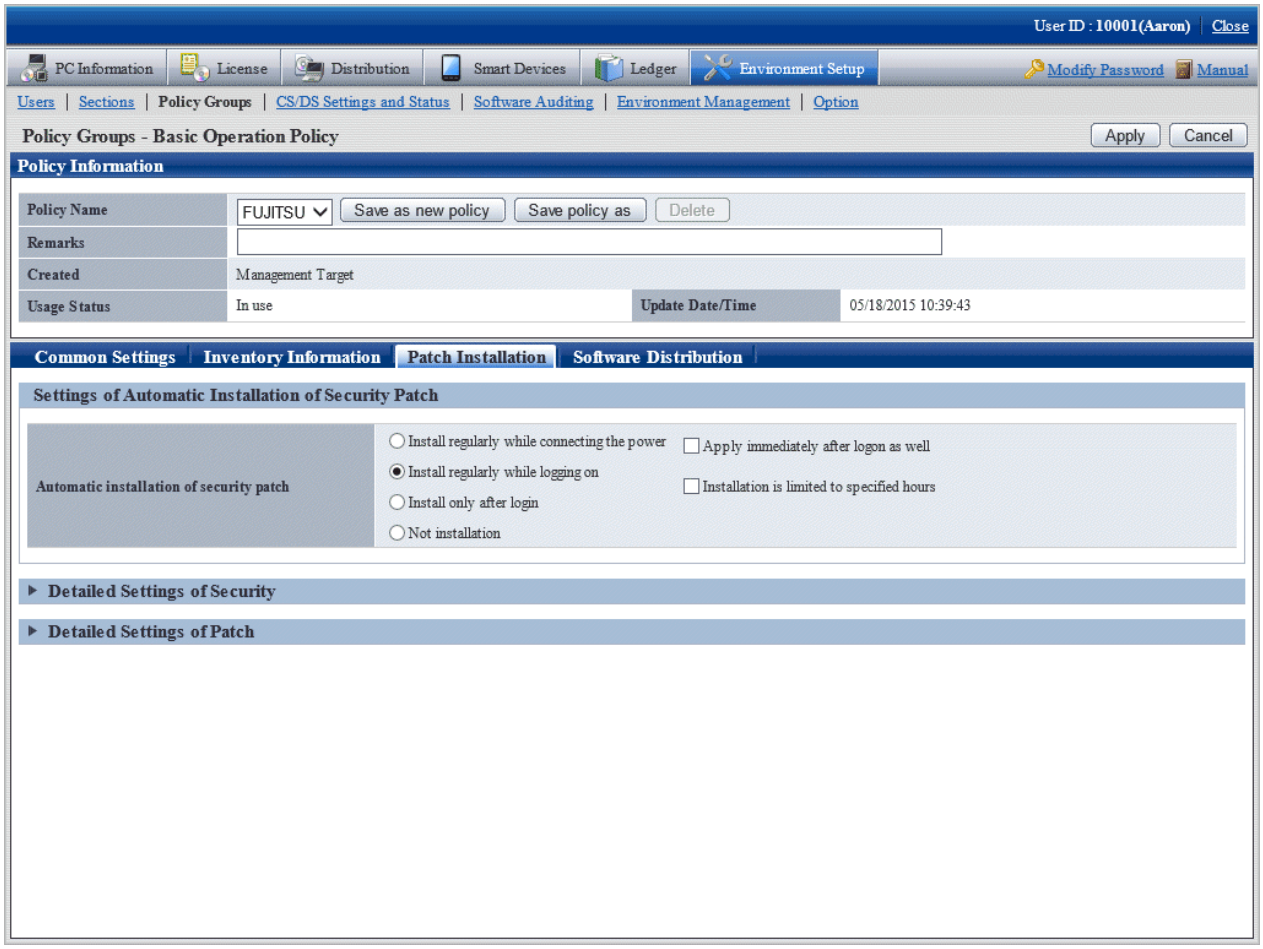
4. Click link of the policy name of the **Basic Operation Policy** tab.

   The following window will be displayed.



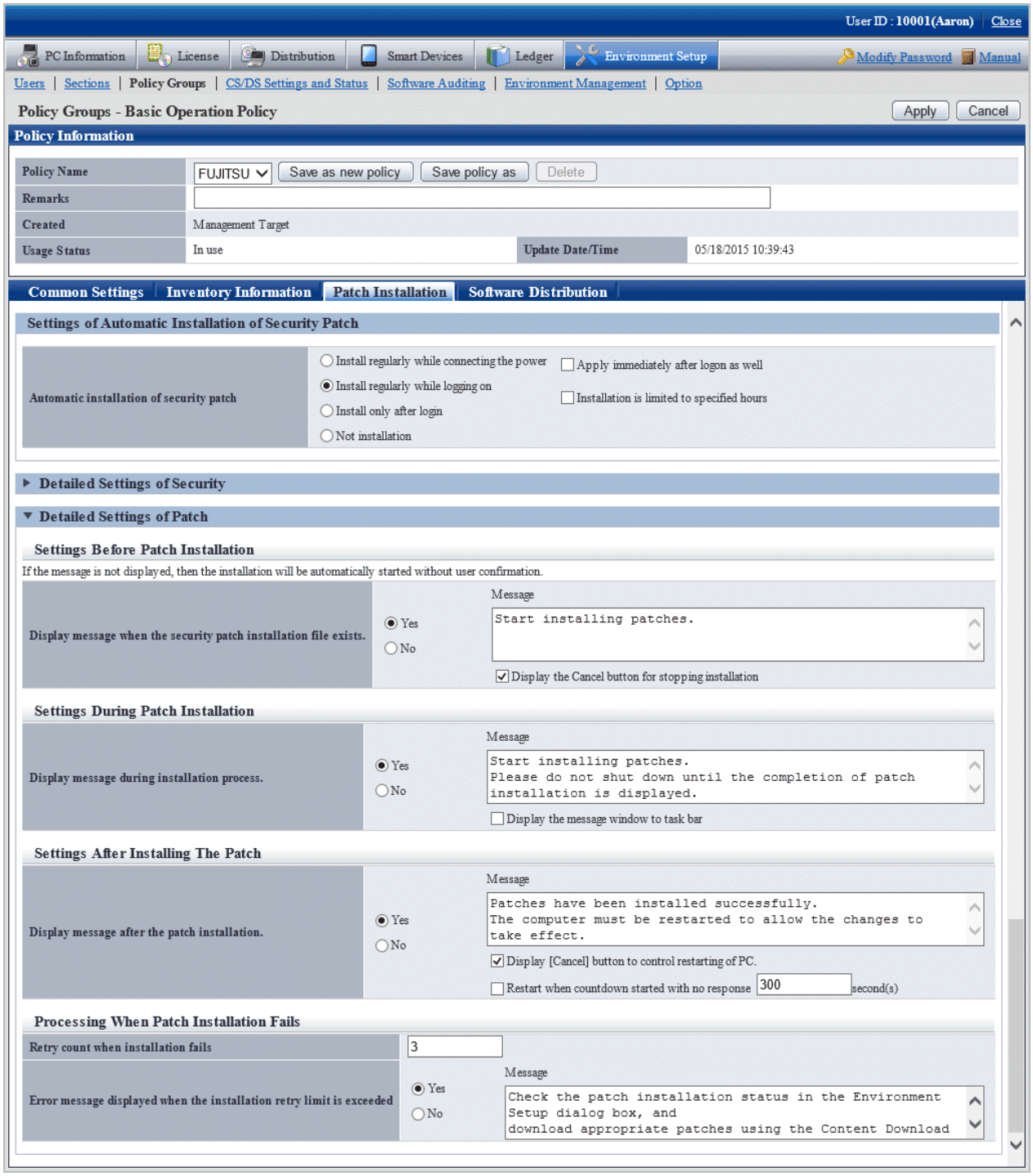
5. Click the **Patch Installation** tab.

   The following window will be displayed.



6. Click **Detailed Settings of Patch**.

   The following item will be displayed.



7. Input the following information, click the **Apply** button.

   - Process of patches installation failure

     - Textbox of **Retry count when installation fails**

     - Select **Yes** in **Error message displayed when the installation retry limit is exceeded**

     - Textbox of **Message**
       Specify up to 1,024 fullwidth characters or 2,048 halfwidth characters.

6.3.4 Steps to Install Security Patches to Server

CT will also be installed in the PC which is installed with CS and DS. In the original setup, the CT installed in CS and DS won't use the security patches automatically.

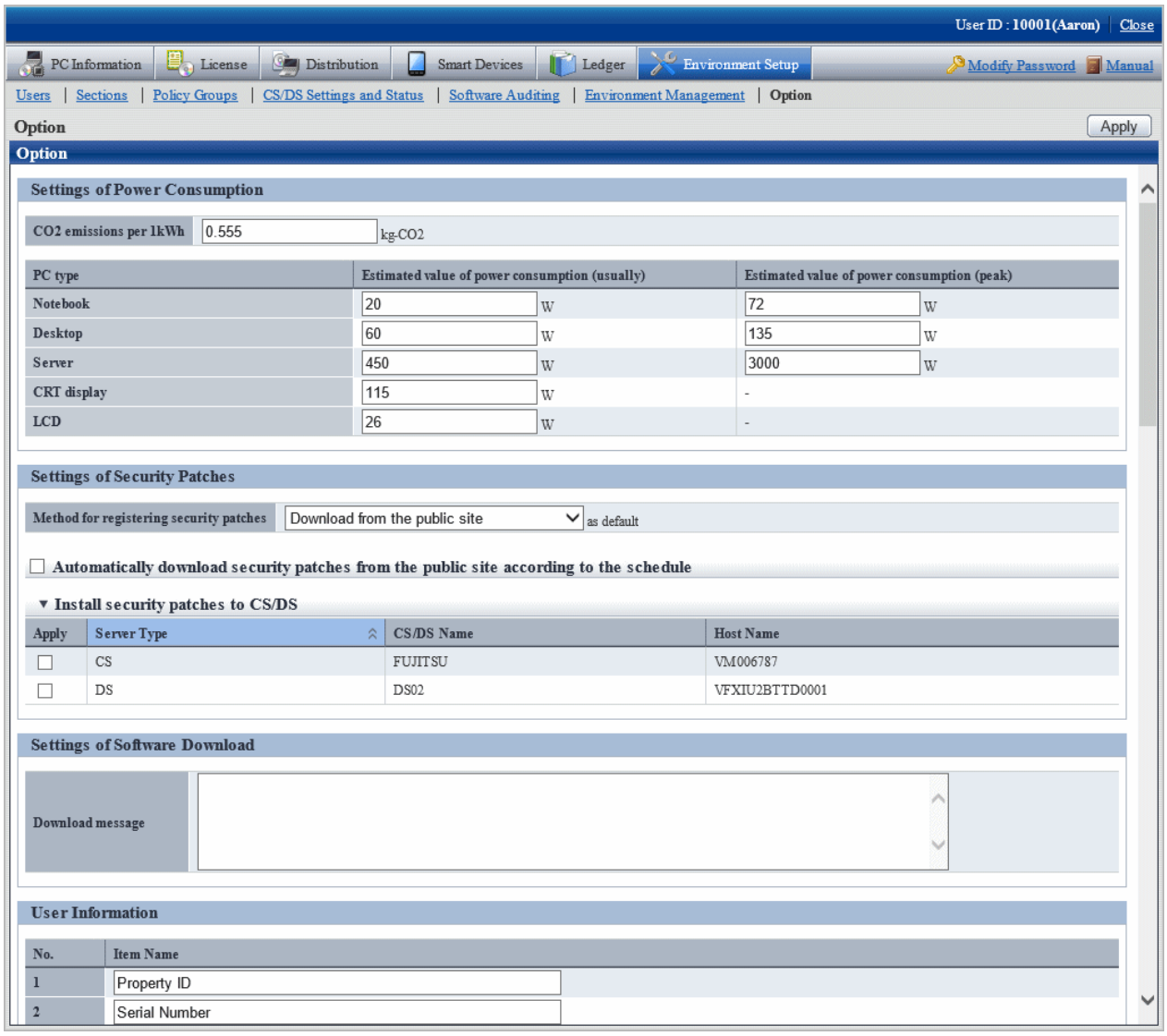
In addition, if CS and DS belong to the policy, the patches will be installed according to the setup by unit of the policy group.

No automatic patches installation for original value of CS and DS. Therefore, the administrator shall take manually as per the following steps to install the security patches on CS and DS.

1. Confirm if there are any problems of installation state of the security patches on CT outside of CS and DS in **PC information** in the main menu.

   Refer to relevant contents of "Steps to confirm installation" for confirmation method.

2. In window of **Environment Setup** > **Option** in the main menu, select the check box of server name of **Install security patches to CS/DS**, click the **Apply** button.



3. As per the specified distribution plan, the Client policy will be distributed to CS and DS, the security patches will be distributed for installation as well.

4. Confirm if there are any problems of security patches status of CT installation on CS and DS in **PC Information** in the main menu.

   Refer to "Steps to confirm installation" for confirmation method.

5. In window of **Environment Setup** > **Option** in the main menu, delete the selection of check box of server name of **Install security patches to CS/DS**, click the **Apply** button.

6.4 Confirmation

Confirm if CS has normally acquired the security patches distributed by Microsoft company. In addition, confirm if the security patches have been installed to CT normally.

6.4.1 Confirmation of Acquisition of Security Patches

This section explains herein how to confirm if the security patches distributed by Microsoft company have been acquired. If the normal acquisition fails, the security patches won't be able to be installed to CT. it also explains the Processing method to acquisition failure of the security patches.

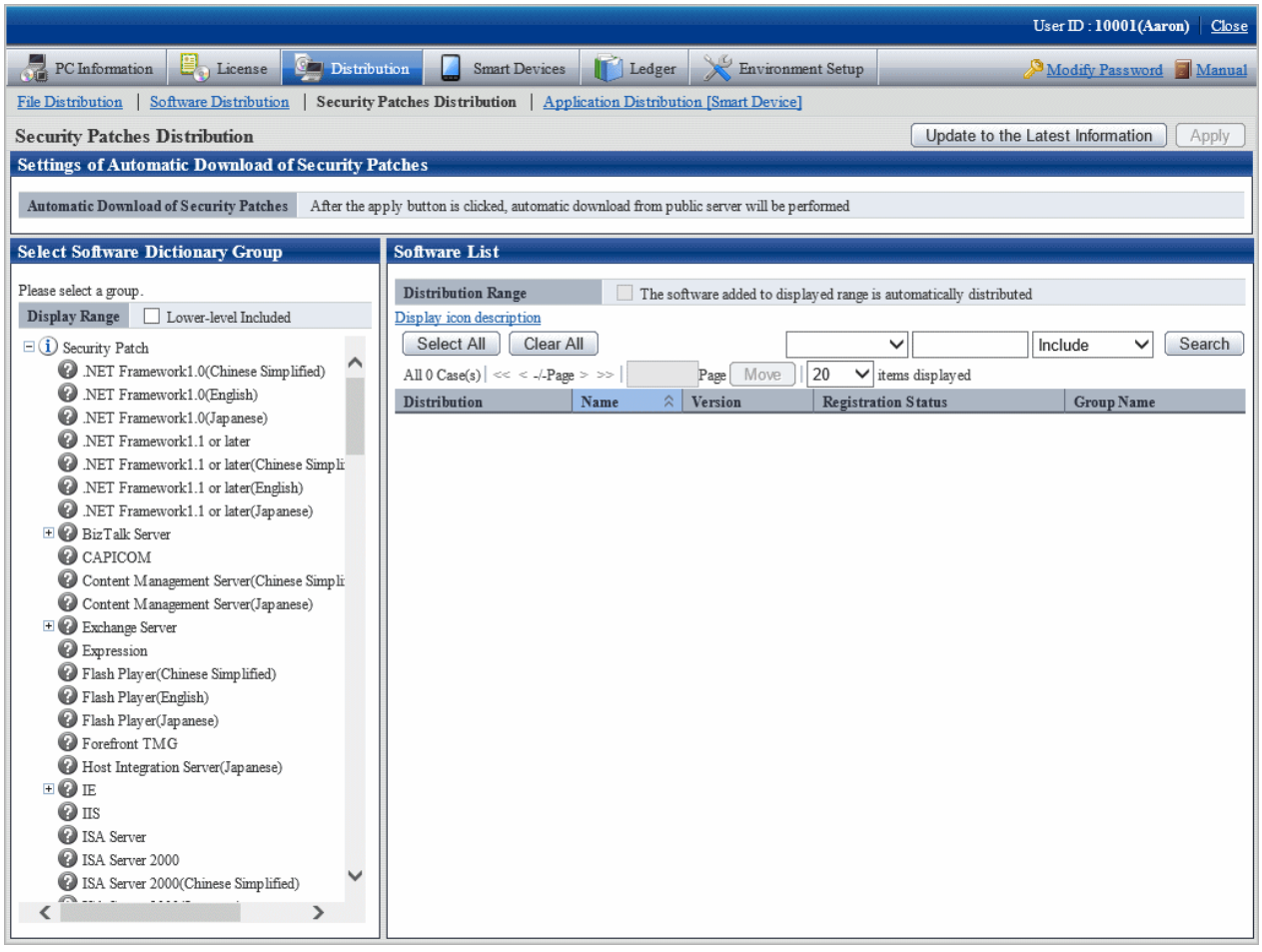
Steps to confirm acquisition

It describes how to confirm if the security patches distributed by Microsoft company have been acquired.

Take the following steps.

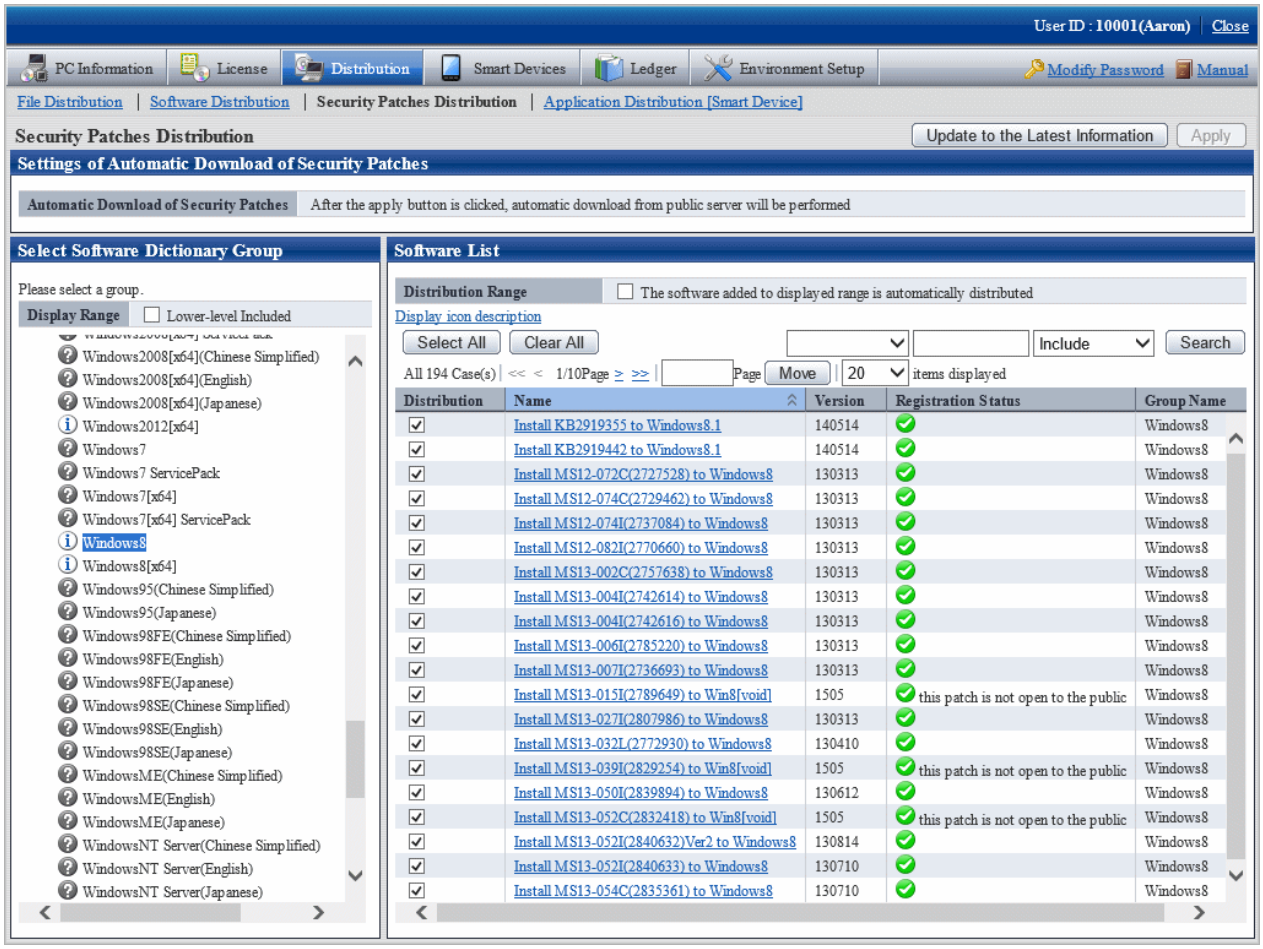
1. Log on the main menu, click **Distribution** and then **Security Patches Distribution**.

   The following window will be displayed.



2. Select the security patches to be confirmed for status on left field of the window.

   List of the selected security patches will be displayed on right side of the window.



Confirm **Registration Status** on right side of the window. Meanings of the icons are as below.

Icon	Description
	Security patches registered.
	Security patches being downloaded from public server.
	Fail to download security patches from public server.
None	No security patches downloaded from public server.

6.4.2 Processing to Acquisition Failure

This section explains how to treat the failure to acquire security patches from Microsoft company. There are 2 ways to acquire the security patches.

- Automatic acquisition of security patches
- Manual acquisition of security patches

Processing to automatic acquisition failure of security patches

If the automatic acquisition fails, refer to "Manually acquire and register security patches from Windows Update directory" of "6.2.5.2 Obtain Security Patches Manually" to acquire security patches from Microsoft company manually and register to CS.

Processing to manual acquisition failure of security patches

If the manual acquisition fails, refer to relevant contents of "Security patches acquired from registration and passing of CD-ROM and other" of "6.2.5.2 Obtain Security Patches Manually" and register the security patches to CS.

6.4.3 Confirmation of Installation of Security Patches

It can be confirmed from the main menu if the security patches have been installed to CT.

In addition, installation state of the security patches can be confirmed via email when setting the warning notice. Refer to relevant contents of "2.5 Set Alarm Notification" for Settings of the warning notice.

Steps to confirm installation

Installation confirmation of the security patches is performed in **PC Information** in the main menu. In addition, the installation state can also be saved as CSV format file.

Whether installation of the security patches is finished normally or failed can be confirmed in the **Environment Setup** window in CT. For detailed information, refer to relevant contents of *Systemwalker Desktop Patrol Operation Guide: for Clients*.

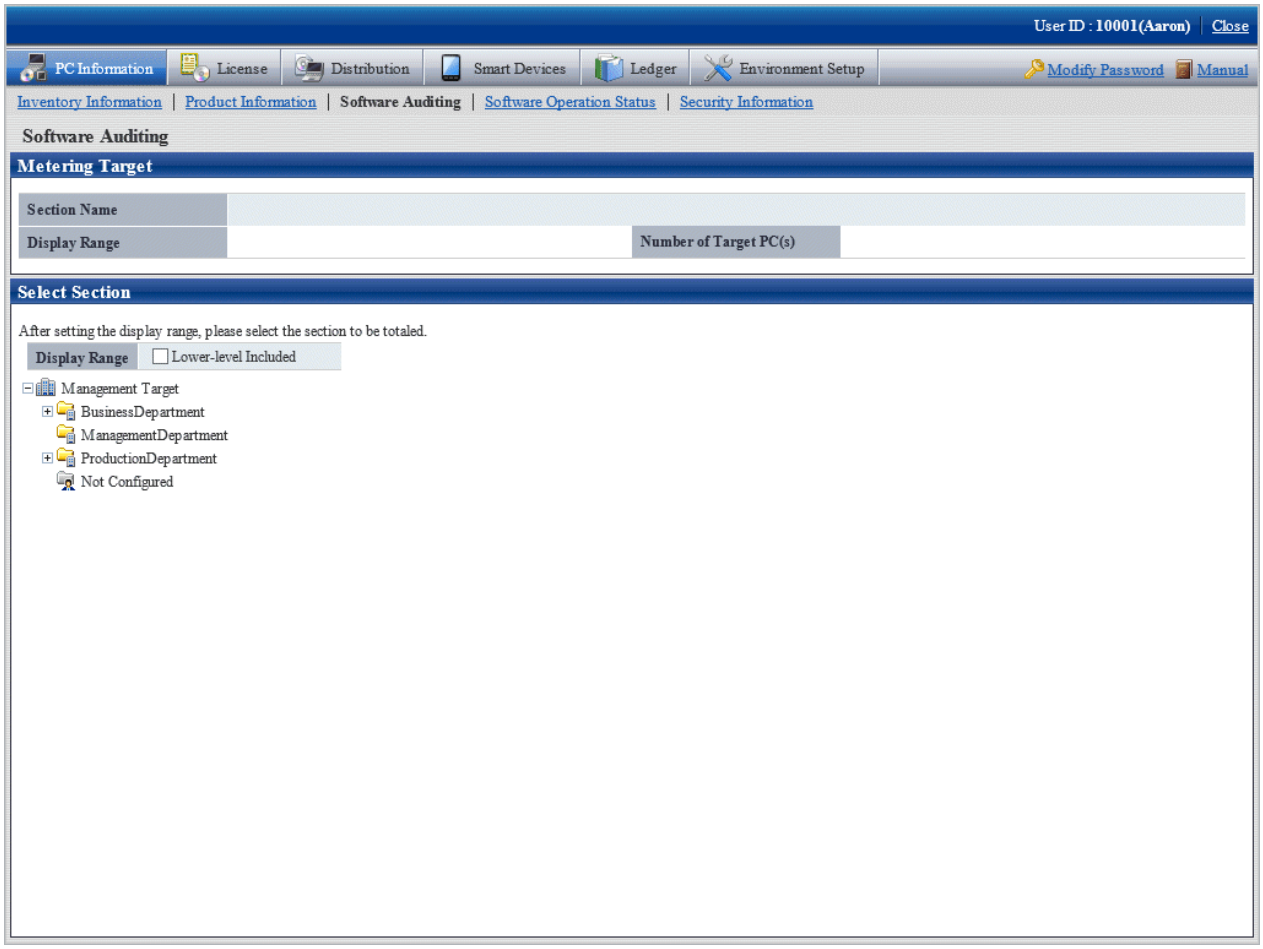
Take the following steps.

1. Log on the main menu, click **PC Information**.

   The **PC Information** window will be displayed.

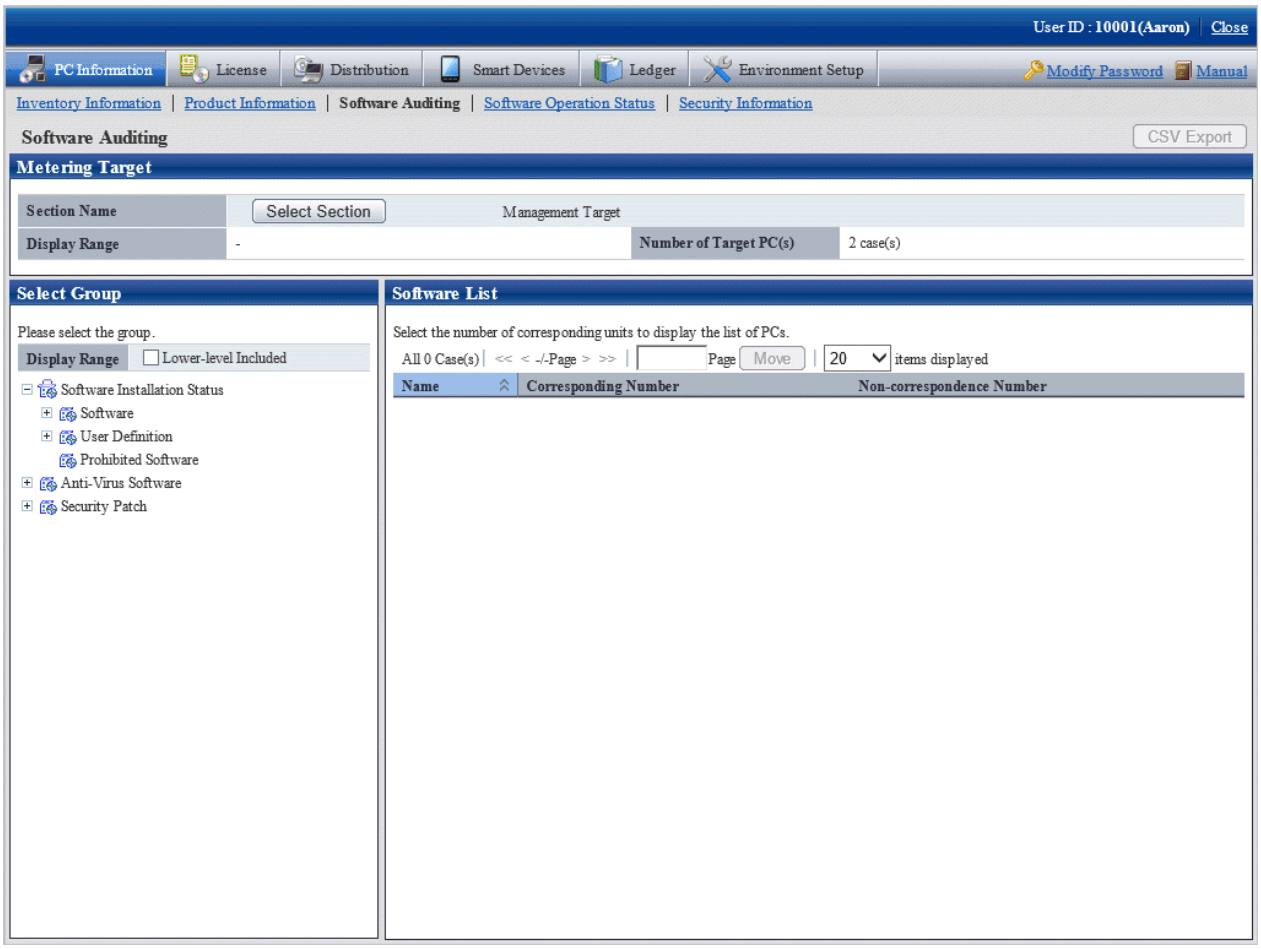
2. Click **Software Auditing**.

   The following window will be displayed.



3. Select the department to be displayed.

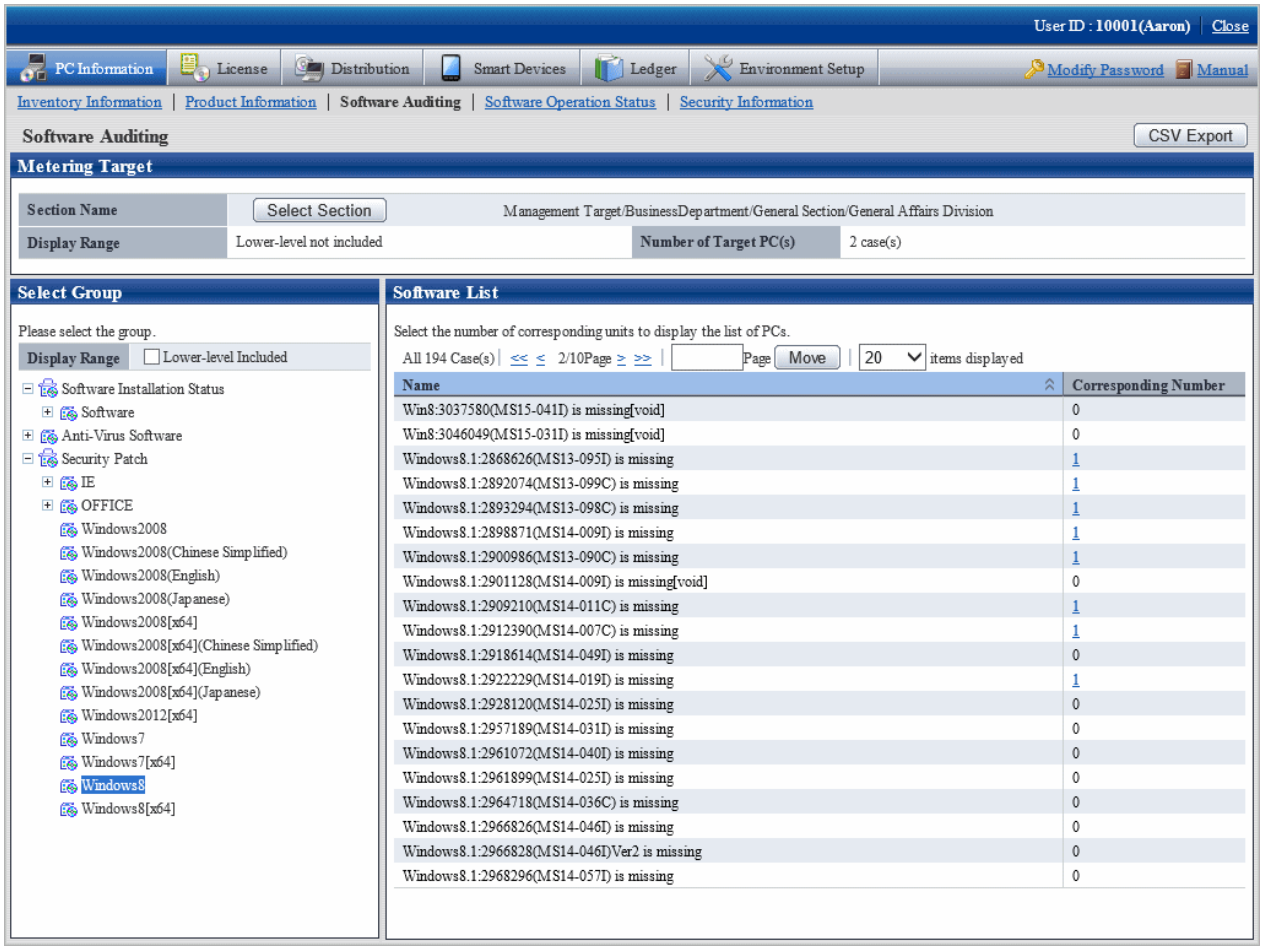
   The following window will be displayed.



4. Select product from **Security patch** in the tree on the left field.

   Security patches corresponding to the selected product will be displayed in the field on the right.

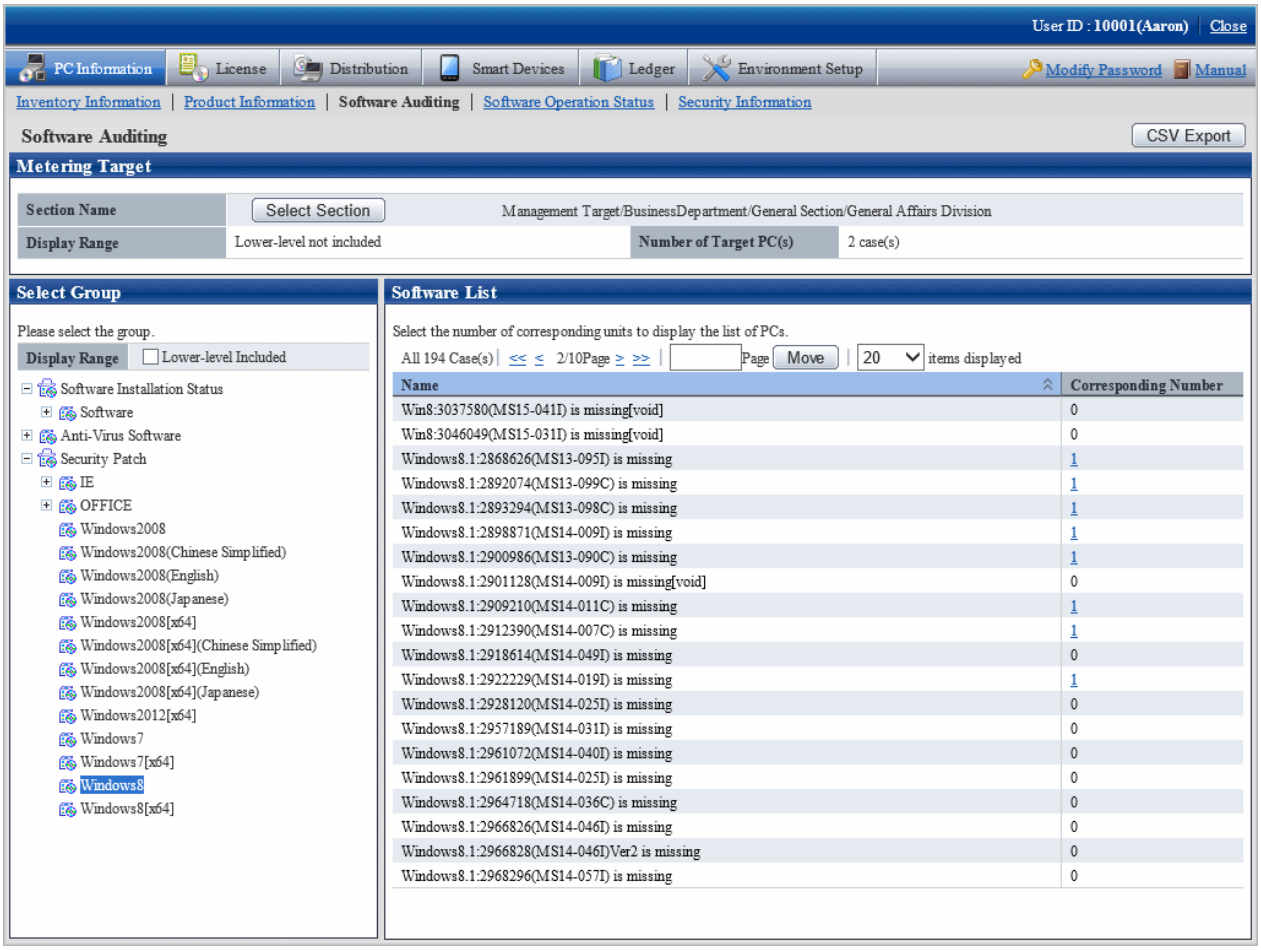
5. Confirm number of the qualified PC displayed in **Software List**.



6. Click **CSV Export** button to download installation state of the security patches as CSV format file.

Method to View the Window of Security Patches Installation State

This section explains how to view the **Installation state of security patches** window. For example, after **Windows8** is selected in window of **Installation state of security patches**, security patches information related to Windows 8 and number of qualified PC will be displayed.



Window of **Installation state of security patches** is composed of the following.

- Name of component (e.g. Windows8)
  - Name of component installed
    (e.g. Windows 8 is installed)
  - Name of component (no installation code) not installed
    (e.g. Windows8:2978668(MS14-047I) is missing)
  - Name of component not installed(invalid)
    (e.g. Windows8:2916036(MS14-005I) is missing[void])

    Security patches and service patches displayed as "void" need not be confirmed or counted.

    "void" of security patches and service patches indicates this security related problem has been solved through other security patches or service patches.

Take the following steps to identify the PC with and without installation of the security patches and service patches in the window of **Installation state of security patches**.

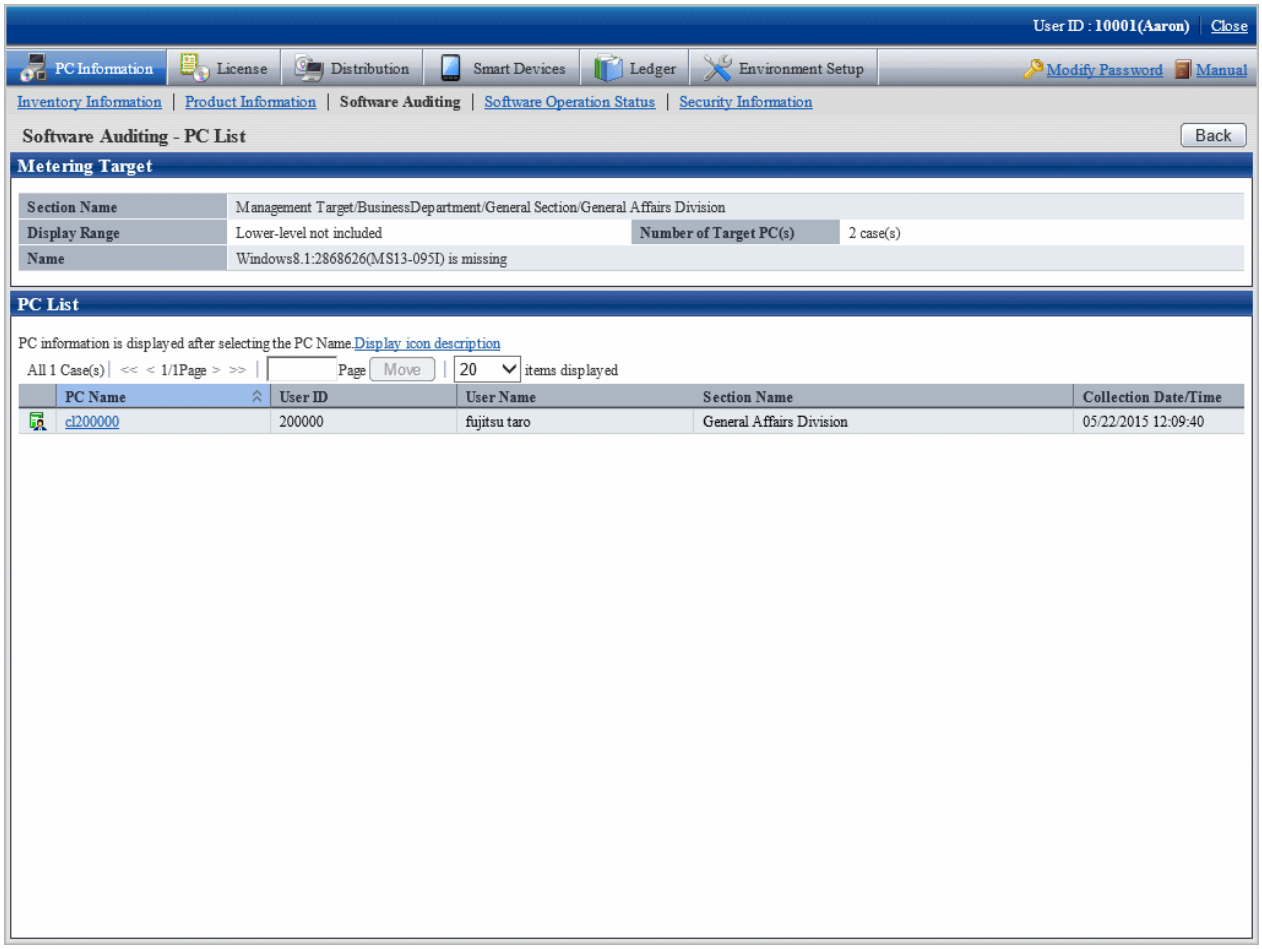
1. Find the items to have the state looked up in list of the security patches.

   When number of the qualified pieces is "0", no insufficient installation of security patches existing in the selected Component. End of the confirmation.

   When number of the qualified pieces is not "0", insufficient installation of security patches is existing in the selected Component. Enter the next step.

2. Click **Corresponding Number** of the security patches and service patches not displayed as "0".

   State of PC desired to be understood shows in the selected security patches and service patches.



When Security Patches Not in Installation are Detected

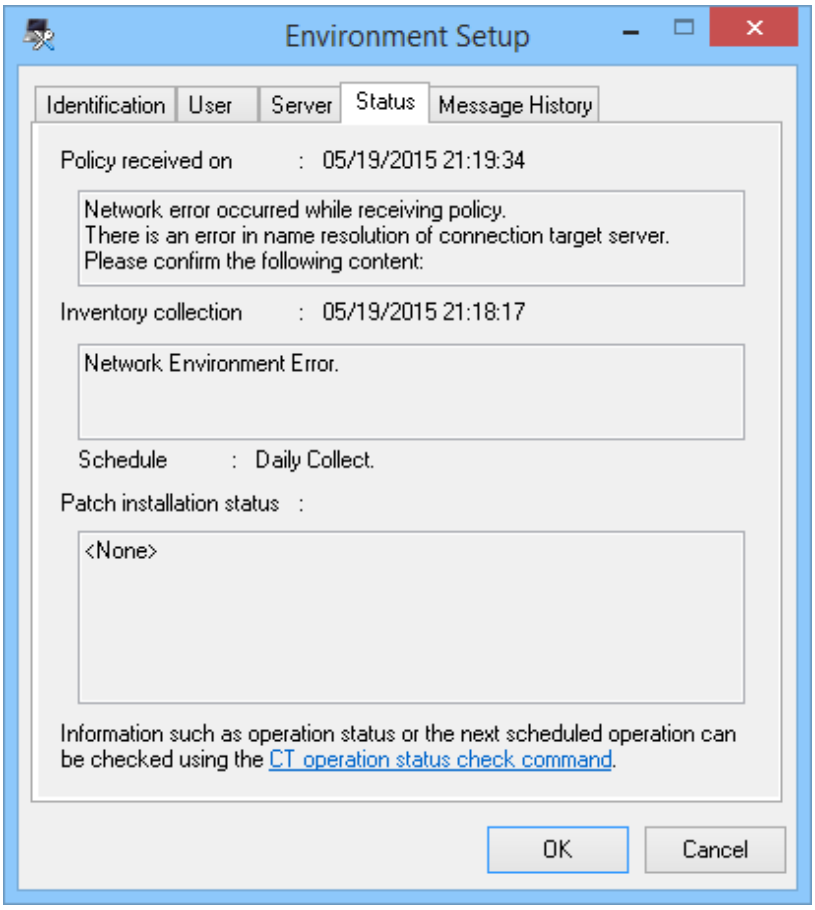
Security patches won't be installed in the following circumstances.

- Power not turned on for CT to install the security patches
- CT to install the security patches not connected to network

Solve the above problems to install the security patches.

It could be that errors have happened in installation Processing of the security patches at the Client when the problems can't be solved. Confirm the CT operation status log and the **State** label in CT **Environment Setup** window and refer to "CT Message of Systemwalker Desktop Patrol" in *Systemwalker Desktop Patrol Reference Manual* for identification of the causes and to perform the corresponding Processing.

See below for an example of the **Environment Setup** window of CT.



Column of **Patch installation status**: relevant information will be displayed here in case of abnormal installation of the security patches.

Confirm with Status Checking Command of CT Operation

As to CT with no security patches installation, its status can be confirmed with the status checking command of CT operation. Refer to relevant contents in *Systemwalker Desktop Patrol Reference Manual* for more information.

Confirmation of Status Log of CT Operation

As to CT with no security patches installation, the status log of Ct operation can be confirmed. See below for method to confirm.

1. Take one of the following measures to identify the PC and its name with no security patches installation.
   a. Confirm name of the PC with no security patches installation in window of **PC Information** > **Software Auditing** in the main menu.
   b. Select **Software supervision** in window of **Event Settings** and set it as name of the passed PC with no security patches installation.
   The administrator can be regularly noticed of name list of the PC with no security patches installation through event settings.
   Refer to relevant contents of "2.5 Set Alarm Notification" for window of event settings.
2. Search the PC name information from the CT operation status log saved on CS to confirm if the security patches have been installed.
3. As to check and retrieval of the CT operation status log, use Microsoft(R) Excel or editor to confirm.
4. Saving of the CT operation status log will default to the following directory.

CS installation directory \FJSVsbinv\ct_trace\ User ID+PC name + superior server name \dpsysdYYYYMMDD.log

Remarks.

Storage path and days of management of the CT operation status log file can be modified with the command of SVPolicy.exe (Server Environment Setup).

Refer to relevant contents in *Systemwalker Desktop Patrol Reference Manual* for detailed information about the file of CT operation status log.

See below for examples of the CT operation status log detected to be without security patches installation.

- Example 1: Failure of security patches installation

```
user1,pc1,server1, 2008/06/12 20:15:05.717,INFO,POLICY,RECEIVE,OK
user1,pc1,server1, 2008/06/12 20:15:05.818,INFO,POLICY,UPDATE,OK
user1,pc1,server1, 2008/06/12 20:15:06.612,INFO,PATCH,START,,1
user1,pc1,server1, 2008/06/12 20:16:10.123,INFO,PATCH,DOWNLOAD,OK,

"install MS04-012(828741) to Windows2000 "
user1,pc1,server1, 2008/06/12 20:16:12.814,INFO,PATCH,INSTALL,OK,

"install MS04-012(828741) to Windows2000"
user1,pc1,server1, 2008/06/12 20:16:14.035,ERROR,PATCH,STATUS,Failed(1603),

"install MS04-012(828741) to Windows2000 "
```

Pay attentions to the lines in red. Detection result of installation status shall be no installation by judgment as abnormality has happened to installation Processing of the security patches.

- Example 2: Failure of policy receiving, causing unavailability of security patches for installation

```
user1,pc1,server1, 2008/06/12 08:53:10.750,INFO,DTP,SVCSTART,
user1,pc1,server1, 2008/06/12 08:53:11.031,INFO,WINDOWS,ACLINEMODE,
user1,pc1,server1, 2008/06/12 09:01:46.953,ERROR,POLICY,RECEIVE,Failed(10060)
```

Pay attention to the line in red. Due to failure to receive policy, the security patches can't be installed to CT, detection result of installation state shall be no installation judging by this.

Example 3: the security patches are installed, but after installation there is no restart

```
user1,pc1,server1, 2008/06/12 20:15:56.612,INFO,PATCH,START,,2
user1,pc1,server1, 2008/06/12 20:15:59.112,INFO,PATCH,DOWNLOAD,OK," install
MS04-011 (835732) to Windows2000"
user1,pc1,server1, 2008/06/12 20:16:10.123,INFO,PATCH,DOWNLOAD,OK,"install
MS04-012(828741) to Windows2000"
user1,pc1,server1, 2008/06/12 20:16:21.917,INFO,PATCH,INSTALL,OK," install MS04-011
(835732) to Windows2000"
user1,pc1,server1, 2008/06/12 20:16:45.345,INFO,PATCH,STATUS,OK(0)," install MS04-011
(835732) to Windows2000"
user1,pc1,server1, 2008/06/12 20:17:11.320,INFO,PATCH,INSTALL,OK," install
MS04-012(828741) to Windows2000"
user1,pc1,server1, 2008/06/12 20:17:48.165,INFO,PATCH,STATUS,OK(0)," install
MS04-012(828741) to Windows2000"
user1,pc1,server1, 2008/06/12 20:19:36.044,INFO,REBOOT,SELECT,,Delete
```

Pay attention to the line in red. The security patches have been installed normally, but after installation, due to lack of restart of Windows, the security patches can't be reflected in Windows, detection result of installation state shall be no installation judging by this.

After restart of Windows, the following contents will be output to the status log of CT operation.

```
user1,pc1,server1,2008/06/12 20:23:15.859,INFO,REBOOT,SELECT,,Now
user1,pc1,server1,2008/06/12 20:23:19.001,INFO,DTP,SVCSTOP,
user1,pc1,server1,2008/06/12 20:23:52.640,INFO,DTP,SVCSTART,
```

- Example 4: No abnormalities are recorded in the status log of CT operation.

  That no abnormalities are recorded in the status log of CT operation means that CT has no problems. Confirm in window of **Environment Setup** > **CS/DS Settings and Status** in the main menu to see if CS and DS are running normally.

Confirmation of unapplied patches information

Patches not automatically installed to PC can be confirmed in the list.

Refer to relevant contents in "3.2.1 View Inventory Information" for confirmation of unapplied patches information with the patches list.

6.4.4 Processing to Installation Failure

This section explains how to treat the failure to install the security patches to CT. In addition, see below for installations of the security patches.

- Automatic installation of security patches
- Manual installation of security patches

Processing to automatic installation failure of security patches

Take one of the following measures to install the security patches manually if the automatic installation fails. Installation of the security patches doesn't require the system limits of authority. Therefore, log on Windows with limits of authority an ordinary user can also install the security patches.

- In CT, click **Start** or **Apps** > **Patch Application** to install the patches manually.
- Install the security patches manually from the software download window in CT.

Processing to manual installation failure of security patches

The following are possible causes of failure to install the security patches manually.

- Using the Client of CT, no installation of the security patches from the software download window.
- Errors have occurred during software download, making it impossible to install the security patches.

In the first instance, install the security patches from the software download window on the Client.

In the second instance, finish the processing corresponding to the error message displayed, then download the software again. Refer to relevant contents of *Systemwalker Desktop Patrol Reference Manual* for the corresponding processing to the error message displayed.

6.5 Type of Use

The following explains usage mode and key points of setup about installation of the security patches.

- Usage mode of security patches installation after logon
- Usage mode of regular confirmation and installation of security patches
- Usage mode of installation at night of security patches

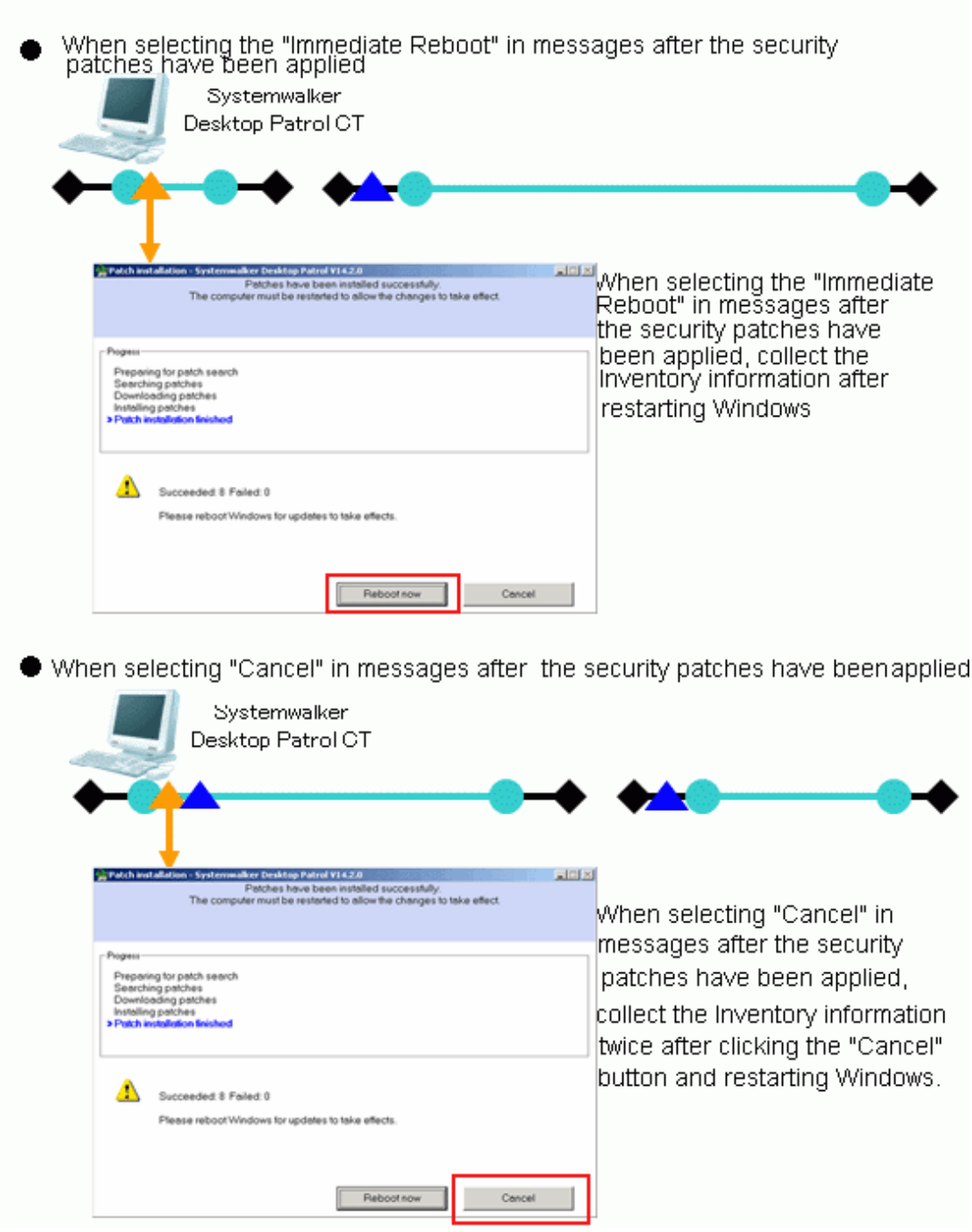
6.5.1 Operation of General Applicability and Key Points of Setup

This section explains the general applicability in usage mode and key points of setup.

Time point of inventory collection after installation of security patches

Inventory information will be collected after installation of the security patches. See below for time points to collect the Inventory information.

In addition, refer to "3.2.10 Timing of Collecting PC Information" for time points to collect the Inventory information outside of installation of the security patches.



Symbol	Symbol meaning
	Startup and shutdown of Windows. ◆— is to startup Windows, —◆ is to shutdown Windows.

	Windows is to logon and log off. is to log on Windows, is to log off Windows.
	Installation of security patches.
	Collect Inventory information after installation of the security patches. Collection of Inventory information will begin after restart of Windows if installation of the security patches requires restart of Windows.

Point

If you do not reboot Windows immediately after the patches are applied, a window prompting you to restart Windows will be displayed the next time you apply patches.

To display a button for canceling Windows reboot in this window, set the following client policy:

Click **Basic Operation Policy** > **Patch Application**, and under **Detailed Settings of Security**, set **Restart the PC automatically without displaying the message after patch installation** to **No**.

Key point of security patches installation or ordinary user PC and server PC

This section explains the usage mode and key points of setup when the security patches are installed to ordinary user's PC and server PC.

- PC of ordinary user

  After log on, set usage mode of security patches installation according to the user's intention.

  - Usage mode of security patches installation after log on
  - Usage mode of regular confirmation and installation of security patches

- Server PC

  Usage mode of installation of security patches at night to avoid impact on business.

  - Usage mode of security patches installation at night

To set up as per the above usage modes, select policy group use or one of the policy setups by DS unit to build the system.

Note

When the security patches are installed to CT automatically, do not select the check box of **Keep the computer constantly up to date** in the setting of automatic update in Windows on the target CT.

Note

Select the option of **Password protection** of the screen savers, under the circumstance of the running screen saver and the user's optional lockup window (press "Windows" key + "L" and etc), after installation of the security patches there won't be restart again.

In addition, when there is no start to update again, even there are still security patches not in installation, the remaining security patches at the position of restart won't be installed.

Pay attention to the following correspondence when installing the security patches.

- Keep Windows in state of log off when the security patches are installed at night.
- Do not select the check box of **Start Countdown, restart when no answer**. After Settings of installation of the security patches the message will be displayed, and restart will begin after selection of the button.

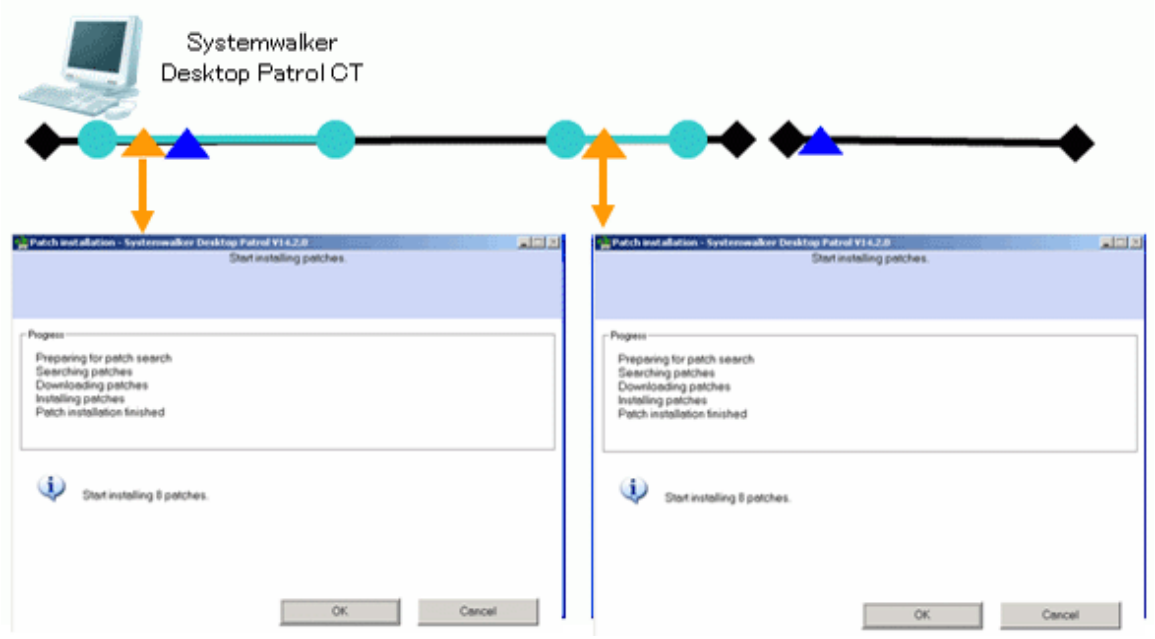
6.5.2 Usage Mode of Security Patches Installation After Logon

CS automatically acquires the security patches made public by Microsoft company, the security patches installation begins after log on CT and message display. Whether the security patches will be installed will be decided by the user's intention.

Installation of the security patches only processed in time of log on. In addition, the message will be displayed in CT window in case of installation failure of security patches.

Use chart

See below for use chart of security patches installation upon log on.



Symbol	Symbol meaning
	Windows startup and shutdown. ◆— is to startup Windows, —◆ is to shutdown Windows.
	Log on and log off Windows. ●— is to log on Windows, —● is to log off Windows.
	Installation of security patches.
	Collect Inventory information after installation of security patches is done. If installation of the security patches requires restart of Windows, collect Inventory information after restart of Windows.

In the usage mode of security patches installation upon log no, confirm if there are any security patches to be installed to CT as needed at the time point of log on Windows.

- Installation of security patches needed

  The following installation confirmation window will be displayed. Select **Cancel** button, the installation confirmation window will be displayed again of the next log on Windows.

  Window to confirm installation, will be displayed for many times when it reaches the installation position.

- Installation of security patches not needed

  No display of installation confirmation window.

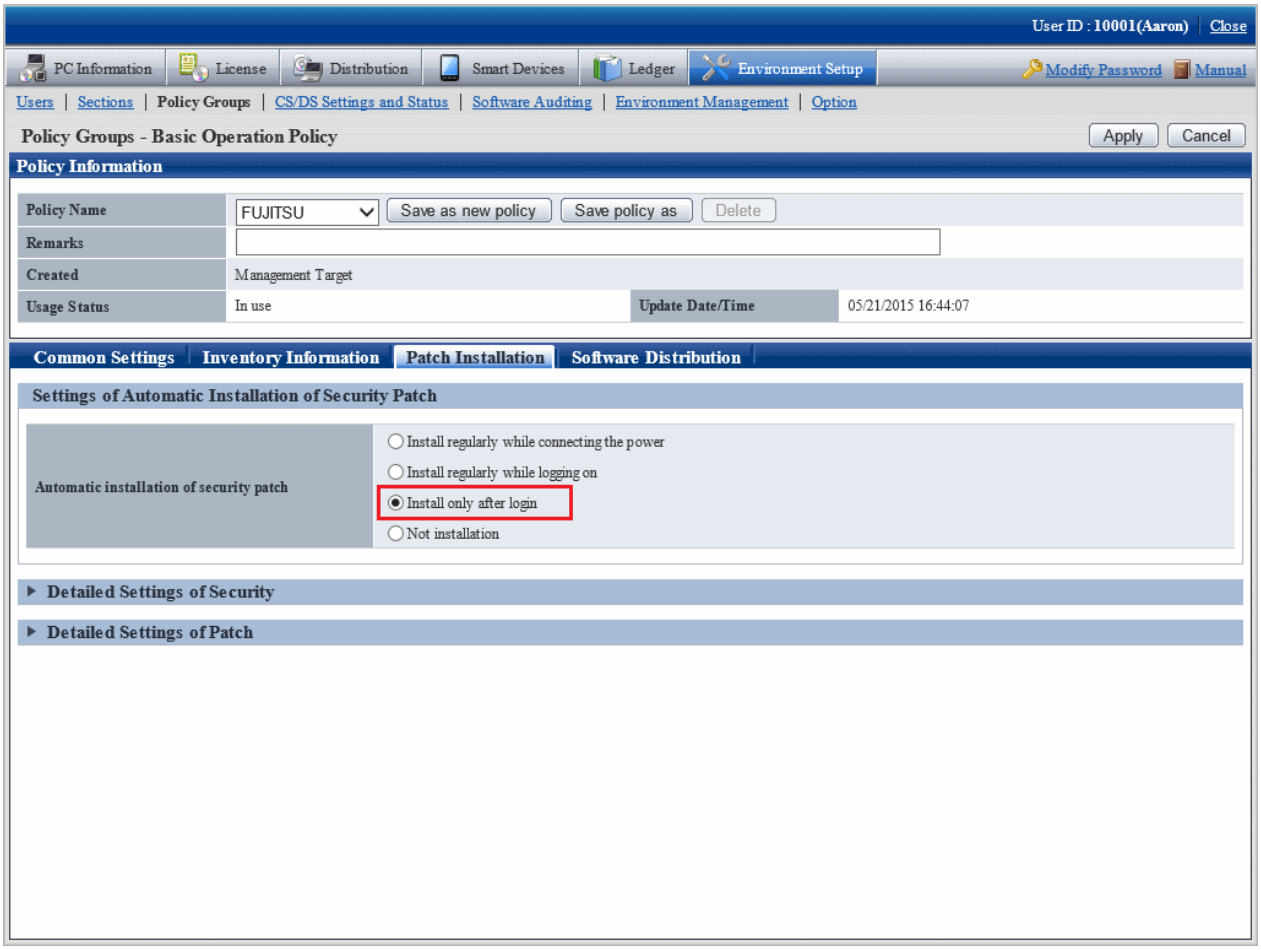
Point of setup

To realize the usage mode of security patches installation upon log on, it is necessary to set up the Client in **Environment Setup** in the main menu.

In addition, refer to "6.2 Setup" for the setup needed for installation of the security patches. This section herein explains the key points, i.e. how to set up at the Client.

Setup at client

See below for Settings of tab of **Patch Installation** in **Basic Operation Policy** in **Customize Various Policies** in **Policy Groups** in **Environment Setup**.



Mandatory items in setup are shown as below.

Setup item	Set value	Mandatory/Optional
Automatic installation of security patch	Install only after login	Mandatory

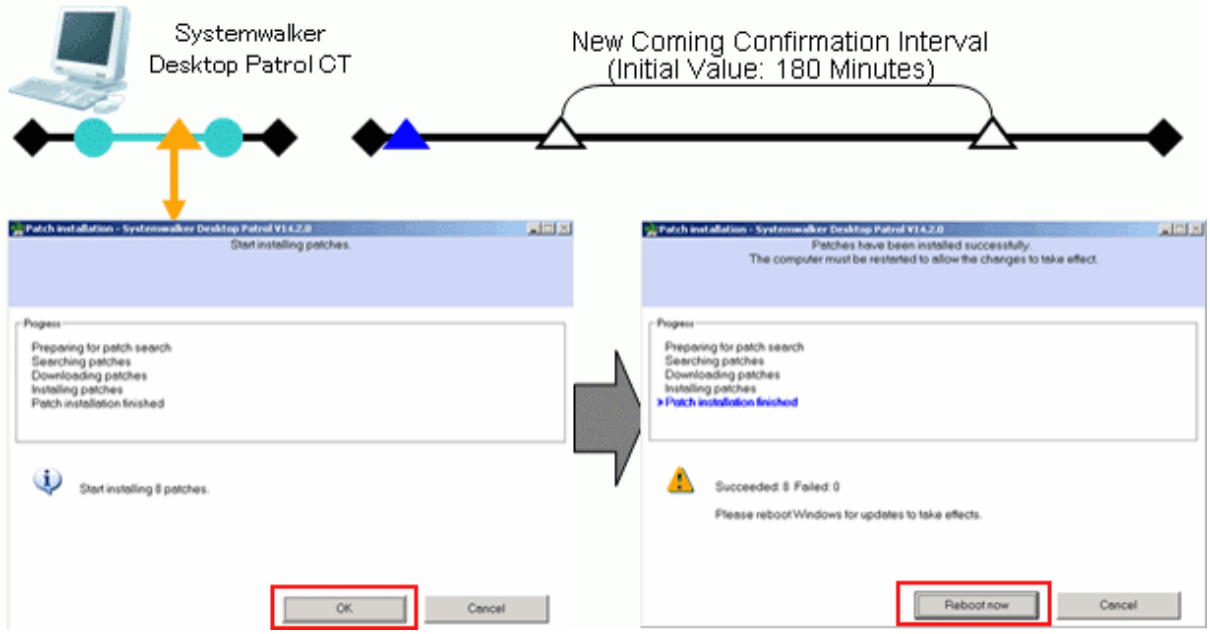
6.5.3 Usage mode of Regular Confirmation and Installation of Security Patches (Use as Per Original Setup)

CS automatically acquires the security patches made public by Microsoft company. The security patches will be regularly confirmed on CT, when there are security patches to be installed, installation of the security patches will begin after the confirmation message is displayed. Whether it is necessary to install the security patches will be decided by the user's intention.

In addition, in this usage mode, the user can install the security patches without having to log on Windows. At this time, message of installation confirmation won't be displayed.

Use chart

See below for use chart of the security patches of regular confirmation and installation.



Symbol	Symbol meaning
	Windows startup and shutdown. ◆— is to startup Windows, —◆ is to shutdown Windows.
	Log on and log off Windows. ●— is to log on Windows, —● is to log off Windows.
	Installation of security patches.
	Collection Inventory information after installation of security patches is done. When installation of the security patches requires restart of Windows, collect Inventory information after restart of Windows.

In the usage mode of security patches of regular confirmation and installation, whether there are security patches needed to be installed to CT will be confirmed as per the interval(original value: 180 minutes) of the confirmation policy.

- Installation of security patches needed

  The installation confirmation window will be displayed. Select **Cancel** button, the installation confirmation window will be displayed again at the time of the next confirmation.

  The installation confirmation window will be displayed all the time till installation of the security patches.

In addition, in the window displayed after installation of the security patches, if restart is not performed and the **Cancel** button is selected, the window requiring restart will be displayed again at the time of the next confirmation interval.

The window requiring restart will be displayed all the time till restart is done.

- Installation of security patches not needed

  No display of installation confirmation window.

Note

When you configure the following settings, a window prompting reboot will be displayed at the next patch confirmation interval.

- Setting items

  Display message when the security patch installation file exists: **Yes**

  Display message after the patch installation: **No**

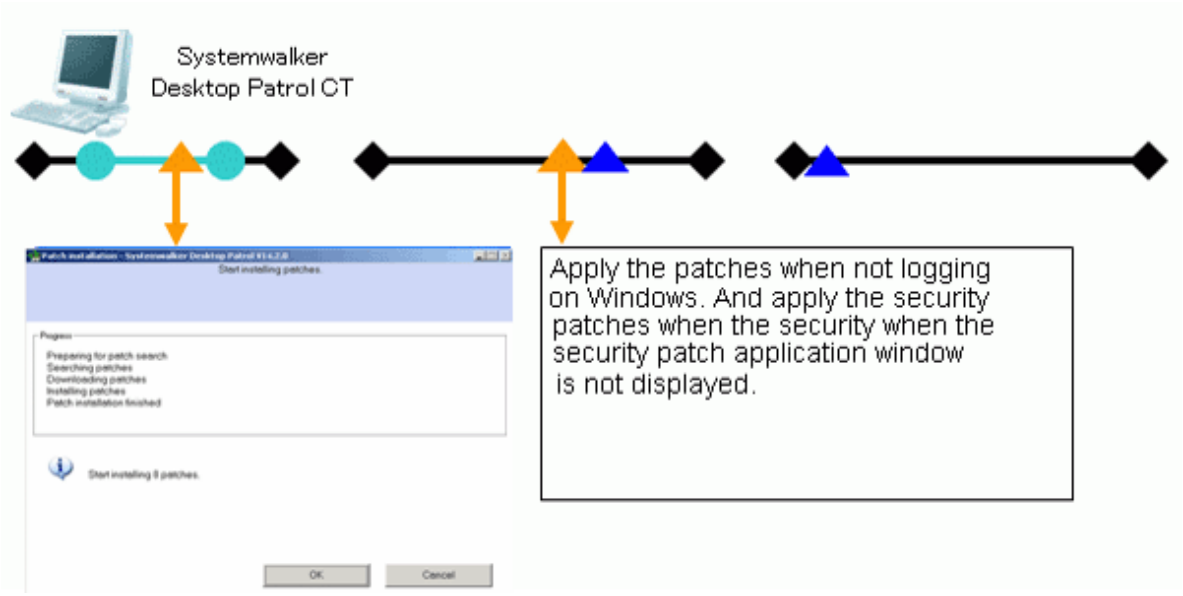
  Restart the PC automatically without displaying the message after patch installation: **No**

In the original setup, installation of the security patches will process upon log on of Windows.

Through the following setup change, the user can install the security patches even without log on Windows.

- Select **Install regularly while connecting the power**

Use chart of security patches installation without log on Windows is show as below.



Symbol	Symbol meaning
	Windows startup and shutdown. is to startup Windows, is to shutdown Windows.
	Log on and log off Windows. is to log on Windows, is to log off Windows.
	Installation of security patches.
	Collect Inventory information after installation of security patches is done.

Symbol	Symbol meaning
	If installation of the security patches requires restart of Windows, collect Inventory information after restart of Windows.

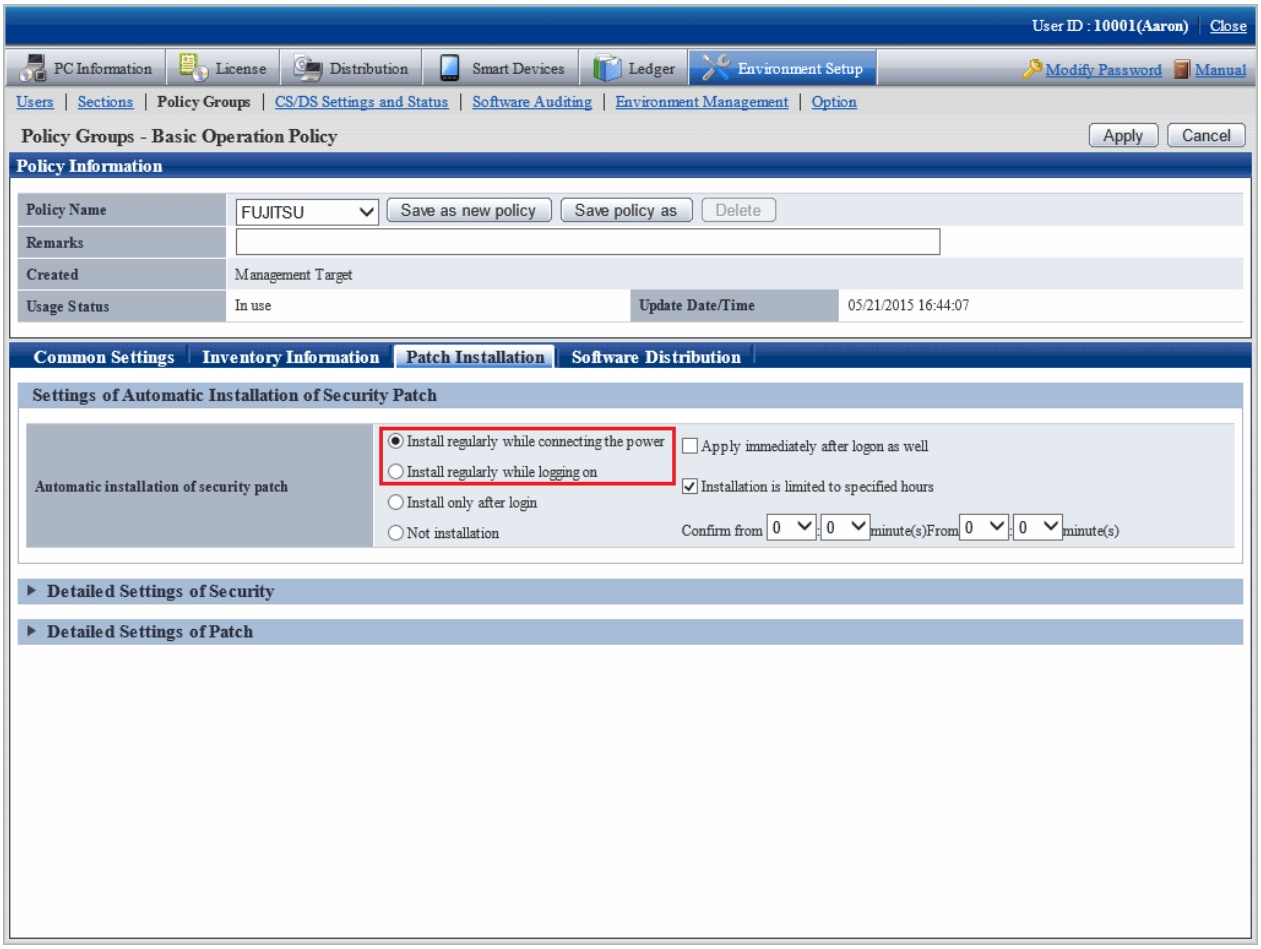
Point of setup

No need for setup when using as per the original setup.

In addition, refer to "6.2 Setup" for the setup needed for installation of the security patches. It explains herein the key points of set up at the Client.

Setup at client

See below for Settings of tab of **Patch Installation** in **Basic Operation Policy** in **Customize Various Policies** in **Policy Groups** in **Environment Setup**.



See below for the necessary setup items. The optional items will be set up as needed.

Setup item	Set value	Mandatory/optional
Automatic installation of security patch	Select one of the following setups. - Install regularly while connecting the power - Install regularly while logging on	Mandatory

6.5.4 Operation of Security Patches Installation at Night

In the operation of security patches installation at night, the security patches made public by Microsoft company will be acquired and installed to CT at night, therefore there is no impact on the business in the day.

It is necessary to turn on the CT power for installation of the security patches. When the power is turned off, it won't be possible to install the security patches.

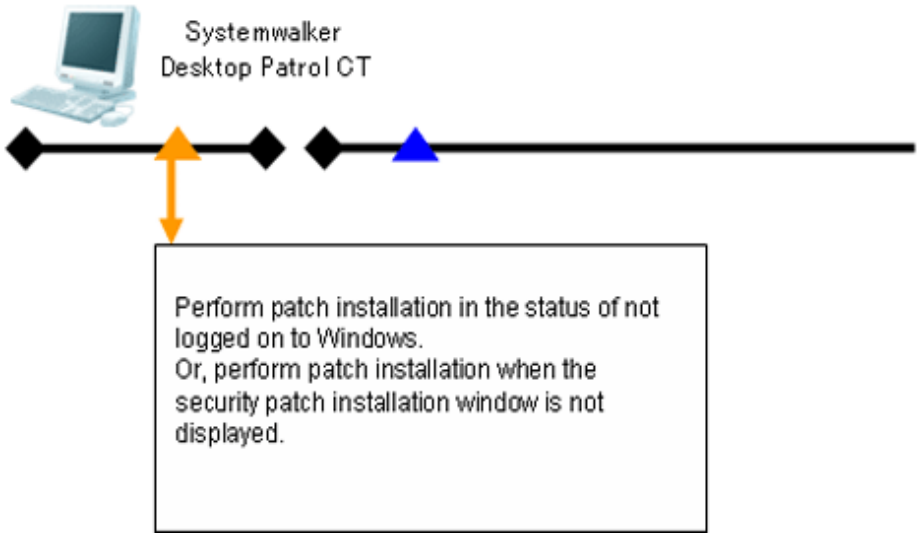
Perform the following corresponding actions.

- Do not turn off the power supply after the business is finished.
- Use the Wakeup On LAN function(Note) to turn on PC power.

  Note) Wakeup On LAN function needs support from the PC itself. Refer to the PC's operation instructions for support status of the PC itself.

Operation image

See below for use chart of installation of the security patches at night.



Symbol	Symbol meaning
	Windows startup and shutdown. ◆— is to startup Windows, —◆ is to shutdown Windows.
	Installation of security patches.
	Collect Inventory information after installation of security patches is done. If installation of the security patches requires restart of Windows, collect Inventory information after restart of Windows.

In the usage mode of security patches installation at night, whether there are security patches needed to be installed to CT will be confirmed as per the interval(original value: 180 minutes) of the confirmation policy.

- Installation of security patches at night needed

  Installation of the security patches begins directly without display of installation confirmation window. In addition, installation of the security patches requires restart, which will proceed automatically.

- No installation of security patches needed

  No installation of security patches.

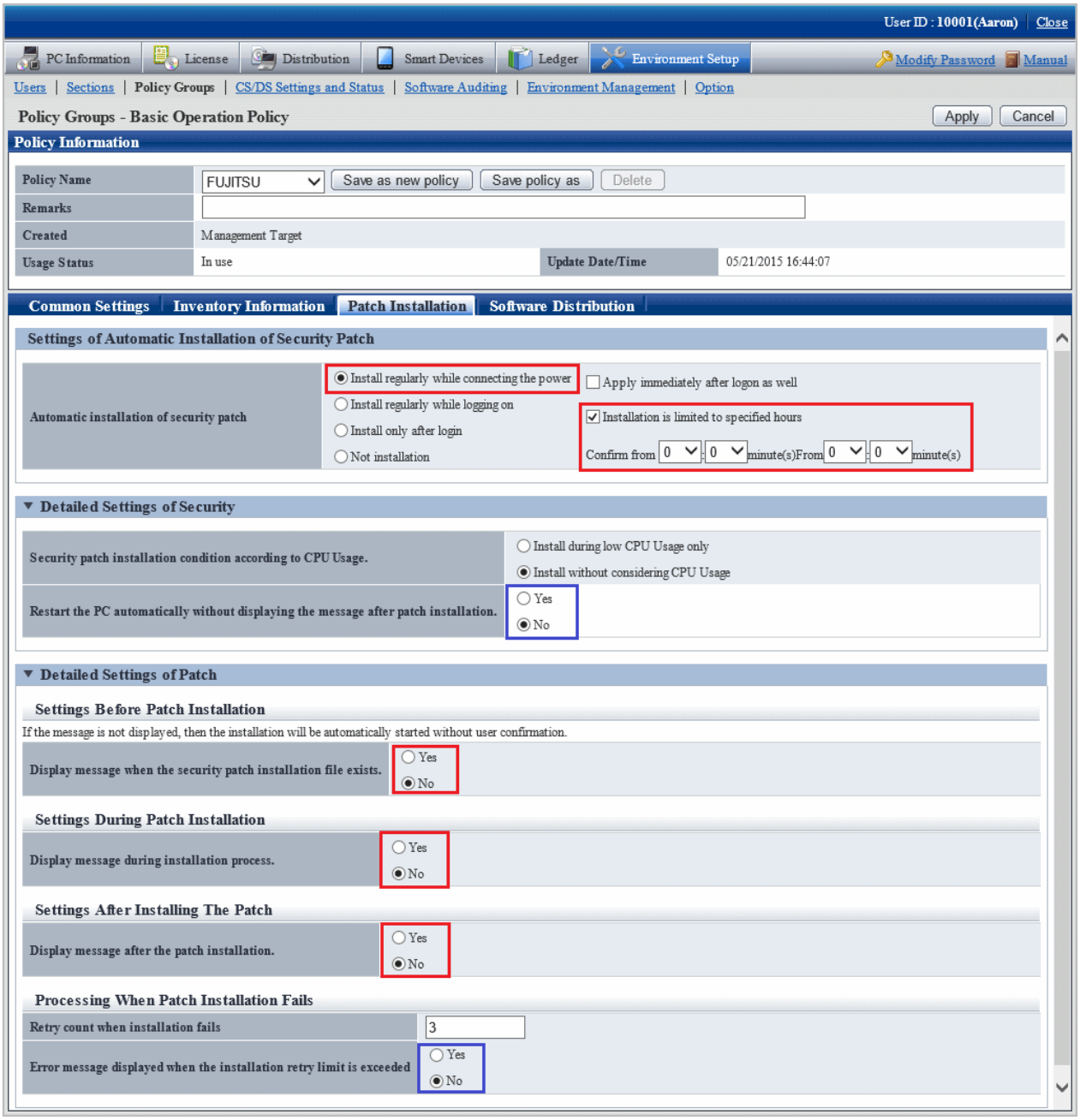
Point of setup

To realize installation of the security patches at night, it is necessary to finish the setup in **Environment Setup** in the main menu.

In addition, refer to "6.2 Setup" for the setup needed for installation of the security patches. It explains herein the key points of set up at the Client.

Setup at client

See below for Settings of tab of **Patch Installation** in **Basic Operation Policy** in **Customize Various Policies** in **Policy Groups** in **Environment Setup**.



Compulsory setup items are shown as below. Settings of an optional item should be performed according to usage needs.

Setup item	Set value	Mandatory/optional
Automatic installation of security patch	Install regularly while connecting the power	Mandatory
Installation is limited to specified time frame only	Selection	Mandatory
Restart the PC automatically without displaying the message after patch installation	Yes	Optional(Note)
Display message when the security patch installation file exists	No	Mandatory
Display message during installation process	No	Mandatory
Display message after the patch installation	No	Mandatory
Error message displayed when the installation retry limit is exceeded	No	Mandatory

Note) for the security patches require restart of OS, installation won't be completed without the restart, therefore, even though there are following security patches to be installed, the next security patch won't be installed.

Chapter 7 Distribute Files

This chapter describes how to distribute files to CT.

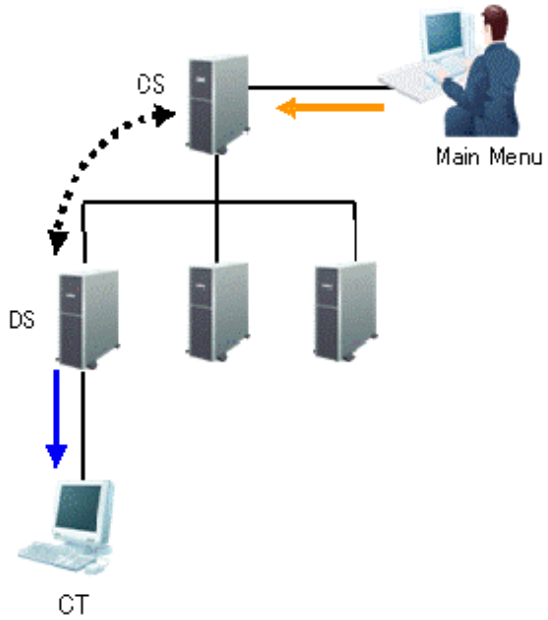
Note

Files can only be distributed to CT with agent mode V14.2.0 or later.

7.1 Operation Procedure

The file that is set to distribution can be distributed to CT automatically from the main menu.

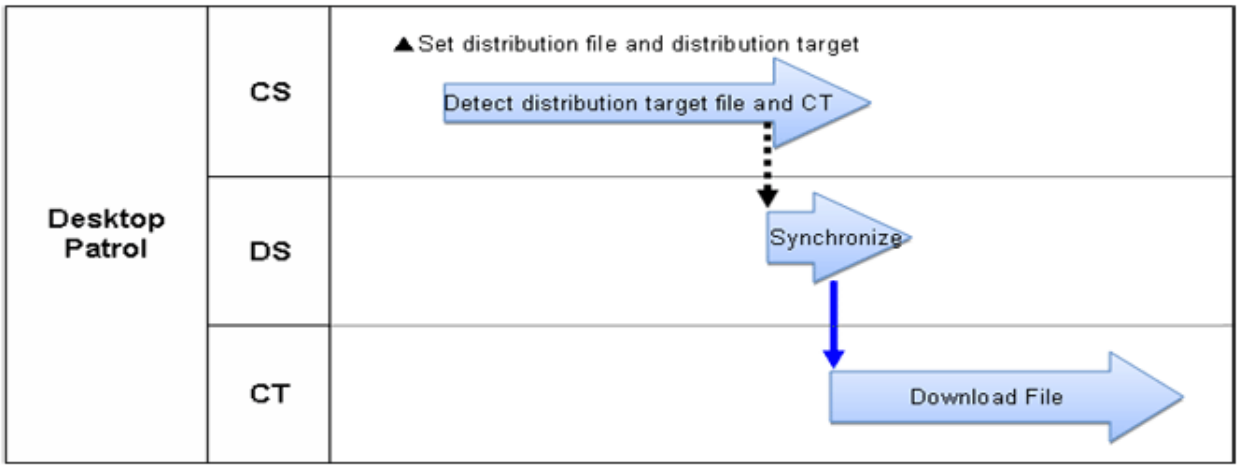
The data flow during file distribution is shown below.



The information required for file distribution and the timing when information is sent (initial value) are shown in the table below.

Type of Line	Operation	Timing of Operation
←	Set file and distribution target	Anytime Distribution settings from the main menu
◄····►	Synchronization of file distribution	Confirm every 5 minutes It is possible to set in **Environment Setup** > **CS/DS Settings and Status - DS Settings** window of the main menu
←	File download	Confirm every 10 minutes It is possible to set through the CustomPolicy.exe command

The time chart until the file has been distributed to CT is shown as follows.



Operation	Timing of Operation
Synchronization of file distribution	Confirm every 5 minutes It is possible to set in **Environment Setup** > **CS/DS Settings and Status** - **DS Settings** window of the main menu
File download	Confirm every 10 minutes It is possible to set through the CustomPolicy.exe command

The following describes the time chart.

Set the file to be distributed and the distribution target. For information on how to set distribution, refer to "7.2.1 Set Distributed File and PC to be distributed and Distribute".

The distribution operation does not require particular settings. Simply operate by following the setting at installation of product.

- Synchronization of file distribution

  To modify settings, refer to the item **Connection Interval with Higher CS/DS** and **Specify hour(s) of receiving distribution software** of "Select DS" of "8.2.1 Perform Settings of Server to Distribute Software".

- File download

Note

When the time frame is set in **Specify hour(s) of receiving distribution software**, the synchronization of CS and DS will be performed in specified time frame only. Therefore, file distribution to CT will be delayed.

7.2 Settings

Perform the setting of file distribution according to the following procedure.

1. Settings of file to be distributed

2. Settings of distribution target

7.2.1 Set Distributed File and PC to be distributed and Distribute

Set the file to distribution file. The file that has been set as the distribution file can be distributed to CT.

Note

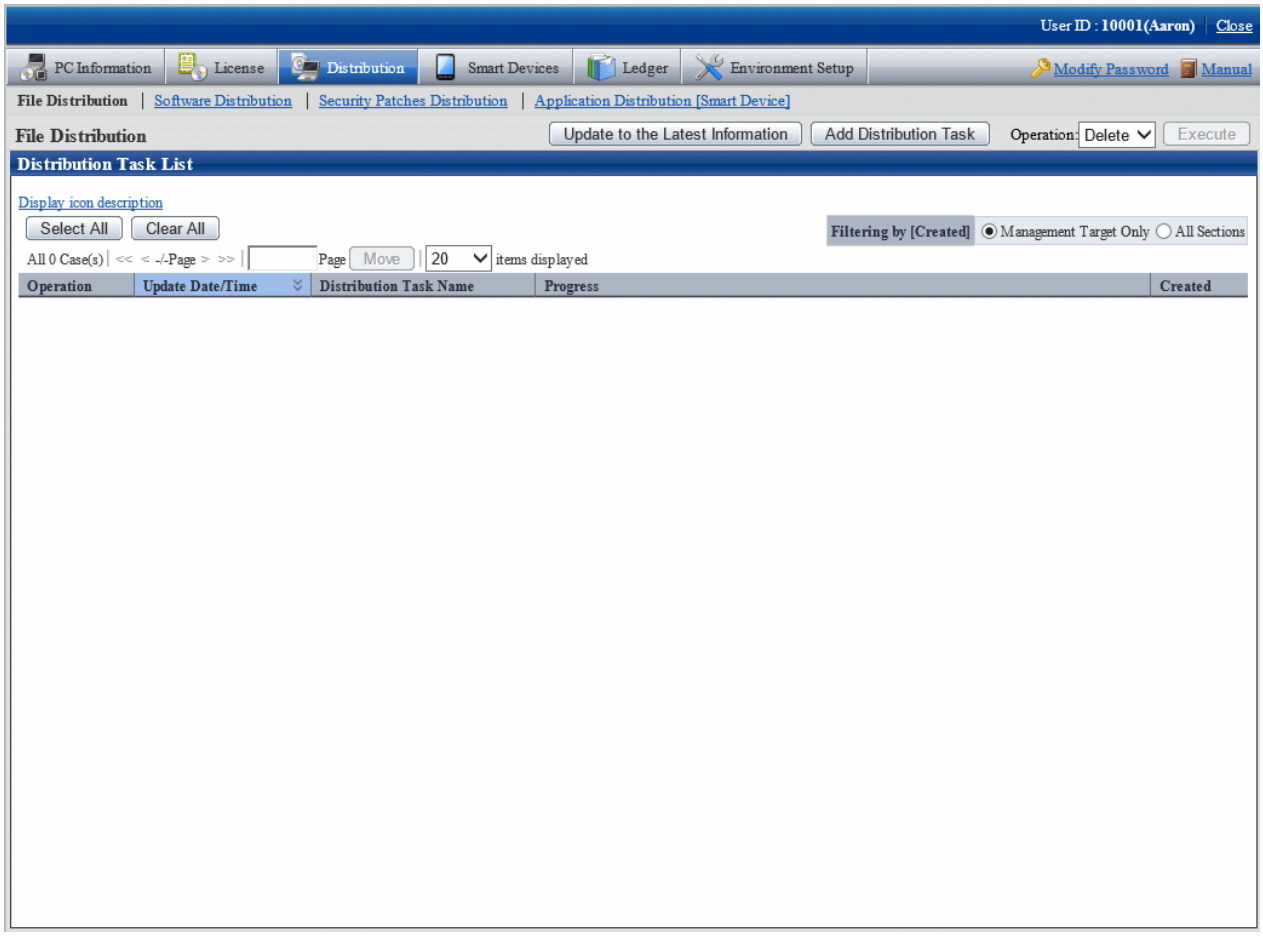
The files registered in the **File Distribution** function will not be displayed in the software download window of CT. Start, stop, re-distribution and result confirmation are performed in the main menu.

Set the file to be distributed.

The procedure is as follows.

1. Log in to the main menu, and click the **Distribution** button.

   The initial window of **File Distribution** will be displayed.



Description of button is shown below.

Button Name	Description
Update to the Latest Information	Update to the latest information.
Add Distribution Task	Add the task for distributing file.

Button Name	Description
Operation list/ **Execute**	Select the check box of distribution task list and this button will be enabled. For the distribution task selected in the check box, select the content expected to be executed from the operation list and click the **Execute** button. The processing of distribution task will be started. There are following options in the operation list. - **Delete** Delete the distribution task from CS. The task being distributed cannot be deleted. - **Start** Start distribution for the tasks for which the distribution is not started, has been stopped or ended abnormally. - **Stop** Stop the distribution for the task that is being distributed.

Description of the items in the **Distribution Task List** is as follows.

Item	Description
Operation (check box)	When processing such as deletion is required, select the distribution task to be operated.
Update Date/Time	Display the date and time when distribution tasks are registered and updated.
Distribution Task Name	Display the name corresponding to the distribution task. The details of distribution task can be viewed by clicking the distribution task name.
Progress	Display the progress of distribution task. The color of column chart shows the percentage of progress. - Green It shows the percentage of distribution completed normally. - Red It shows the percentage of failed distribution due to some reasons. - Gray It shows the percentage that is not distributed. The meaning of icons is described as follows. : Distributed normally. : Distribution has ended abnormally. : Distribution is not started yet. : Distributing. : Distribution is stopped. Beside the icon, the total number of "number of files x distribution target PC" will be displayed as "Number of items". The meanings are described as follows. - *n* items in total Display the number of items to be distributed. - *n* items are normal

Item	Description
	Display the number of items that has completed distribution normally. - *n* items are abnormal Display the number of items failed to be distributed due to some reasons. For failed content, click the distribution task name to check the detailed condition tab. - *n* items are being distributed Display the number of items being distributed. - *n* items are not distributed Display the number of items that are not distributed.
Created	Display the section to which the administrator who created the distribution task belongs. When it is created by system administrator, it is displayed as the fixed name of "Management target".
Filtering by [Created]	The content in the distribution task list can be narrowed down according to **Created**. The content displayed in the distribution task list will be different depending on the authority of user logging in to the main menu. - When the authority is system administrator - Management target only Only the distribution task of which the **Created** is "Management target" will be displayed. - All sections All distribution tasks will be displayed regardless of **Created**. - When the authority is section administrator - Affiliated section only Only the distribution task created by the section to which the login user belongs will be displayed. - All sections that can be viewed The distribution tasks created by the section to which the login user belongs and distribution tasks created by all the lower-level sections will be displayed.

Point

Maximum number of managed tasks

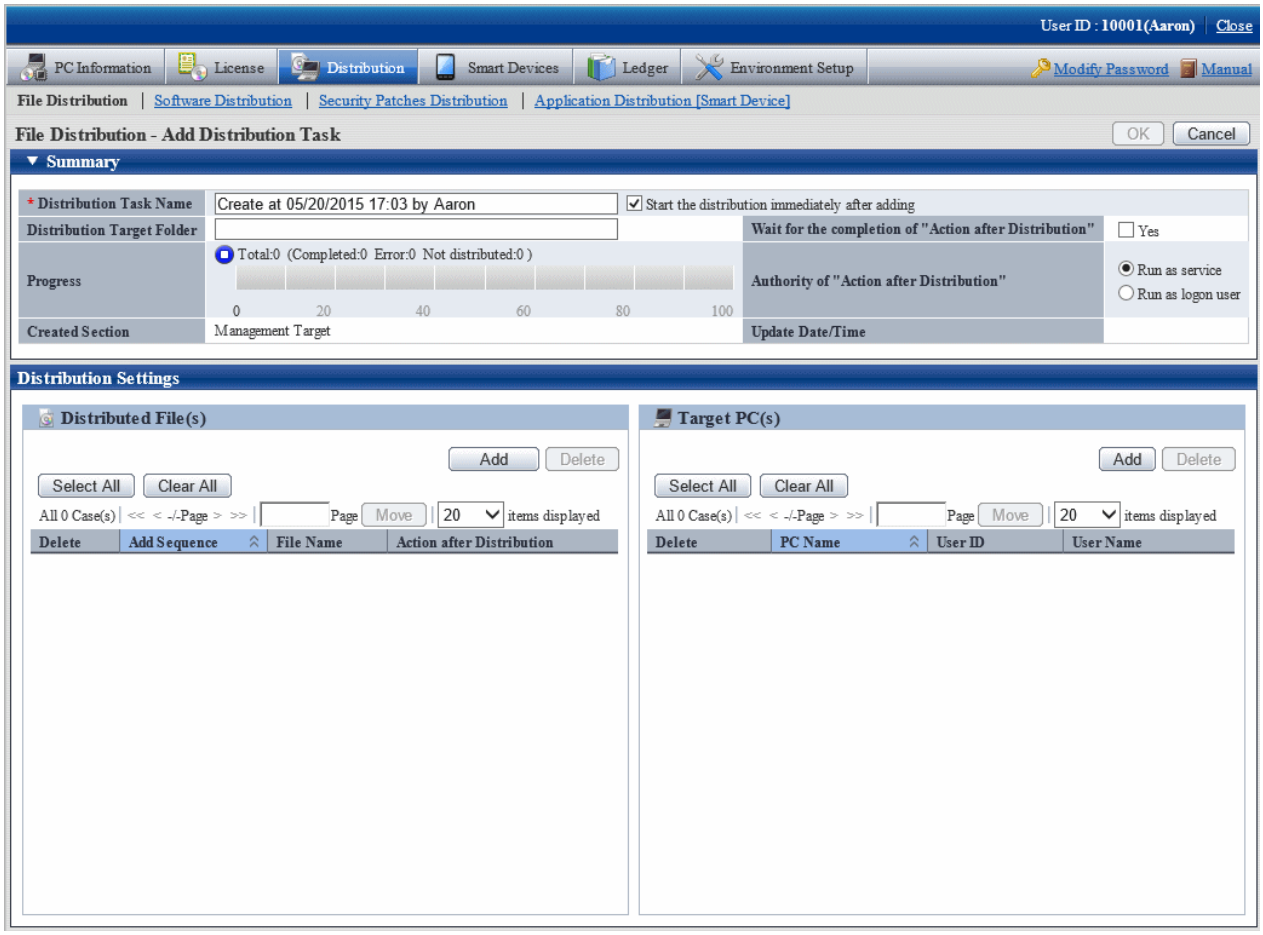
Maximum 100 tasks can be managed on the system.

Tasks cannot be deleted automatically, so delete the tasks that have been completed normally and are not needed in operation.

When the number of tasks on the system reaches 100, new distribution task will not be added even if the **Add Distribution Task** button is clicked.

2. Click the **Add Distribution Task** button.

   The window for selecting the file to be distributed and the distribution target PC will be displayed.

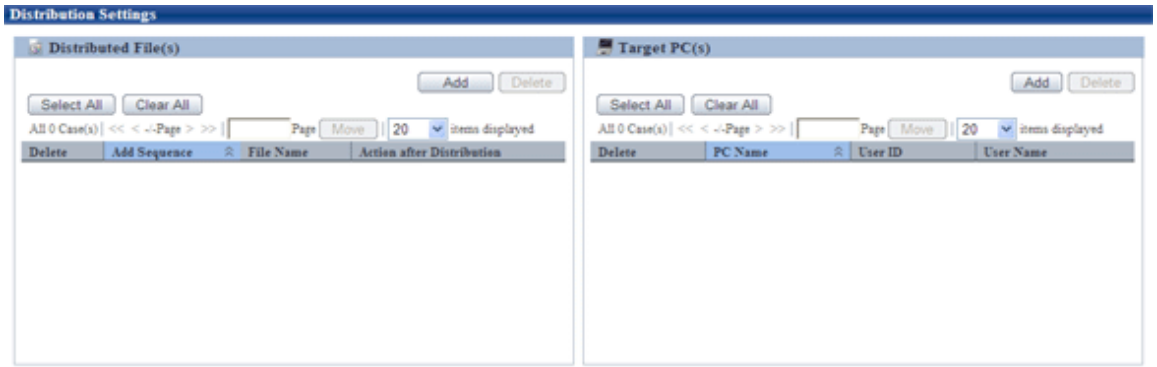


   The content of setting item is shown as follows.

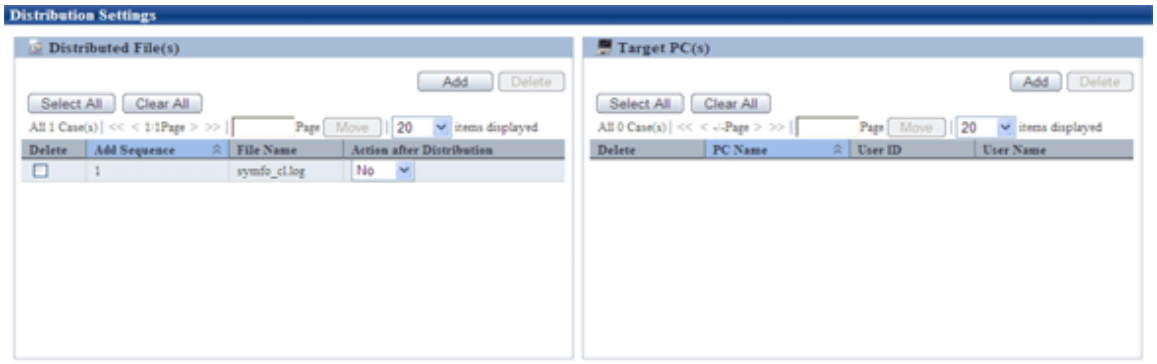
Item	Description
Distribution Task Name	Enter the name of task to be distributed within 30 multi-byte or 60 single-byte characters. It displays "Created on" and "Created User Name" in default. - **Start the distribution immediately after adding** After this item is selected and the **OK** button is clicked, distribution will be started immediately. When preparing for distribution, do not select this item and click the **OK** button.
Distribution Target Folder	Specify the folder name for saving distributed files on CT using up to 128 fullwidth characters or 256 halfwidth characters. When specifying with absolute path, specify an existing folder on CT. When it is unable to create a folder or a drive that does not exist has been specified, error will occur. When specifying a relative path or the distribution target folder is omitted, files will be saved under "CT installation directory\contents" on CT. In addition, system environment variables and macro can be used in distribution target folder. (User environment variables such as %HOMEDRIVE% .etc cannot be used.)

Item	Description
	- System environment variables The system environment variables that have been set can be used on CT. For example, specify to "%systemdrive%\xxxx". - Macro <ProgramFiles> It indicates the folder used by application. For example, "C:\Program Files". <ProgramFilesX86> It indicates the folder used by 32bit applications. Example in case of 64bit OS: "C:\Program Files (x86)". In addition, if the file to be distributed has already existed under the distribution target folder, it will be overwritten.
Progress	It is the same as the progress displayed in the initial window.
Created Section	Display the section to which the administrator that created the distribution task belongs.
Wait for the completion of "Action after Distribution"	Set the waiting for completion when executing the file specified in **Action after Distribution**. When processing the file specified in **Action after Distribution** after one file processing has completed, select **Yes**.
Authority of "Action after Distribution"	There are the following two methods to execute the file specified in **Action after Distribution**. - Run as service - Run as logon user
Update Date/Time	Display the date and times when distribution task is registered and updated.

3. In the **Distribution settings** tab in the bottom left field of the window, click the **Add** button of **Distributed file** and select the file to be distributed.



After a file is selected, it will be added to the list of files to be distributed.



In case of wrong registration, select the file that should be deleted from the list and click the **Delete** button.

Point

Number of files can be registered in a single task

In a single task, maximum 10 files can be registered.

When there are more than 10 files, compress it to zip file in advance or register separately.

Note

- The file/folder properties of registered file (read-only .etc) cannot be kept after distribution. When it is required to set file/folder properties, reset the properties after downloading.
- When uploading the file that is being used, the file after uploading will be a 0-byte file. No matter if the original file is 0 byte or not, it will be displayed as 0 byte after uploading. Stop using this file and upload again.
- Do not upload a file that is more than 2GB. Once uploaded, the browser cannot be operated.

Point

About Action after Distribution

The content specified in the list of **Action after Distribution** will be operated after the distribution of all files registered in the same distribution task has completed.

The operation timing is shown as follows.

- When **Authority of "Action after Distribution"** is **Run as service**

  Processing will be performed right after distribution no matter whether the user has logged on to Windows or not.

- When **Authority of "Action after Distribution"** is **Run as logon user**

  Action after Distribution will be performed after the user has logged on to Windows. If there is no user logged on to Windows, Action after Distribution will not be performed until logon to Windows.

Open the file displayed on the window according to the **Run as logon user** method.

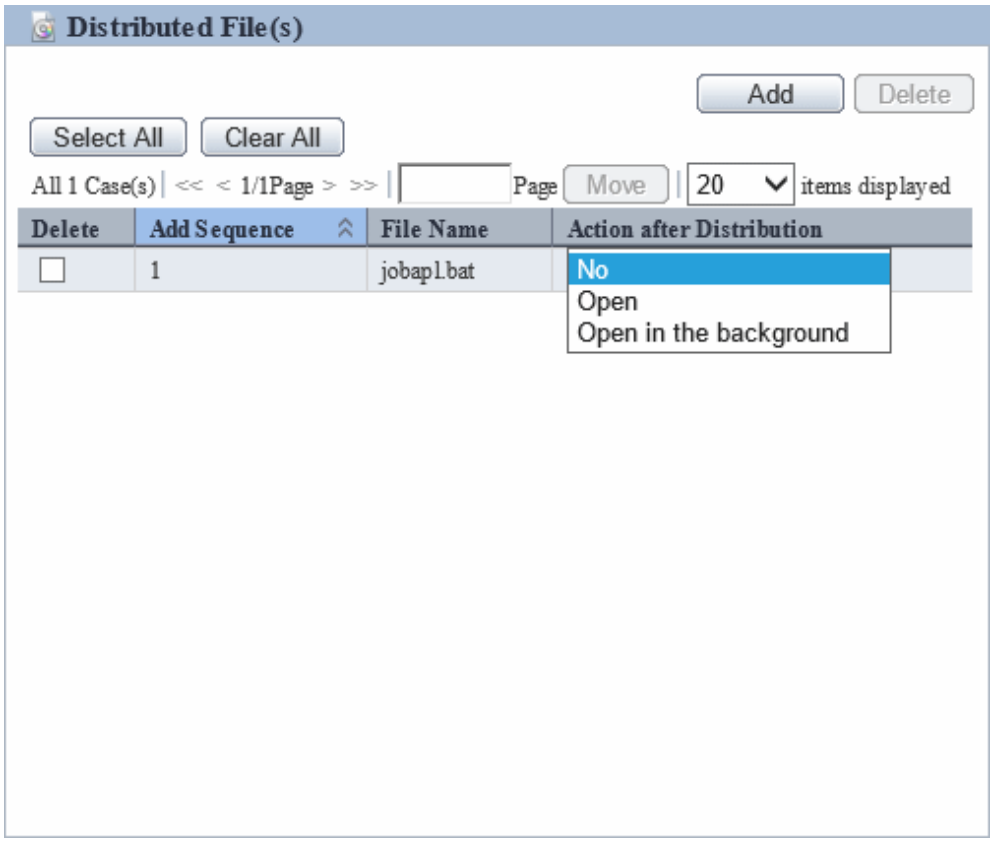
When the file displayed on the window is opened according to the **Run as service** method, the window of application will not be displayed on the window of logon user, and it will be in stopped status sometimes during the processing.

When the application for which **Wait for the completion of "Action after Distribution"** is set to **Yes** is in stopped status all the time and cannot be terminated, **Distribution has ended abnormally** will be displayed in **Progress** after 3 hours.

The Action after Distribution is performed according to the sequence of adding files to distribution task.

The content displayed in the list may vary with file extension.

- When the extension is not "zip"



The following can be specified.

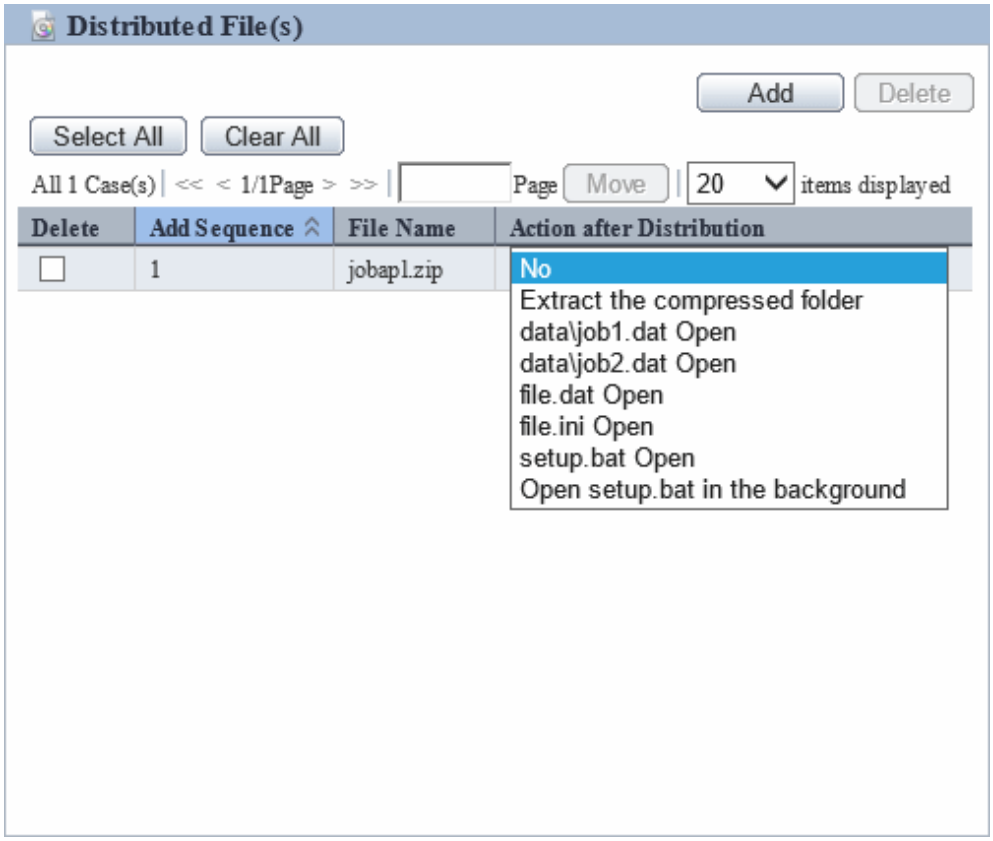
No	No processing will be performed after distribution.
Open	Open the file with related application defined by logon user.
Open in the background	Specify this option if the files to be distributed have an extension of .exe, .bat, .msi, .vbs, or .wsf. The files will be opened in the background after distribution.

Note

For files that require inputs, do not select **Open in the background** and distribute.

If they are distributed, the process will continue to run until the files opened in the background are closed.

- When the extension is "zip"



The following can be specified.

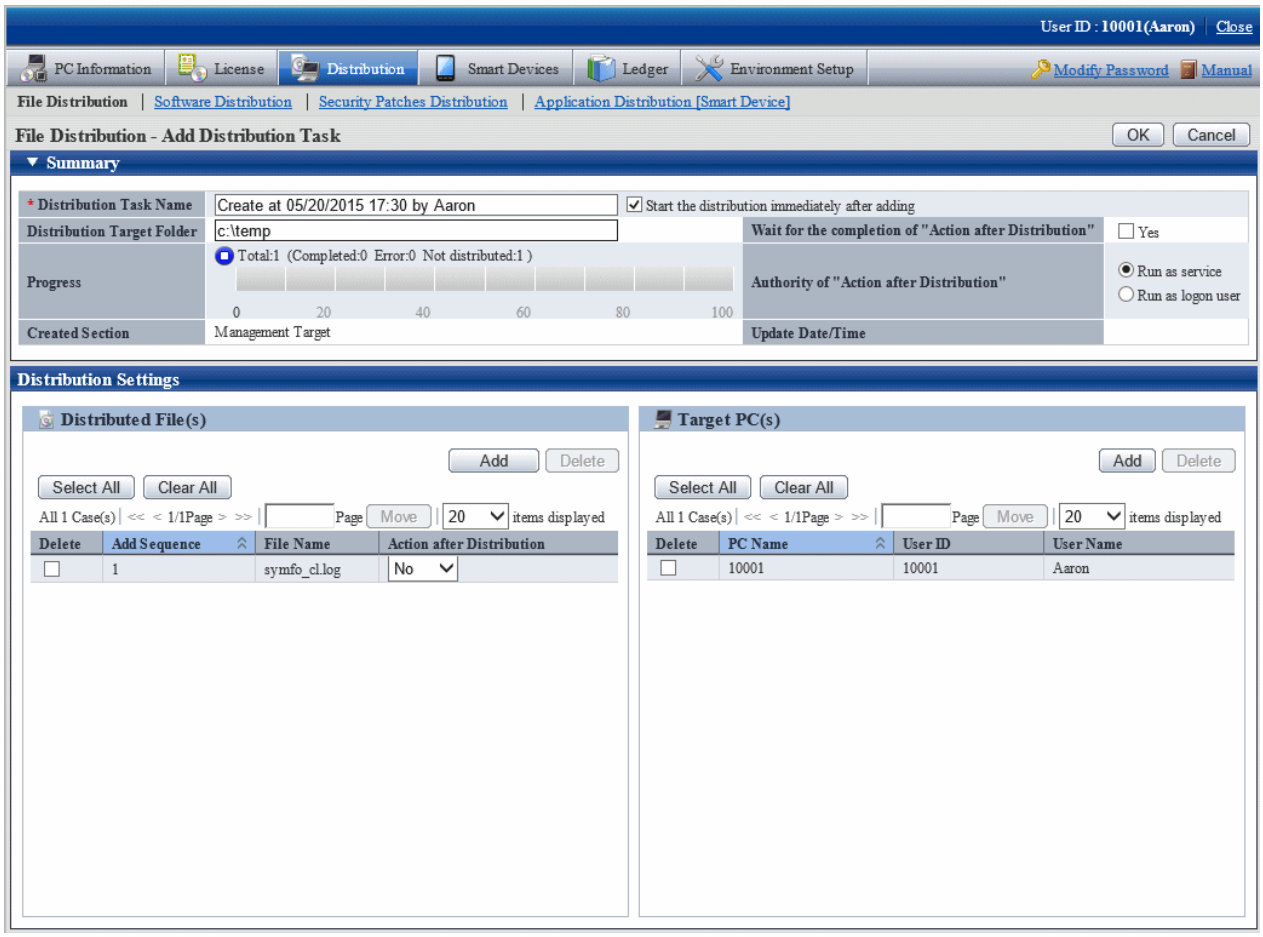
No	No processing will be performed after distribution.
Extract the compressed folder	Extract automatically according to the structure within the compressed folder on PC. The target directory of extraction is **Distribution Target Folder**.
***file* Open**	Open the file with related application defined by logon user. ***file*:** All file names up to the second level within the compressed folder
Open *file* in the background	Specify this option if the files in the compressed folder have an extension of .exe, .bat, .msi, .vbs, or .wsf. The files will be opened in the background after distribution. ***file*:** File names with an extension of .exe, .bat, .msi, .vbs, or .wsf, up to the second level within the compressed folder

Note

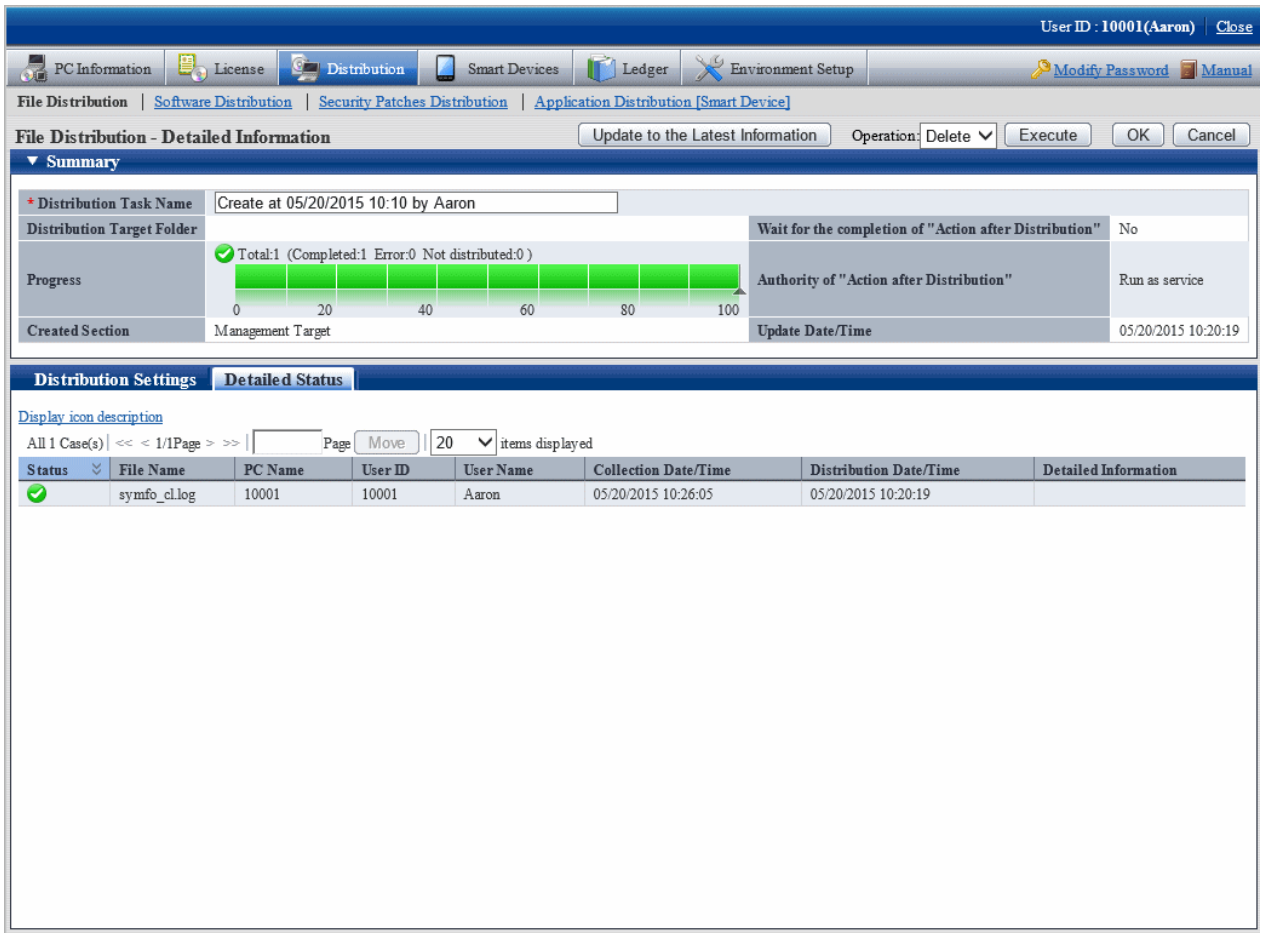
For files that require inputs, do not select **Open in the background** and distribute.

If they are distributed, the process will continue to run until the files opened in the background are closed.

In addition, after **Action after Distribution** has been specified, control for **Action after Distribution** can be set for each distribution task.

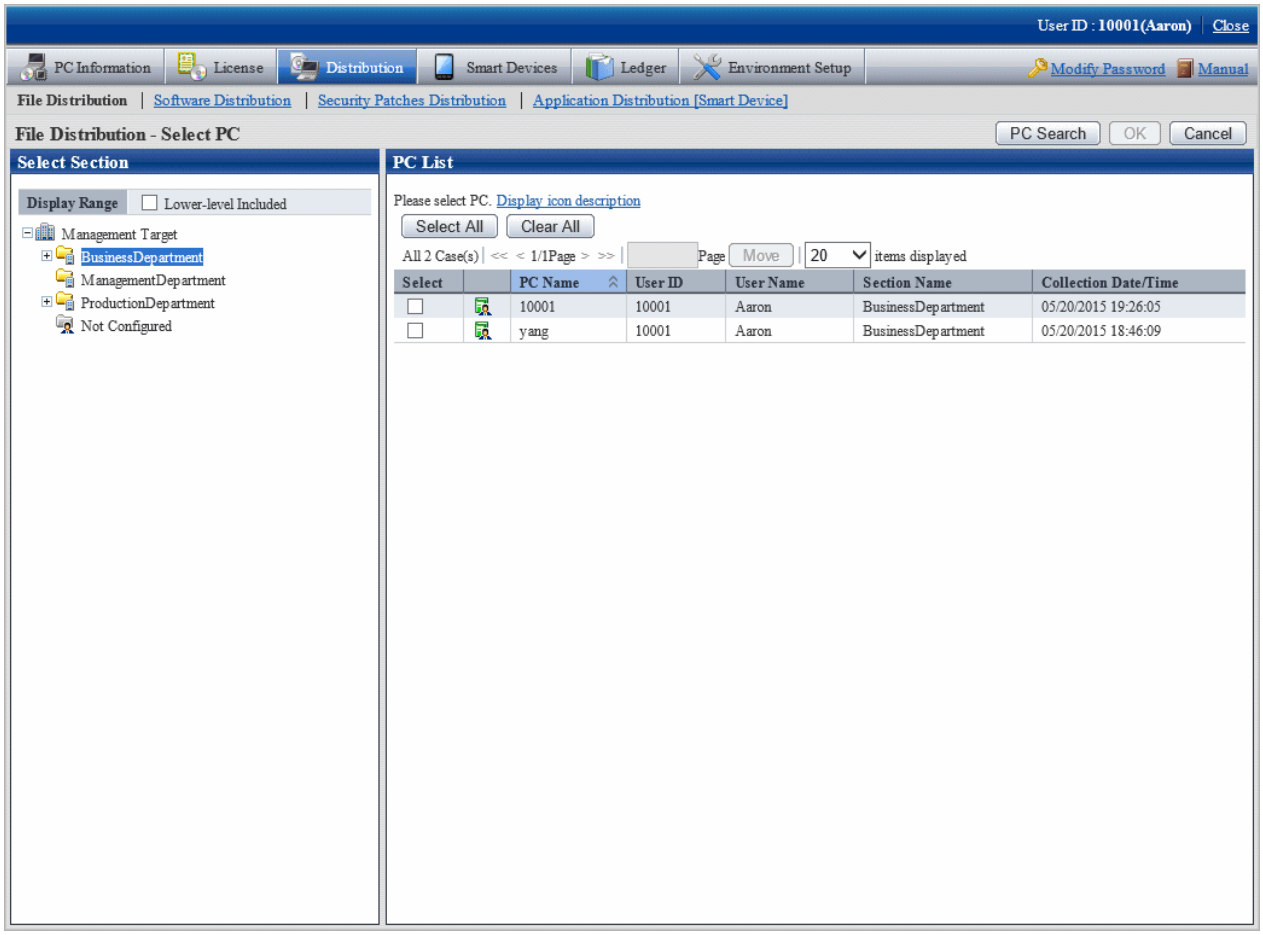


Here, when the check box **Yes** of **Wait for the completion of "Action after Distribution"** item is selected, for the files of which **Open** has been selected, as the result of waiting for completion of execution, the return value of file will be output to detailed information.


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 - Detailed Information
Update to the Latest Information
Operation:
Delete
Execute
OK
Cancel
Summary
* Distribution Task Name
Create at 05/20/2015 10:10 by Aaron
Distribution Target Folder
Wait for the completion of "Action after Distribution"
No
Progress
Total:1 (Completed:1 Error:0 Not distributed:0)
0
20
40
60
80
100
Authority of "Action after Distribution"
Run as service
Created Section
Management Target
Update Date/Time
05/20/2015 10:20:19
Distribution Settings
Detailed Status
Display icon description
All 1 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
symfo_cl.log
10001
10001
Aaron
05/20/2015 10:26:05
05/20/2015 10:20:19

4. Click the **Add** button of **Target PC(s)** in the bottom right field of window.

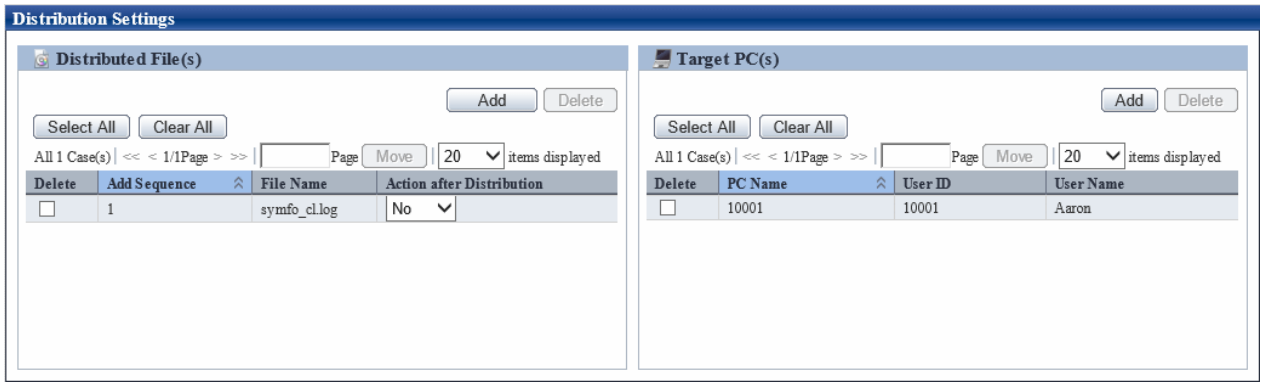
   The PC selection window will be displayed.



Note

If the PC in which the check box is not displayed is the CT prior to V13.2.0 or the command mode CT. Distribution cannot be performed.

Select the target Target PC(s) from the PC selection window, select the check box and click the **OK** button, the PC will be added to the list of distribution target PC.



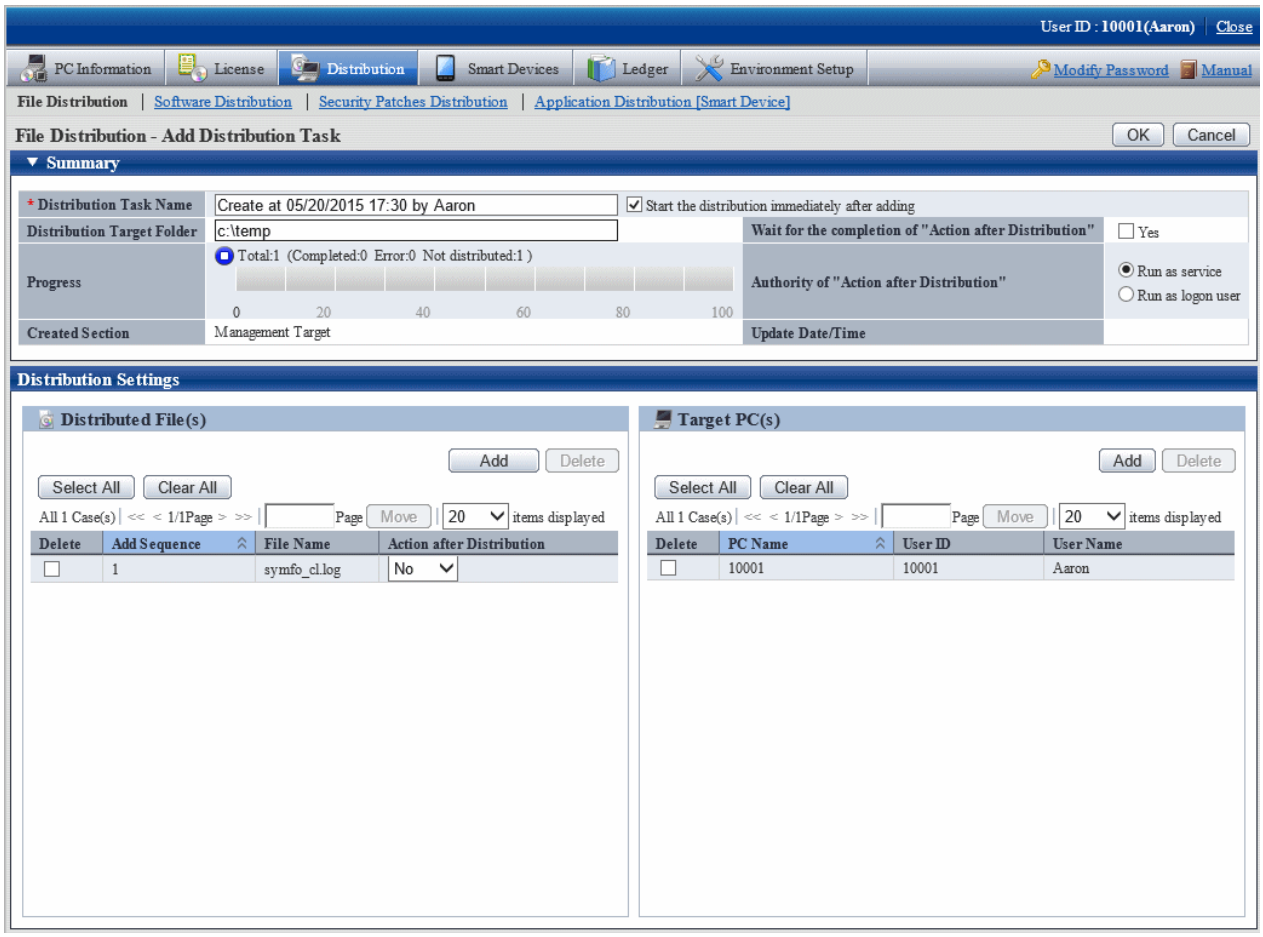
Point

Number of PCs can be registered in a single task

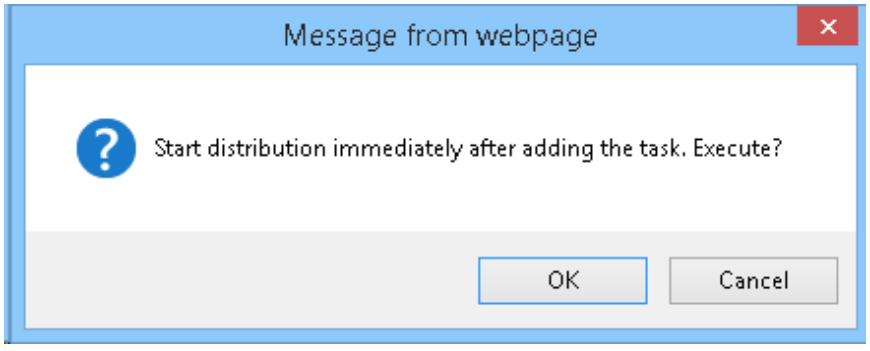
In a single task, maximum 2000 PCs can be registered.

When there are more than 2000 PCs, separate the task and register again.

5. If there is no problem in the settings, click the **OK** button.



When **Start the distribute immediately after adding** is selected, and the **OK** button is clicked, the following message box will be displayed.



Click the **OK** button in the message box, the distribution task will be added and file distribution will start.

Click **Cancel** to cancel the file distribution.

7.3 Operation

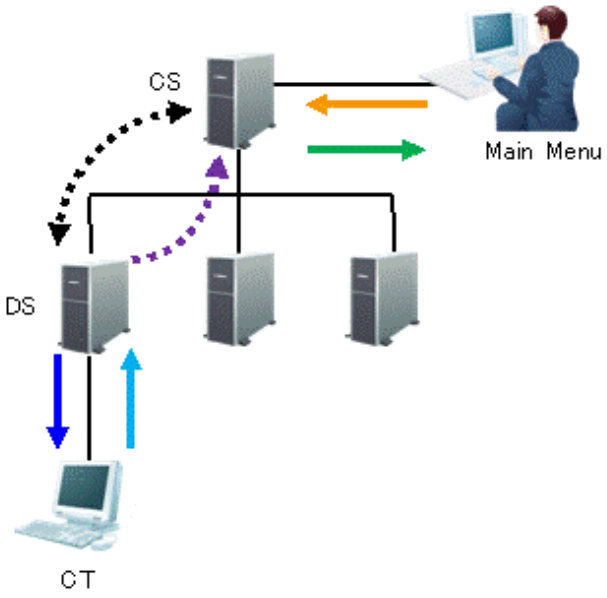
This section describes the following operation items of file distribution.

- Confirm distributed result
- Stop distribution
- Re-distribute
- Distribute the distribution task that has completed distribution preparation
- Confirm the content of registered distribution task
- Modify the content of registered distribution task
- Delete unnecessary distribution tasks
- Confirm the distribution result using CT operation status check command

7.3.1 Confirm Distributed Result

The distributed result can be confirmed in the initial window of **File Distribution**.

The flow from distribution settings to the status when distribution result can be confirmed is shown below.



Line Type	Operation	Timing of Operation
←	Set file and distribution target	Anytime Distribution settings from the main menu
◄····►	Synchronization of file distribution	Confirm every 5 minutes It is possible to set **Connection Interval with Upstream CS/DS** in **Environment Setup** > **CS/DS Settings and Status - DS Settings** window of the main menu
←	File download	Confirm every 10 minutes It is possible to set through the CustomPolicy.exe command

Line Type	Operation	Timing of Operation
	Upload immediately	Immediately After file has been downloaded, upload distribution result immediately
	Upload	Confirm every 5 minutes Upload distribution result from DS to CS
	Result confirmation	After uploading from DS to CS Distribution result can be confirmed from the main menu

As described above, after distribution settings have been performed on the main menu, distribution result can be confirmed after about 20 minutes.

Note

- Due to the network between CS and DS and between DS and CT, distribution to CT may be delayed.
- When the PC with CT installed is not started, it will be set to the status of distributing. After PC has started, file will be distributed.

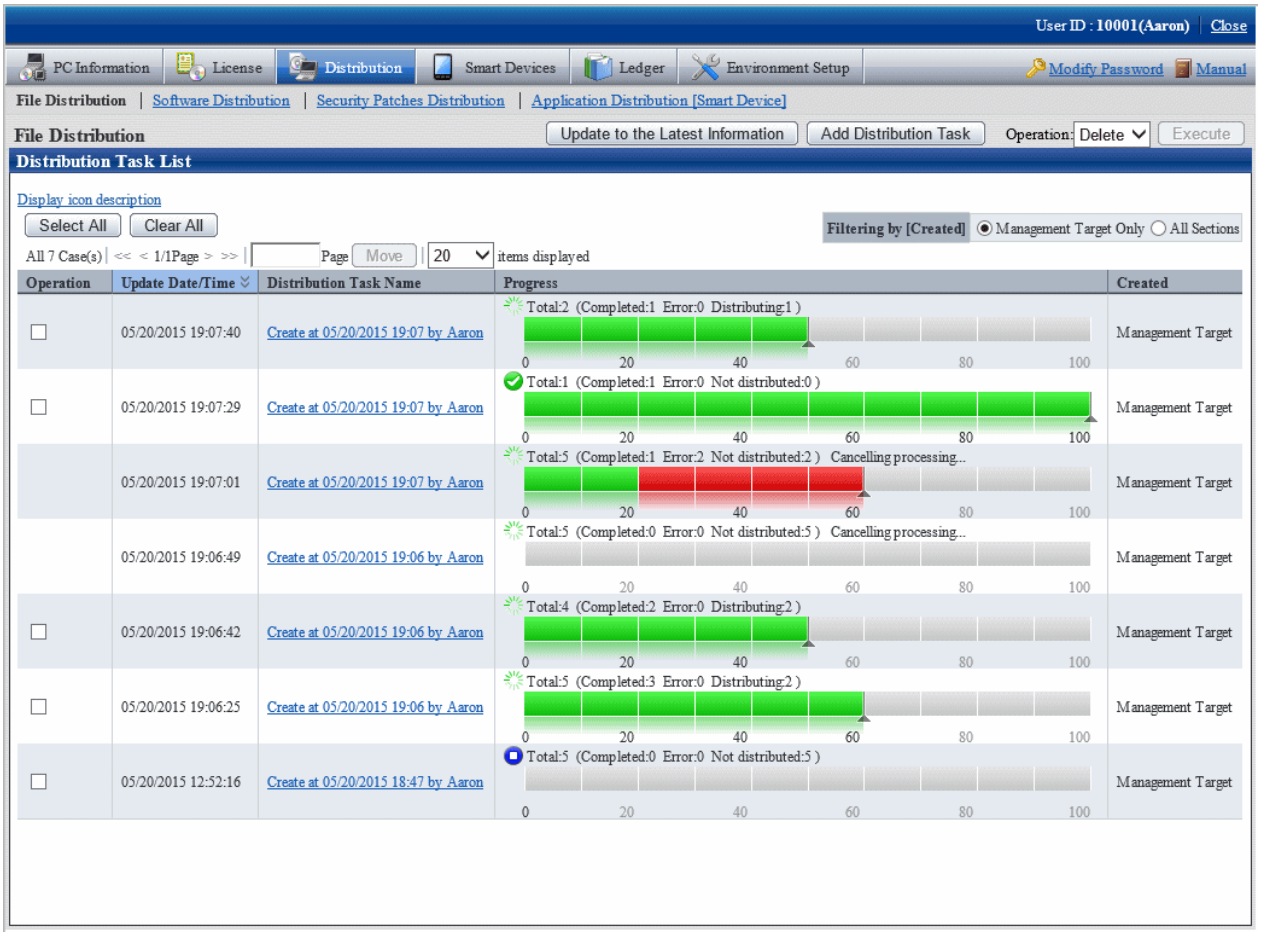
Note

If the distribution result is not notified after 7 days since the last **Start** and **Stop** operation for the distribution task, the distribution result will be displayed as abnormal termination.

The following describes the window display of distribution result.

When all distributions have completed successfully

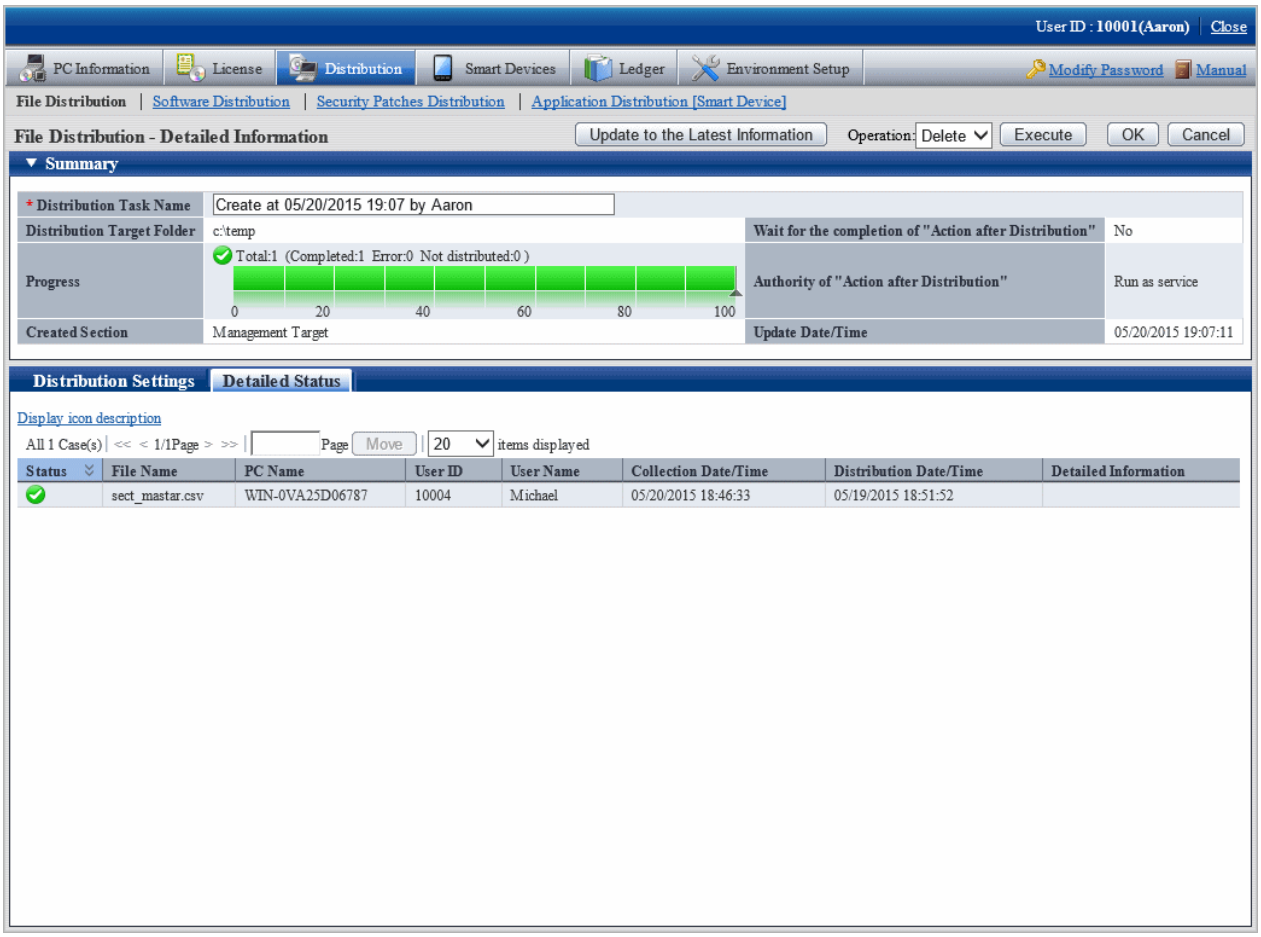
The icon will be .



No particular operation is required after confirmation.

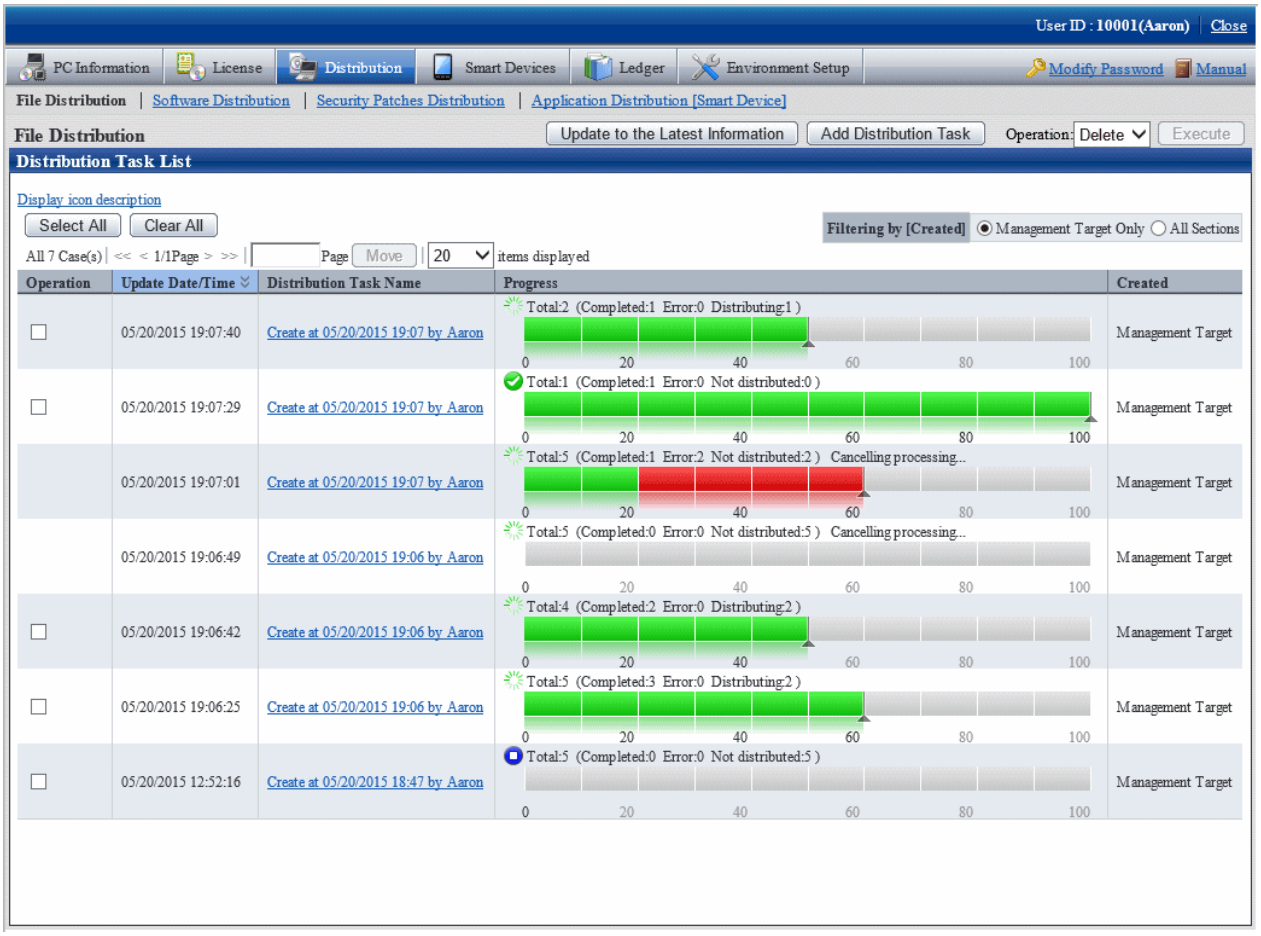
To confirm the content, click the link of distribution task name.

In the **File Distribution - Detailed Information** window, the details of distribution result of the distribution task can be confirmed.



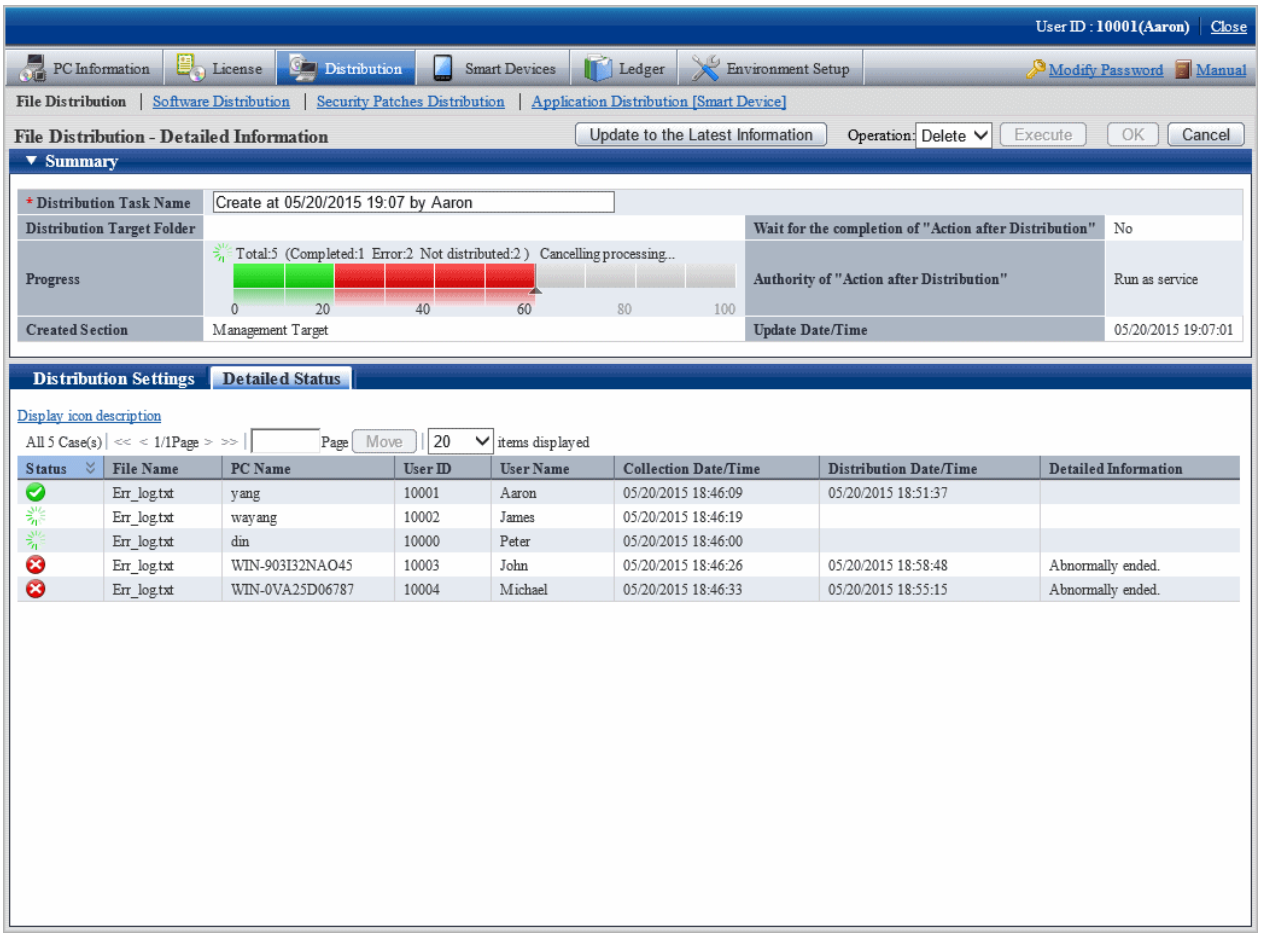
When all distributions have completed but the failed distribution exists

The icon will be .



To view the details of failed distribution, click the link of distribution task name.

In the **File Distribution - Detailed Information** window, the details of distribution result of the distribution task can be confirmed.



In the **Detailed status** tab at the bottom of window, you can see which file was failed to be distributed to which PC.

Confirm the error content displayed in details and adjust it to the status that enables distribution to this PC.

7.3.2 Stop Distribution

For PC that has not completed distribution, distribution can be stopped.

Note

On the PC as follows, distribution cannot be stopped.

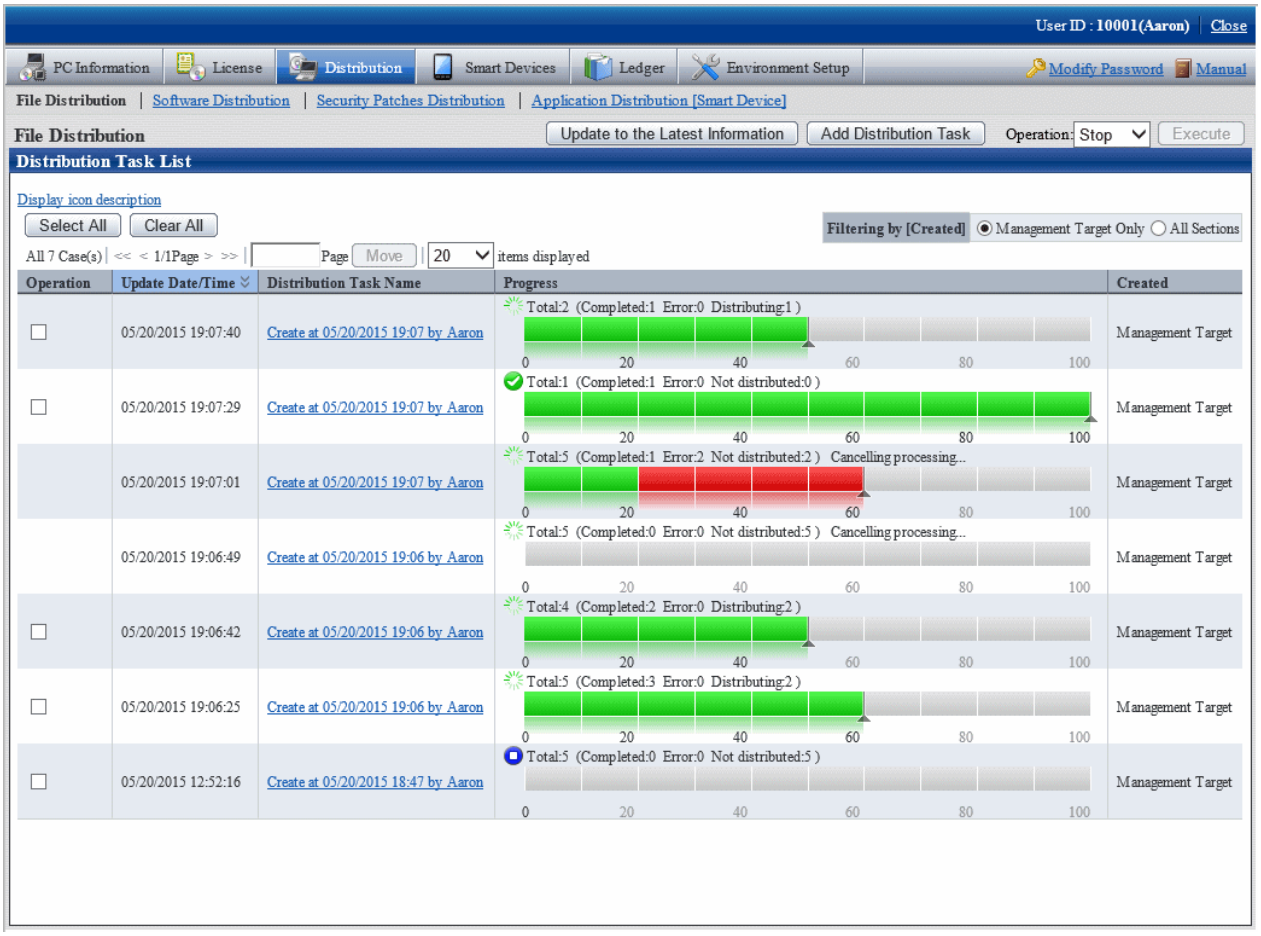
- PC that is not connected to power
- PC that is not connected to network

For this kind of PC, even if stop of distribution is performed, result will not be notified, and the window will show stopping all the time.

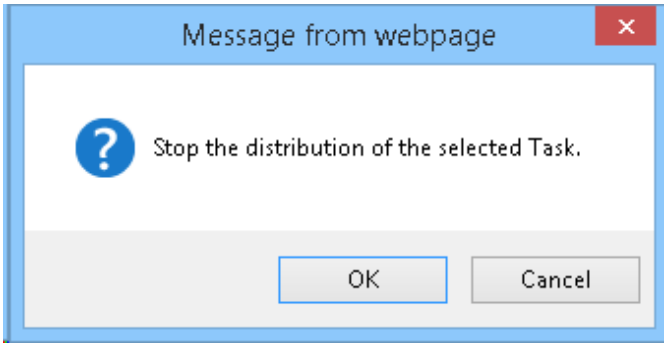
In addition, as described in "7.3.1 Confirm Distributed Result", it will take around 20 minutes from the time when distribution settings have been performed till the time when distribution result can be confirmed (the time depends on the value of interval of communication with the higher server of DS and the value of confirmation interval for file distribution/processing instruction of CT).

Therefore, it may show in distribution on the window, but the distribution has been completed actually or the status may change into completed after the stopping process sometimes.

Select the distribution task you wish to stop distribution, select **Stop** and click the **Execute** button.



Click the **Execute** button and the following message box will be displayed.

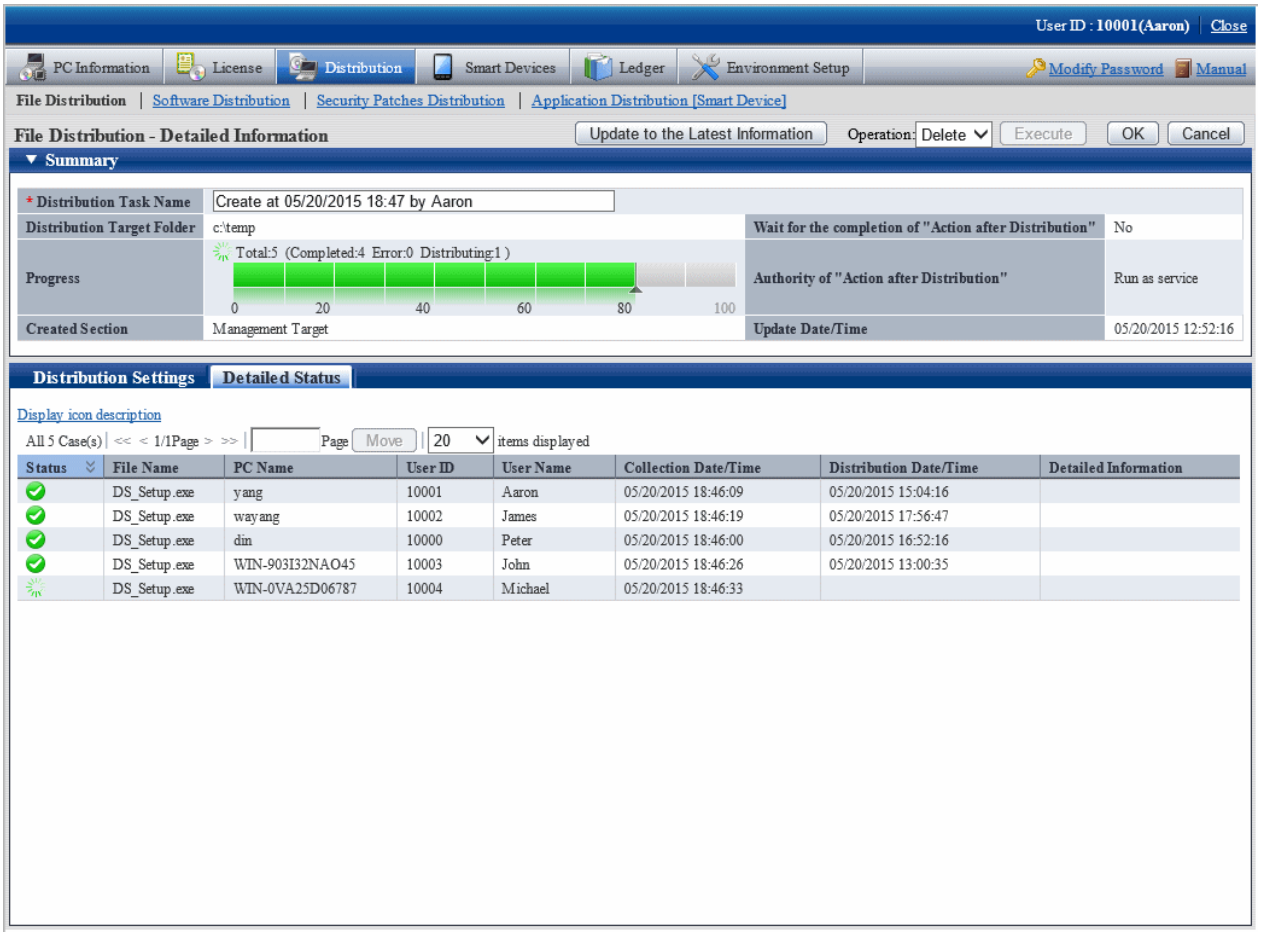


Click the **OK** button in the message box, and file distribution will be stopped.

Click the **Cancel** button, and file distribution will not be stopped.

When multiple distribution tasks have been selected, if the distribution task that cannot be stopped is contained, only the distribution task that can be stopped will be stopped.

In addition, distribution can also be stopped from the details window.



7.3.3 Re-Distribution

The PC that can perform re-distribution of files is as follows.

- PC that has stopped distribution (PC on which the distribution is not completed)
- PC on which the distribution has completed but part of the distribution failed

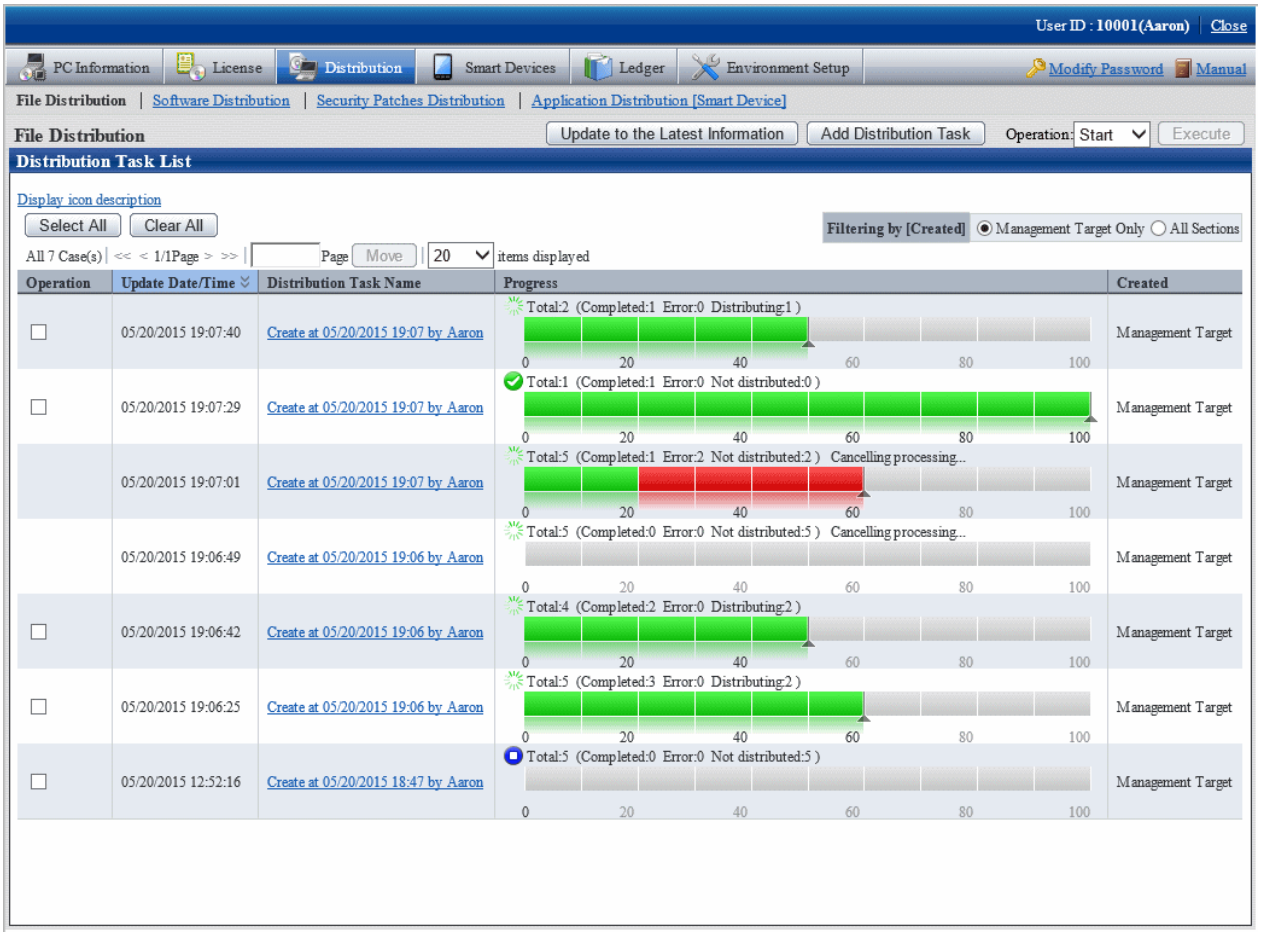
If both of the two reasons exist in the distribution task at the same time, re-distribution will be performed at the same time.

In following conditions, before eliminating the causes of failure, the status of failed distribution will remain in spite of re-distribution.

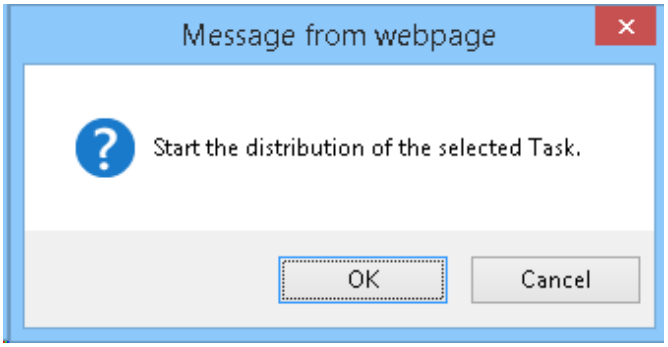
- Failed to distribute to DS.
- Failed to distribute to CT.
- The file that cannot be executed has been distributed.

For details of error displayed on the window, refer to *Systemwalker Desktop Patrol Reference Manual*.

Select the content that requires redistribution, select **Start** and click the **Execute** button.



After clicking the **Execute** button, the following message box will be displayed.

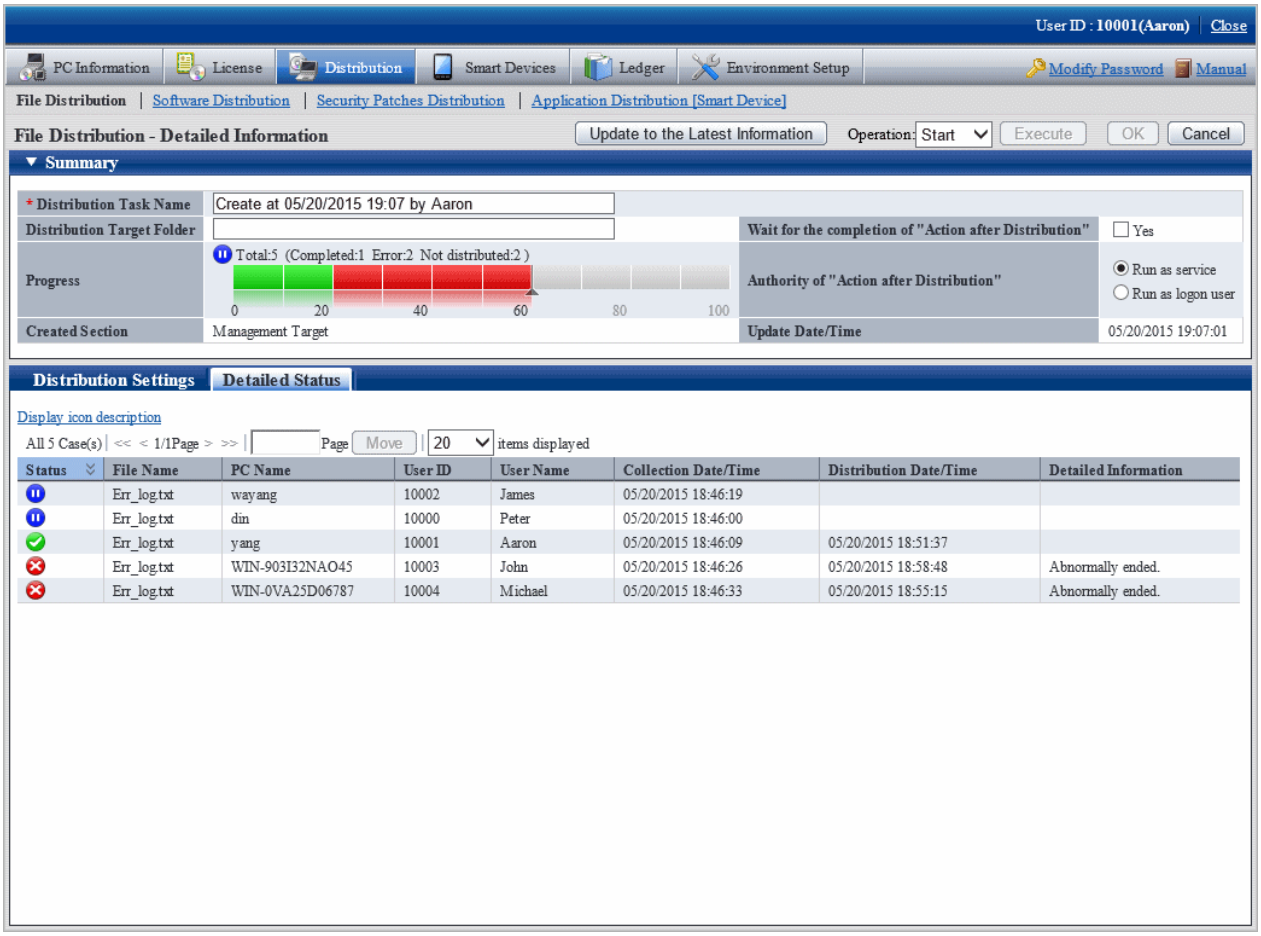


Click the **OK** button in the message box and file distribution will be started.

Click the **Cancel** button and file distribution will not be started.

When multiple distribution tasks are selected, and the task that cannot start distribution is contained, only the distribution task that can be started will be started.

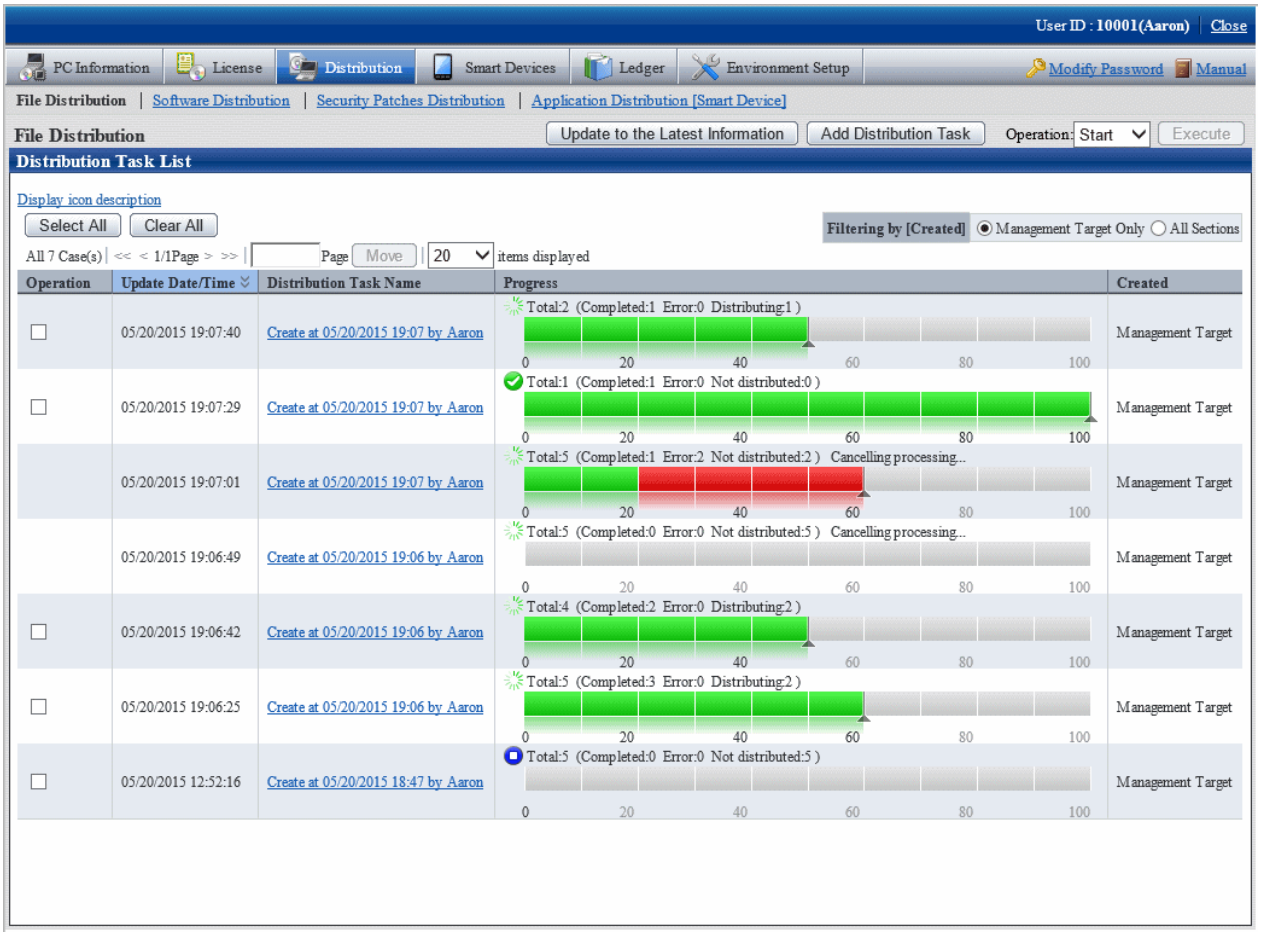
In addition, the distribution can also be started on the details window.



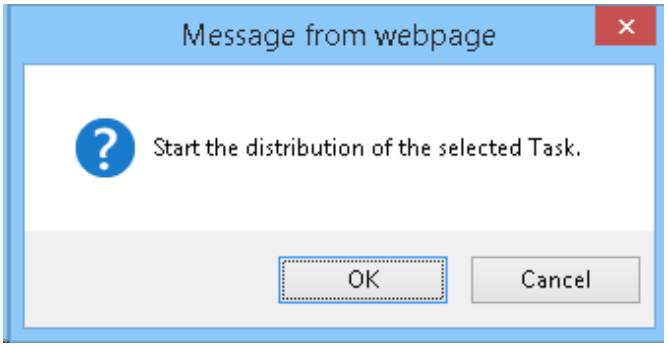
7.3.4 Distribute the Distribution Task that is Ready to be Distributed

When performing distribution settings, if the selection of **Start the distribution immediately after adding** of distribution task is canceled, distribution preparation is not completed and distribution will not be performed.

When distributing the task that has completed the preparation of distribution, select the task to be distributed, select **Start** and click the **Execute** button.



After clicking the **Execute** button, the following message box will be displayed.



Click the **OK** button in the message box and file distribution will be started.

Click the **Cancel** button and file distribution will not be started.

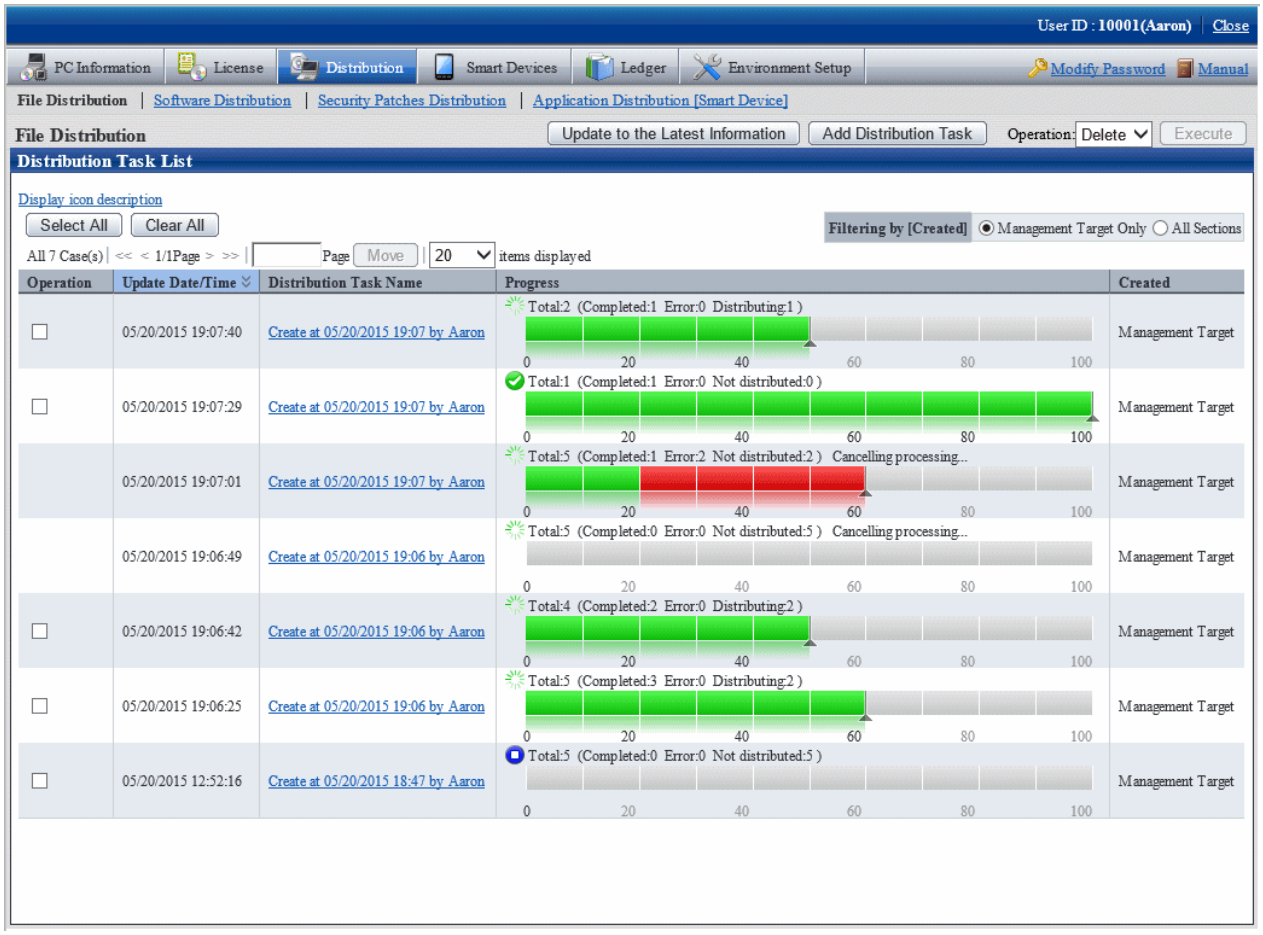
7.3.5 Confirm the Content of Registered Distribution Task

The content of distribution task registered in the distribution settings can be confirmed.

The procedure is as follows.

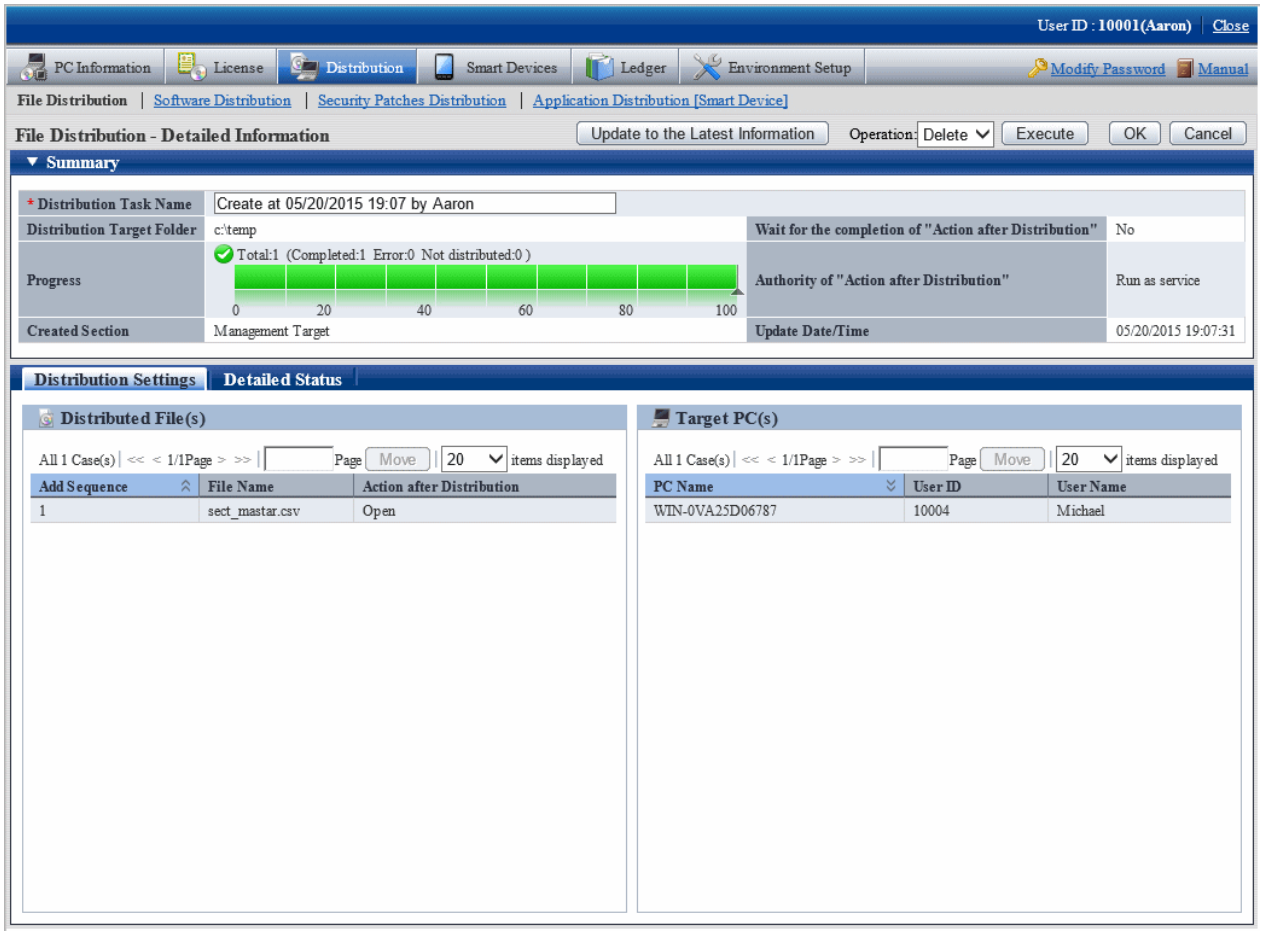
1. Log in to the main menu, and click the **Distribution** button.

   The initial window of **File Distribution** will be displayed. click the distribution task name.



2. Select the **Distribution settings** tab at the bottom field of the **File Distribution - Detailed Information** window.

   The software to be distributed and the distribution target PC can be confirmed.



7.3.6 Modify the Content of Registered Distribution Task

The following content of distribution tasks registered in the distribution settings can be modified.

- File to be distributed
- Distribution target PC
- Summary

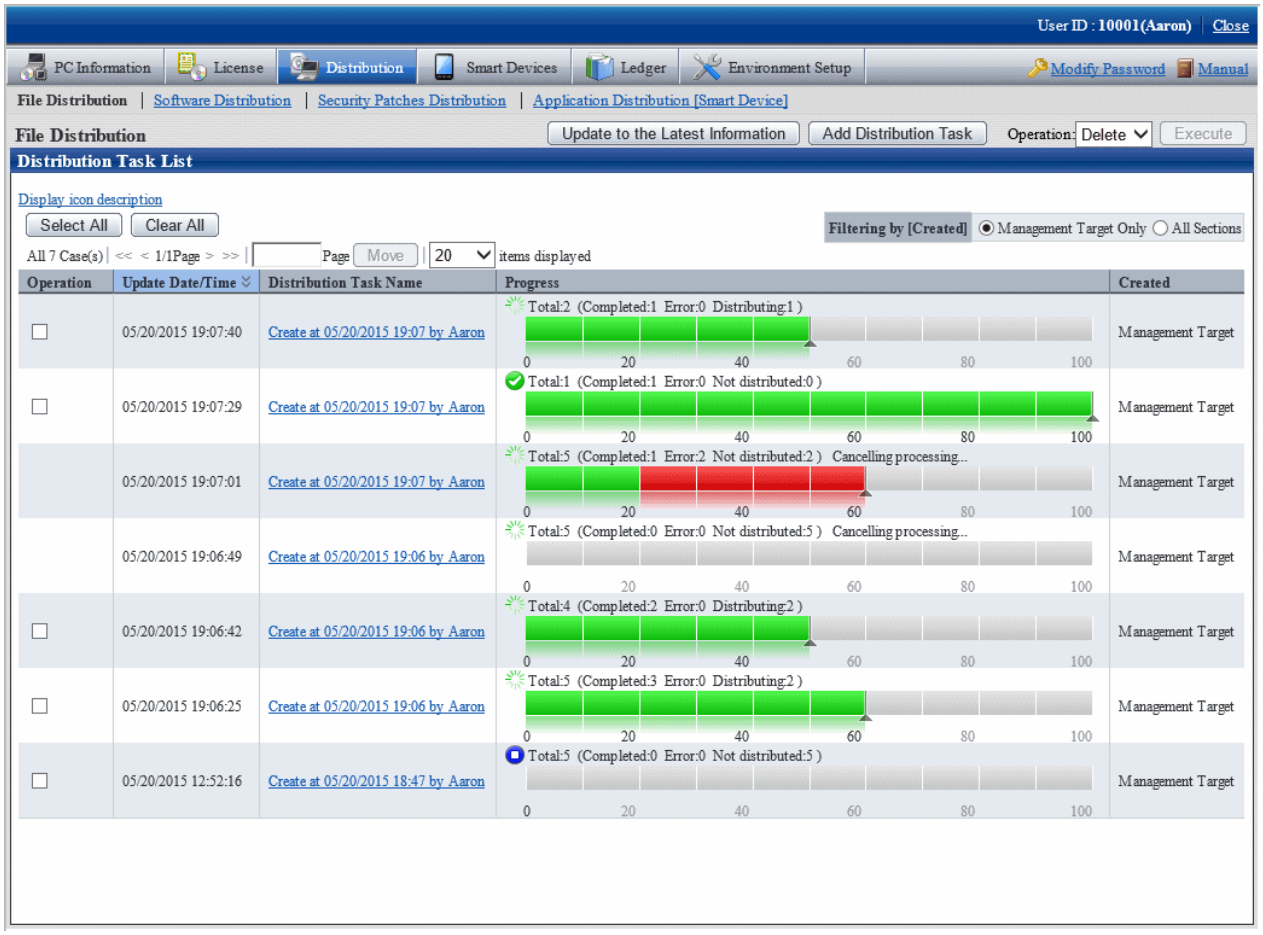
However, only the part that has completed preparation of distribution can be modified.

After distribution has been started (even once), the registered content cannot be modified.

The procedure is as follows.

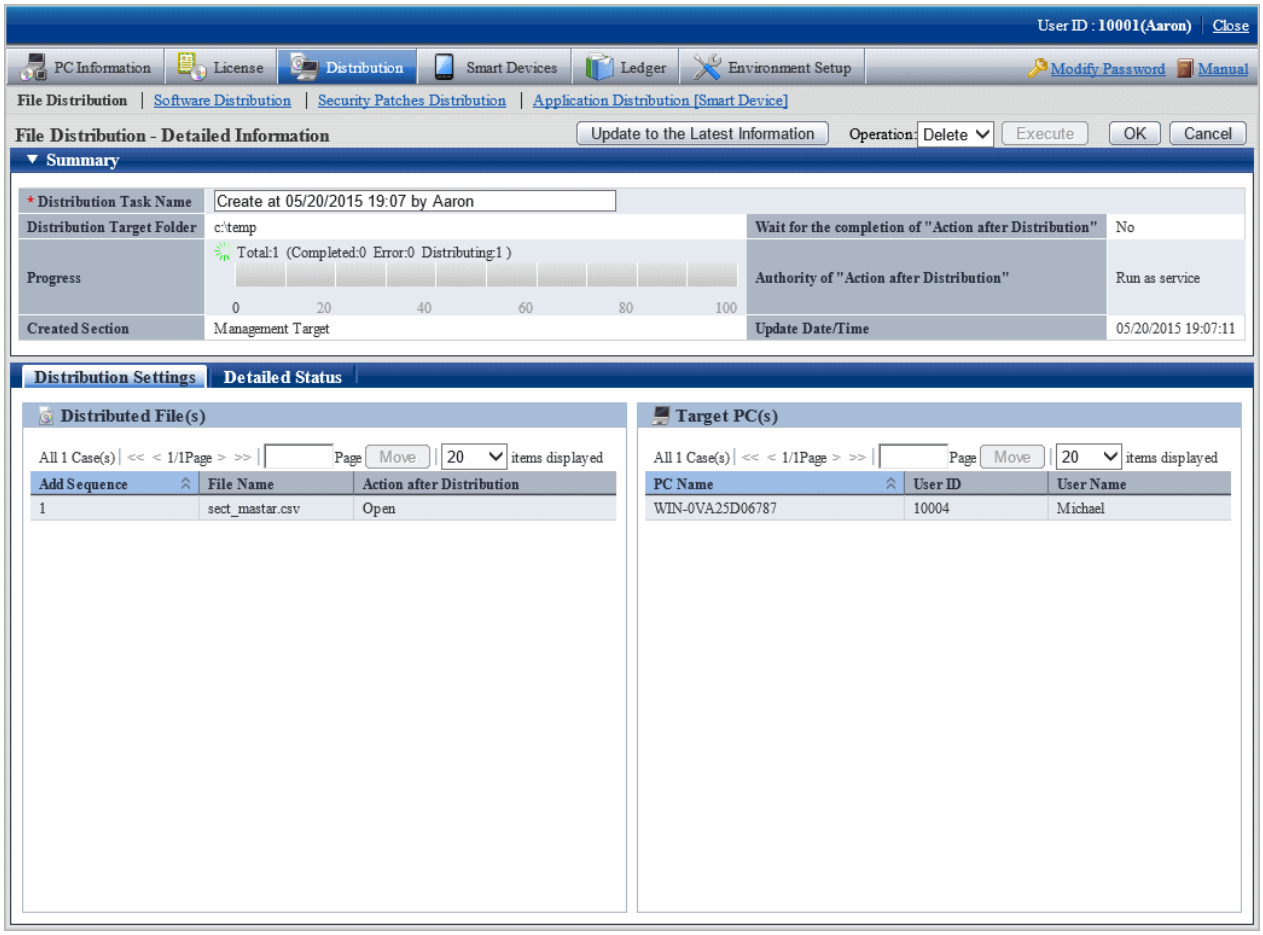
1. Log in to the main menu, and click the **Distribution** button.

   The initial window of **File Distribution** will be displayed. Click the distribution task name.



2. Select the **Distribution settings** tab at the bottom field of the **File Distribution - Detailed Information** window.

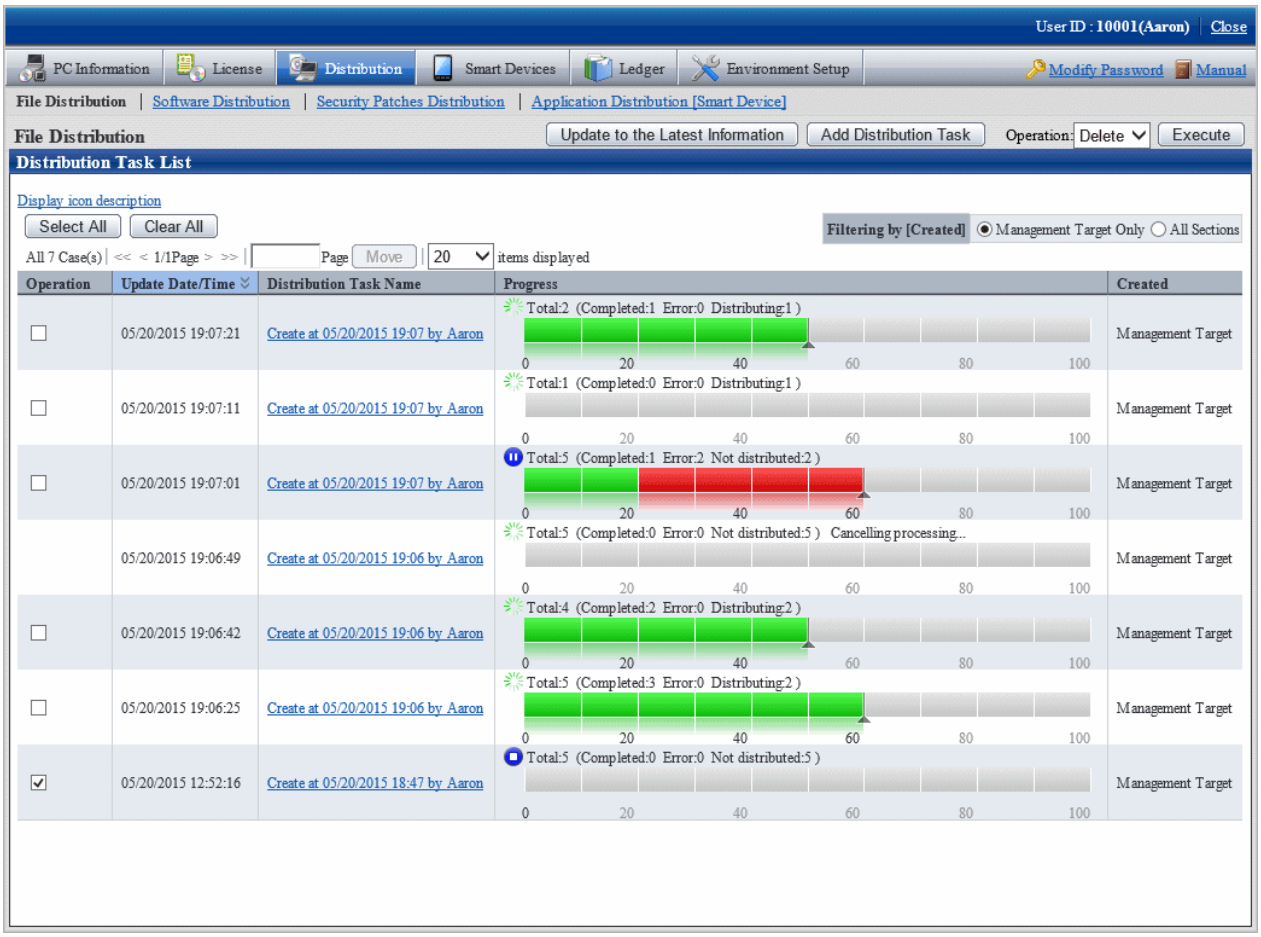
   The file to be distributed, distribution target PC and **Summary** at the top field of window can be modified.



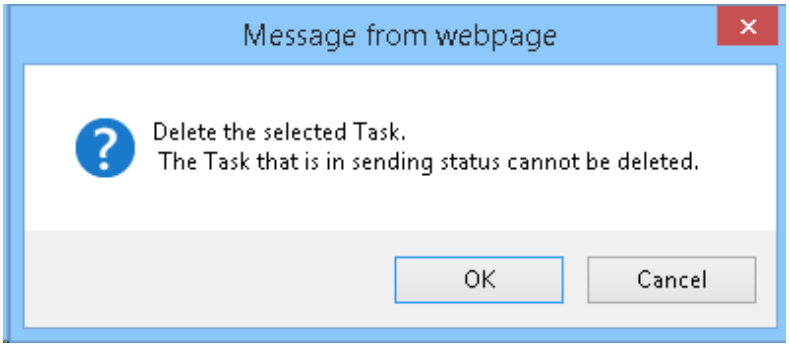
7.3.7 Delete Unnecessary Distribution Task

Distribution task cannot be deleted automatically.

To delete the task that has completed distribution, distribution task that is registered by mistake and other unnecessary tasks, select the task to be deleted from the initial window of **File Distribution**, select **Delete** and click the **Execute** button.



After clicking the **Execute** button, the following message box will be displayed.



Click the **OK** button, and the distribution task will be deleted.

Click the **Cancel** button, and the distribution task will not be deleted.

When multiple distribution tasks are selected, and the task that cannot be deleted is contained, only the distribution task that can be deleted will be deleted.

The distribution task that is being distributed cannot be deleted. To delete it, execute the stop operation first.

7.3.8 Confirm Distribution Result with CT Operation Status Check Command

The result of file distribution can be confirmed through executing the logcheck.exe (CT operation status check) and logcheckcs.exe (CT operation status check on CS) commands.

For details of CT operation status check command, refer to *Systemwalker Desktop Patrol Reference Manual*.

After the CT operation status check command has been executed, it will be displayed according to the following category of "File Distribution List".

```
------------------------------------------------------------------------
Distribution file list
------------------------------------------------------------------------
======== The distributed task ========
Name                                  Status      Distribution date        Completion date
Task1                                End normally      9. 20, 2011          9. 21, 2011
Task2                                End abnormally    9. 21, 2011          9. 21, 2011
Task3                                Pause            9. 21, 2011           9. 21, 2011
```

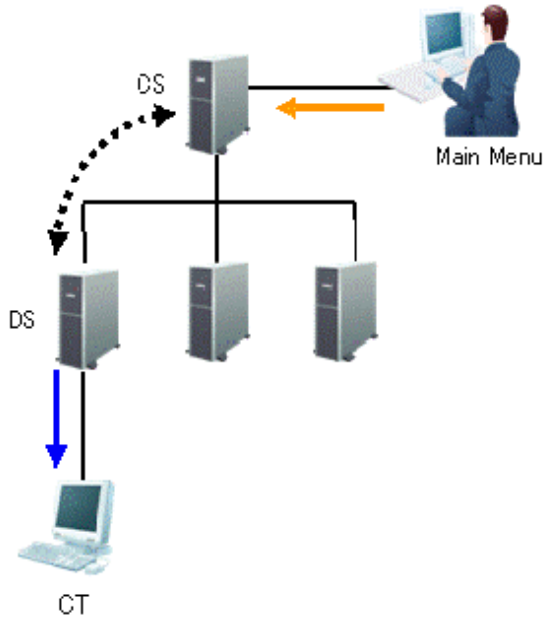
Chapter 8 Distribute Software

This chapter describes how the software will be distributed to the CT.

8.1 Operation Steps

The software registered from the main menu can be automatically or manually distributed to CT.

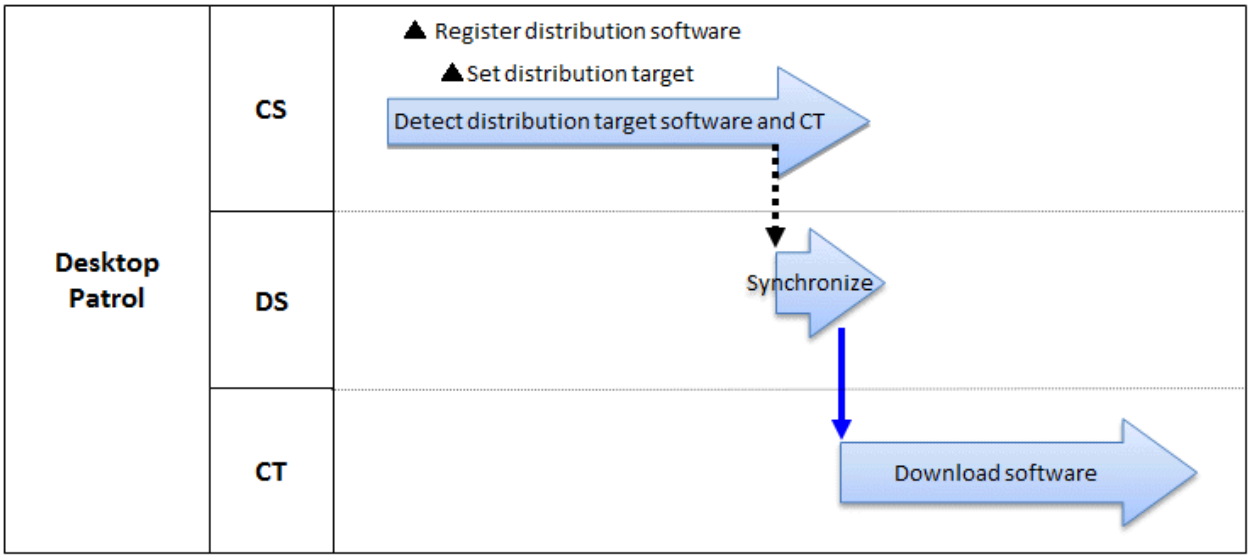
See below for the data flow at software distribution.



The information needed for software distribution and the time point (original value) when the information is sent are shown in the following table.

Type of line	Operation	Operation Opportunity
←	Software registration	Anytime Register software from main menu.
◄····►	Software synchronization	Confirm every 5 minutes Settings in DS name selection in **Environment Setup** > **CS/DS Settings and Status** in main menu.
←	Automatic software download	Confirm at the following time points - At logon to Windows - Standby of the previous day, resume from standby on the next day - Open the software download window - Specified time point
	Manual software download	In CT, select **Start** > **Programs** > **Systemwalker Desktop Patrol CT** > **Software Download**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Software Download**.

The time chart up to software distribution to CT is shown below.



Operation	Operation Opportunity
Identification of software to be distributed and CT	Within 1 hour after confirmation of release object
Software synchronization	Confirm in every 5 minutes Settings in DS name selection in **Environment Setup** > **CS/DS Settings and Status** in main menu.

The sequence chart is described as below.

Register the software to be distributed. Refer to relevant contents of "8.2.3 Register Software Distribution to be Released" for logon method.

Through setup of the release object, the software registered will be distributed to the target PC. Refer to relevant contents of "8.2.4 Settings of Distribution Target" for setup method.

No special setup needed for release operation. Operation as per setup when the product is imported.

- Software synchronization

  Refer to relevant contents of "8.2.1 Perform Settings of Server to Distribute Software" to modify settings.

- Software download

  Refer to relevant contents of "8.2.2 Set Conditions to Distribute Software to Client" to modify settings.

8.2 Settings

Perform settings of software distribution according to the following procedure.

1. Setting of server to distribute software
2. Set conditions to distribute software to client
3. Register software to be distributed
4. Set Distribution Target

8.2.1 Perform Settings of Server to Distribute Software

Perform the following settings of conditions under which to distribute the software for CS and DS.

- Interval and time frame of software download

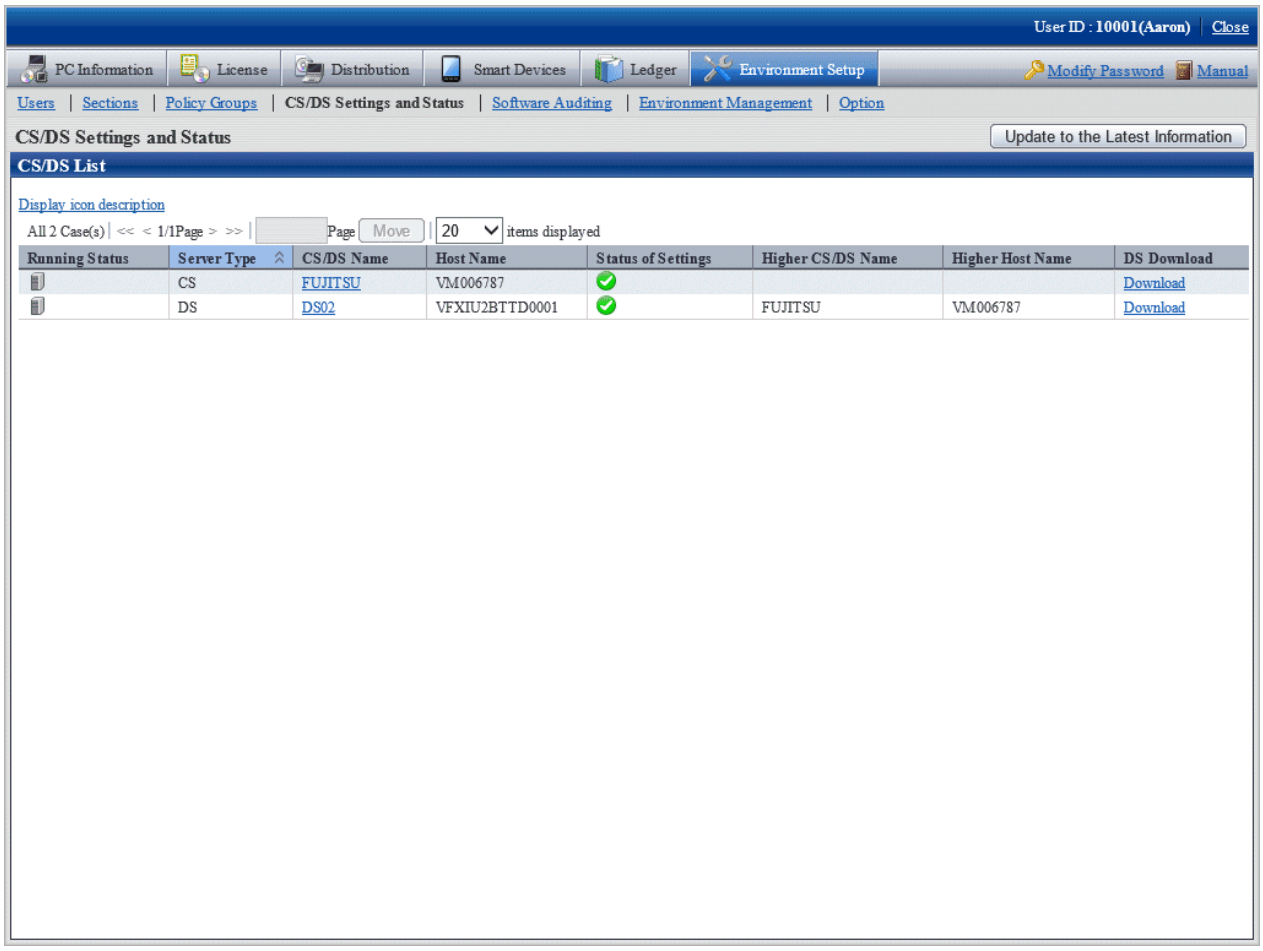
The procedure is as follows.

1. Logon to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **CS/DS Settings and Status**.

   The following window will be displayed.



The following describes the items in the window.

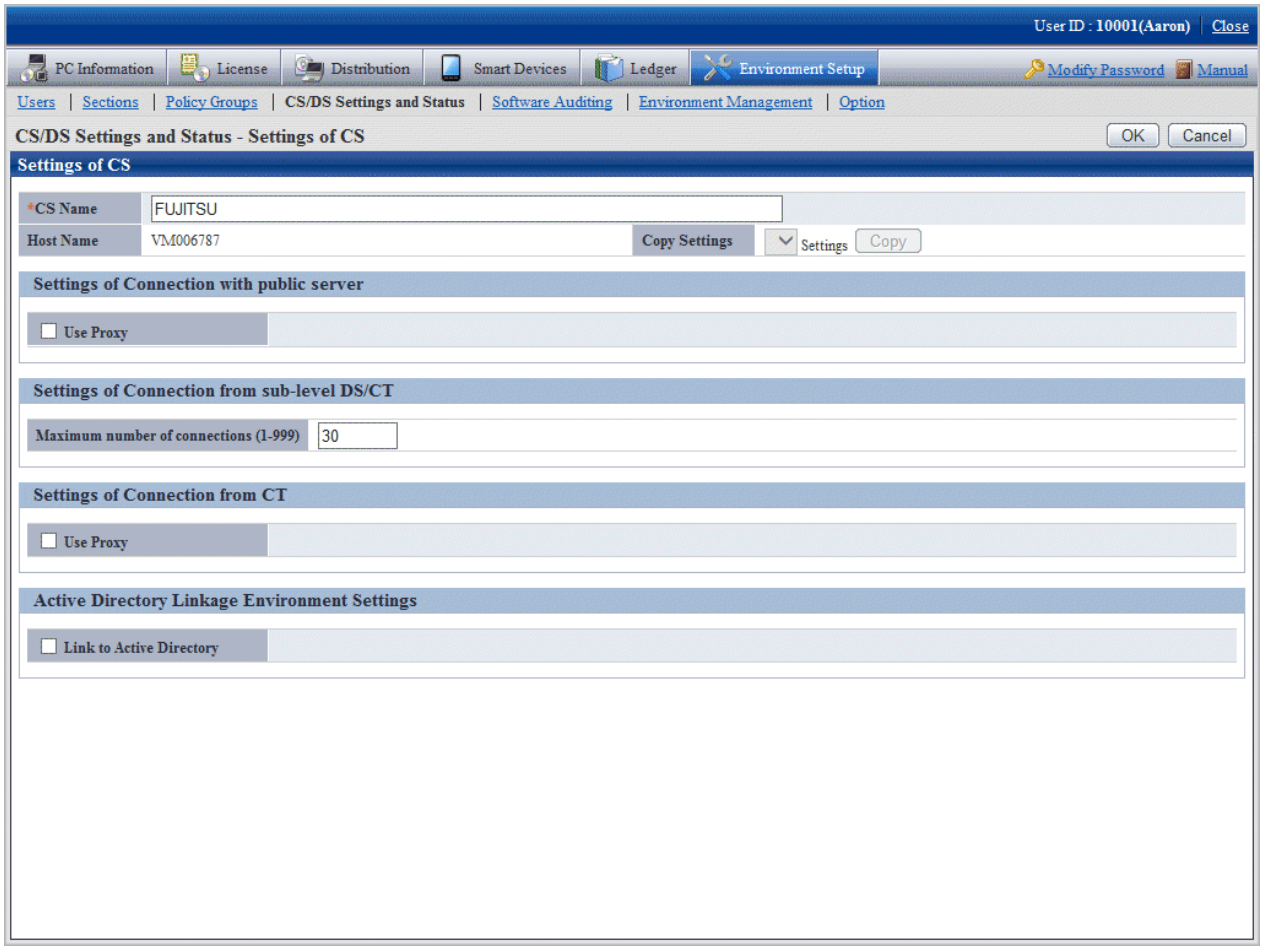
Item	Description
Running Status	Display operation status of CS/DS. : Running. : Not running for some reasons.
Server Type	Display the type of CD/DS
CD/DS Name	Display respective CS/DS name. Click CD/DS name to confirm and change the setup of each CD/DS. But you cannot click server name when the section management ID is used to log on.
Host Name	Display Host name corresponding to CD/DS name.

Item	Description
Status of Settings	Indication of reflection state of each server corresponding to respective setup information on CS/DS/CT. : Settings have been reflected. : Settings are being reflected. : Settings are failed to be reflected.
Higher CD/DS Name	Corresponding to server, displayed when higher server existing.
Higher Host Name	Display of Host name corresponding to higher CS/DS name.
DS Download	It can download the installer of DS.

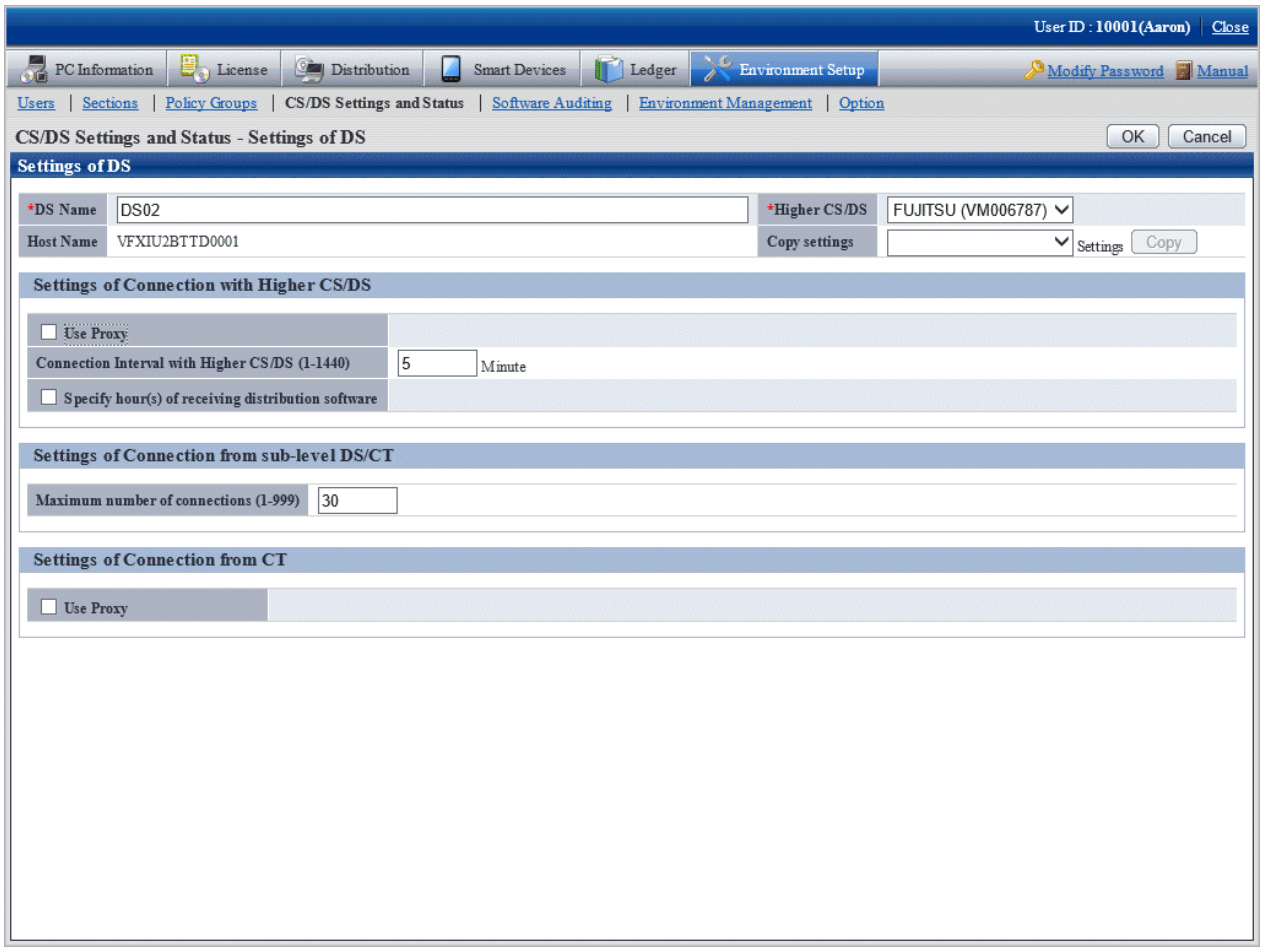
3. Click the link of server name.

   The following window will be displayed.

   When CS is selected



When DS is selected



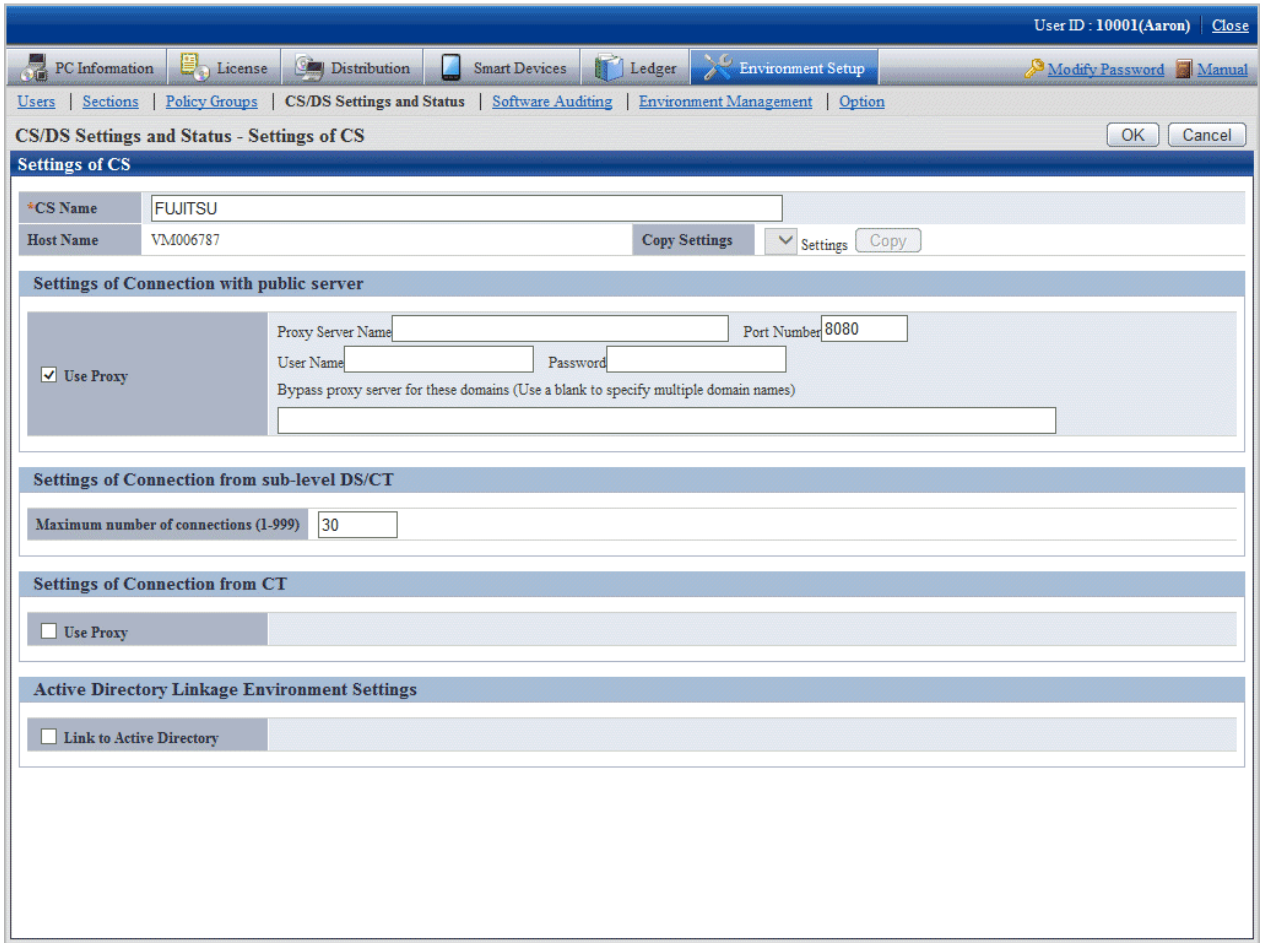
Set the following items.

Item	Description
CS/DS name	Display of general name specified for CS/DS in installation. Japanese, single-byte alphanumeric characters, including special characters of "-", "@", and "." within 50 characters for server name. blank characters not allowed. Cannot be omitted.
Higher CS/DS	Select from the list to change the higher server. This item can only be set when DS is set.
Copy button	Settings of CS/DS registered can be rewritten. Select the Cs/DS registered from the list, click **Copy** button, setup of the CS/DS selected will be rewritten.

4. Input the following items in **Settings of Connection with public server** and **Settings of Connection with Higher CS/DS**.

   Connection setup with higher server to DS when it's DS.

When CS is selected

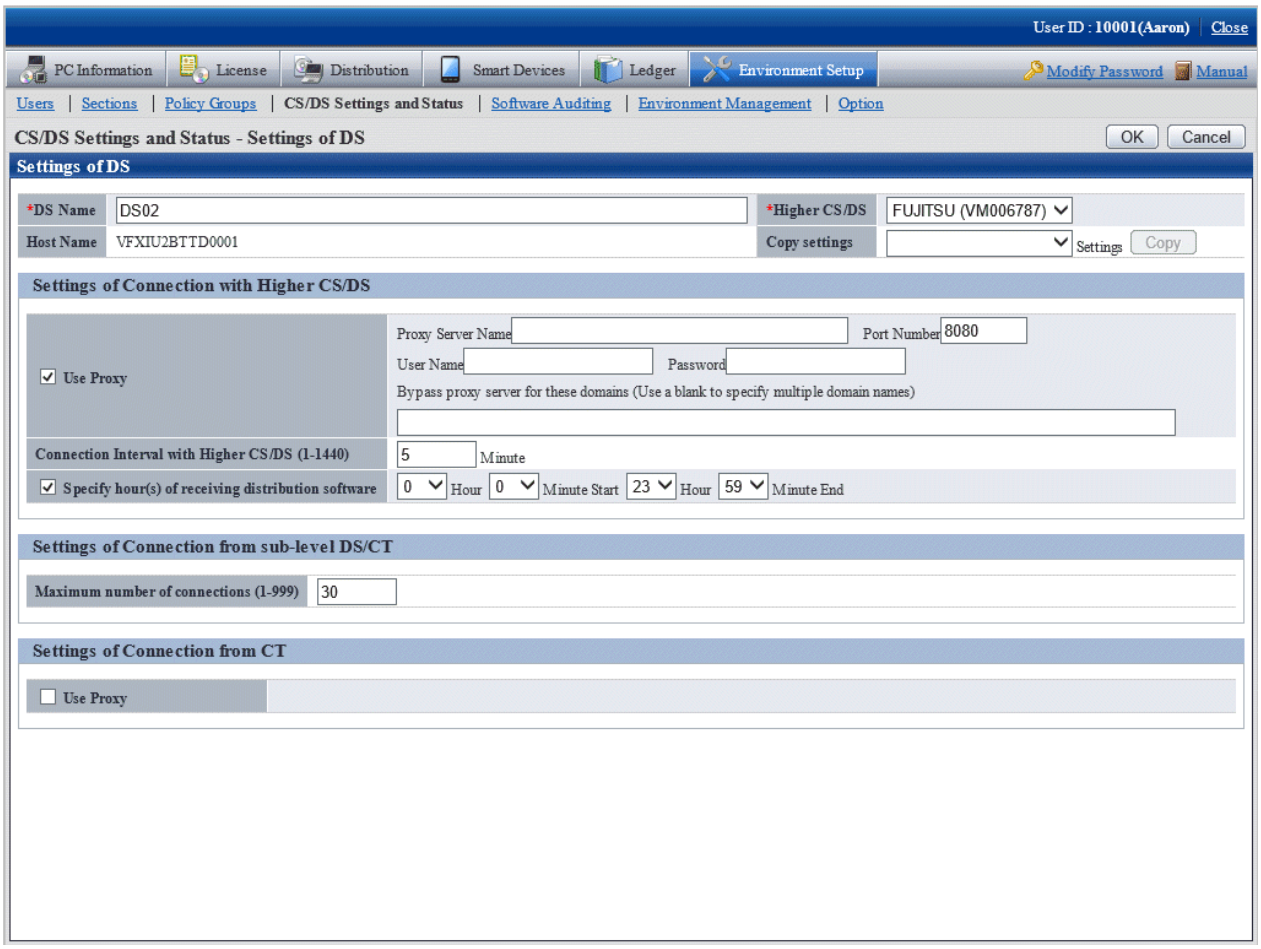


Set the following items.

Item	Description
Use proxy	Select this item in case of use proxy. Finish specifying the following contents during selection. - Proxy Server Name Designation of proxy server name. Input of FQDN or IP address composed of single-byte English number, "-" and "." within 64 characters. Note **Communication in an IPv6 environment** You cannot specify an IPv6 address. For communication in an IPv6-only environment, perform one of the following registrations beforehand and enter the host name: - Register the host name and IP address of the CS and DS in the DNS server - Register the host name and IP address of the CS and DS in the hosts file on the communication source PC - Port Number

Item	Description
	Port number of specified proxy server. Specify in 1-65535. Cannot be omitted. - User Name Specify user name of proxy server using up to 256 halfwidth characters. - Password Specify password to proxy server using up to 256 halfwidth characters. - Bypass proxy server for these domains Specify domain name not using proxy server. Use blank space to separate when many domain names are specified. Specify a value using up to 2,064 halfwidth characters. Specify domain name composed of single-byte English number, "-" and ".".

When DS is selected



Set the following items.

Item	Description
Use proxy	Select this item in case of proxy use. Finish designating the following contents during selection.

Item	Description
	- Proxy Server Name Designation of proxy server name. Input of FQDN or IP address composed of single-byte English number, "-" and "." within 64 characters. Note **Communication in an IPv6 environment** You cannot specify an IPv6 address. For communication in an IPv6-only environment, perform one of the following registrations beforehand and enter the host name: - Register the CS and DS host names and IP addresses in the DNS server. - Register the CS and DS host names and IP addresses in the hosts file of the communication source PC. - Port Number Port number of specified proxy server. Specify in 1-65535. Cannot be omitted. - User Name Specify user name of proxy server using up to 256 halfwidth characters. - Password Specify password to proxy server using up to 256 halfwidth characters. - Bypass proxy server for these domains Specify domain name not using proxy server. Use blank space to separate when many domain names are specified. Specify a value using up to 2,064 halfwidth characters. Specify domain name composed of single-byte English number, "-" and ".".
Connection Interval with Higher CS/DS	Specify download period of file and software from the higher server, specify in 1-1440, a value in unit of minute. Default is 30 and it cannot be omitted.
Specify hour(s) of receiving distribution software	Select this item in time frame when specifying file and software download. Specify time frame to download file and software from higher server. Without selection, the download period can be any time in the 24 hours. Select between 0-23 for hour unit and 0-59 for minute unit. The start time and end time shall not be specified to be the same.

5. Enter the following items in **Settings of Connection from sub-level DS/CT**.

Item	Description
Maximum number of connections	Total number of lower DS or CT connecting to CS or DS simultaneously, specify in 1-999 (number of pieces). Default is 30 and it cannot be omitted.

6. Click **OK** button.

8.2.2 Set Conditions to Distribute Software to Client

Set the following as conditions for distribution of software to CT.

- Confirmation of new software
- User's limits of authority needed for download

Set the client policy.

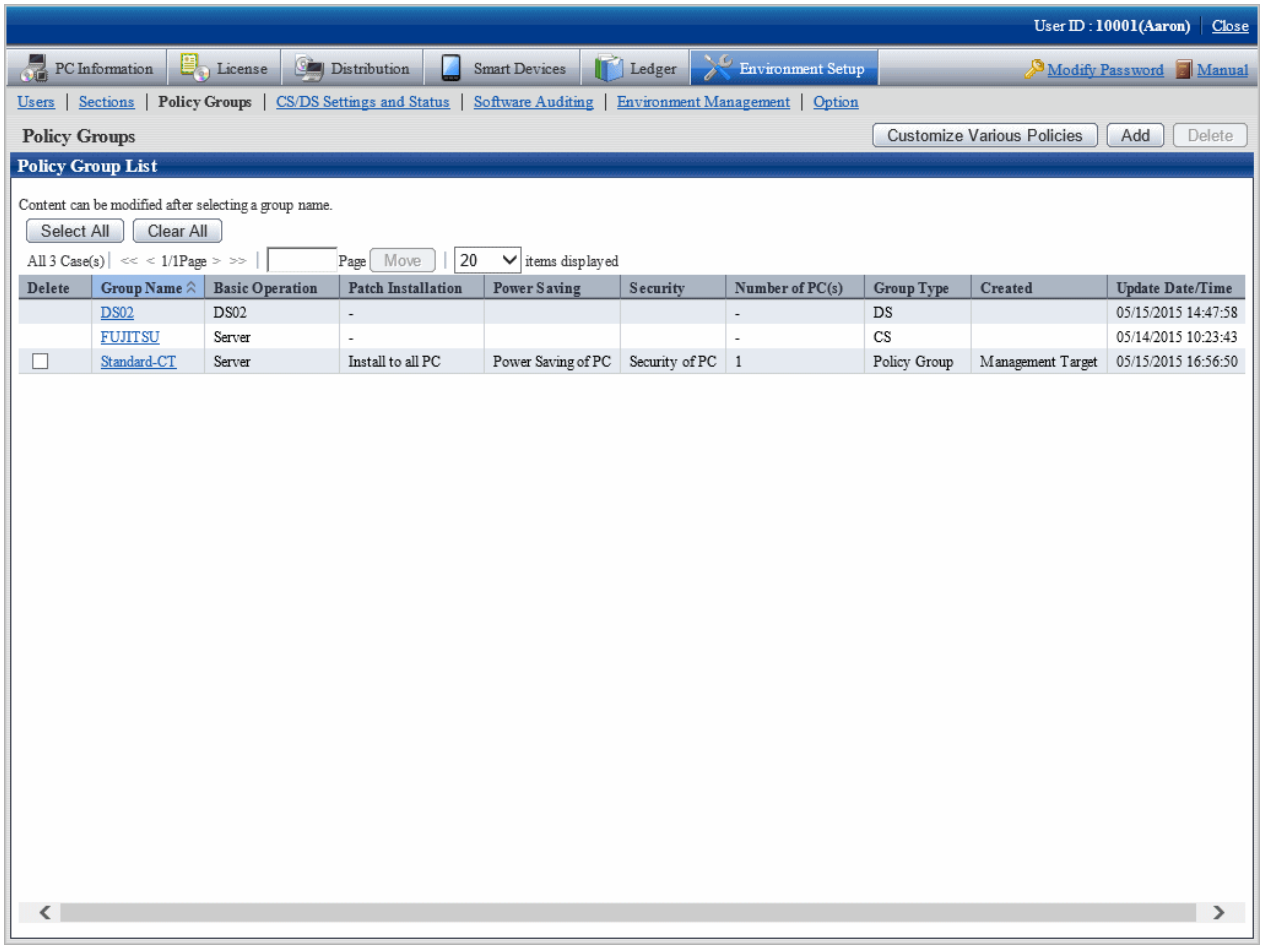
The procedure is as follows.

1. Log on to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

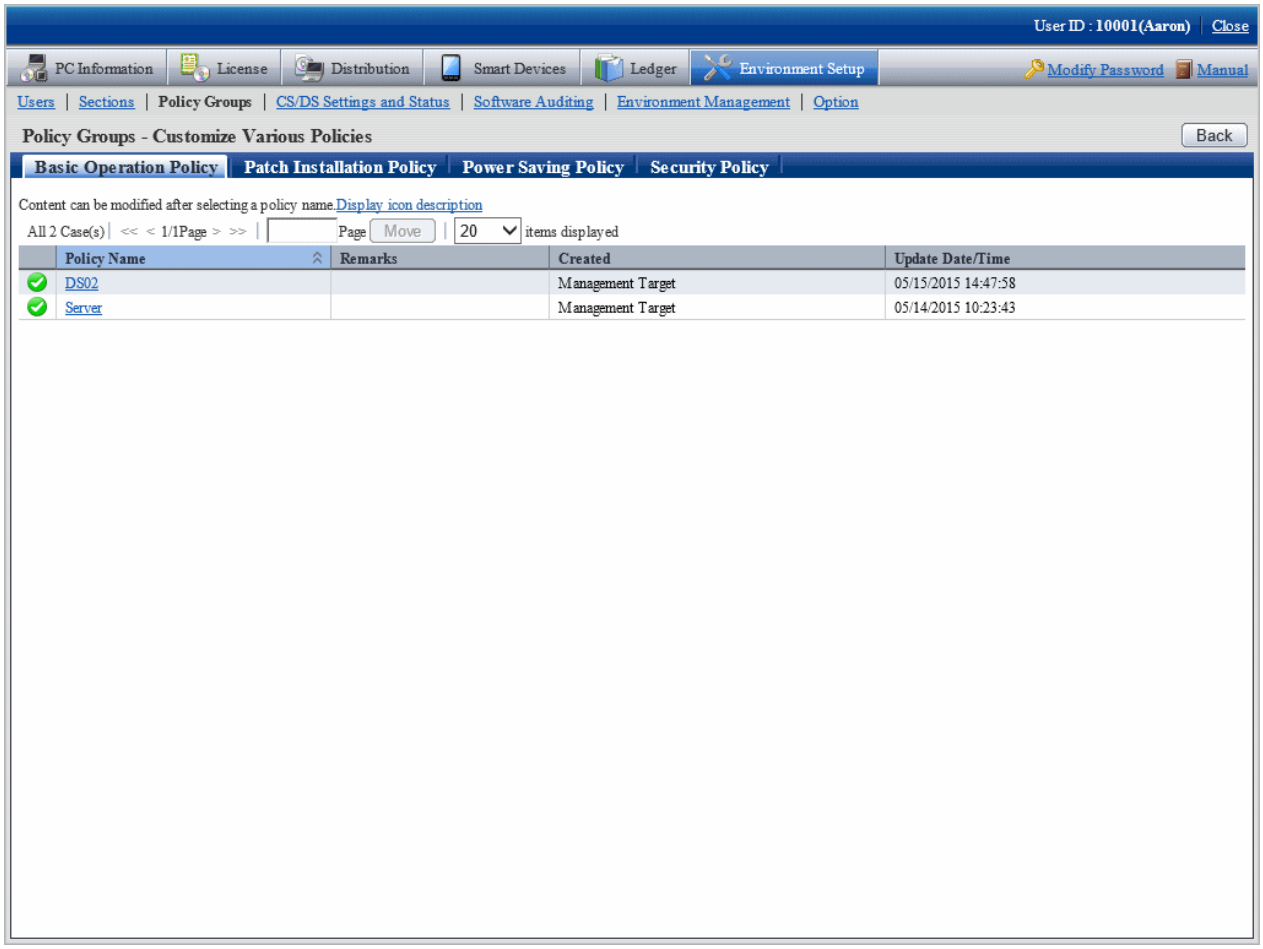
2. Click **Policy Groups**.

   The following window will be displayed.



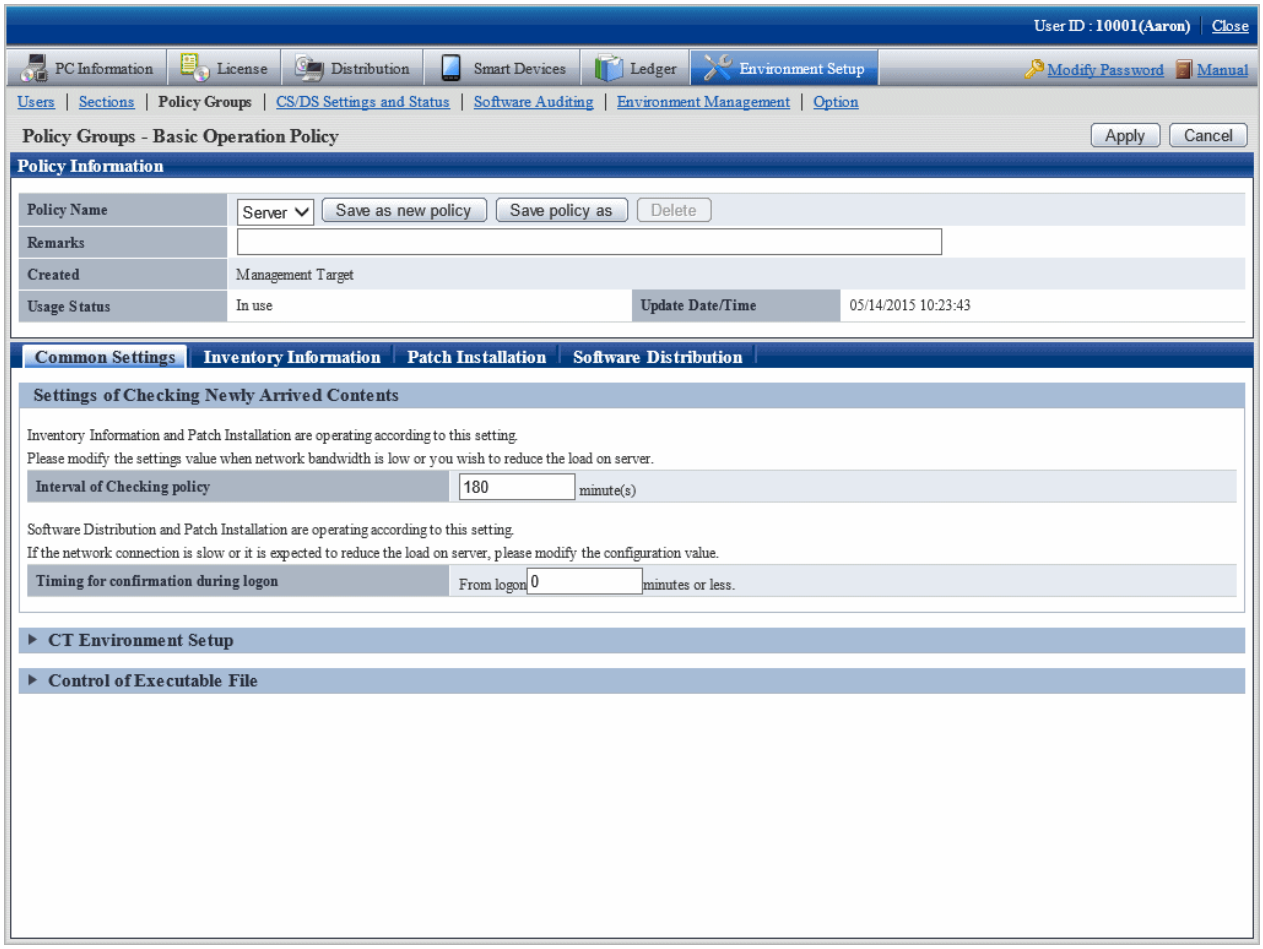
3. Click **Customize Various Policies** button.

   The following window will be displayed.



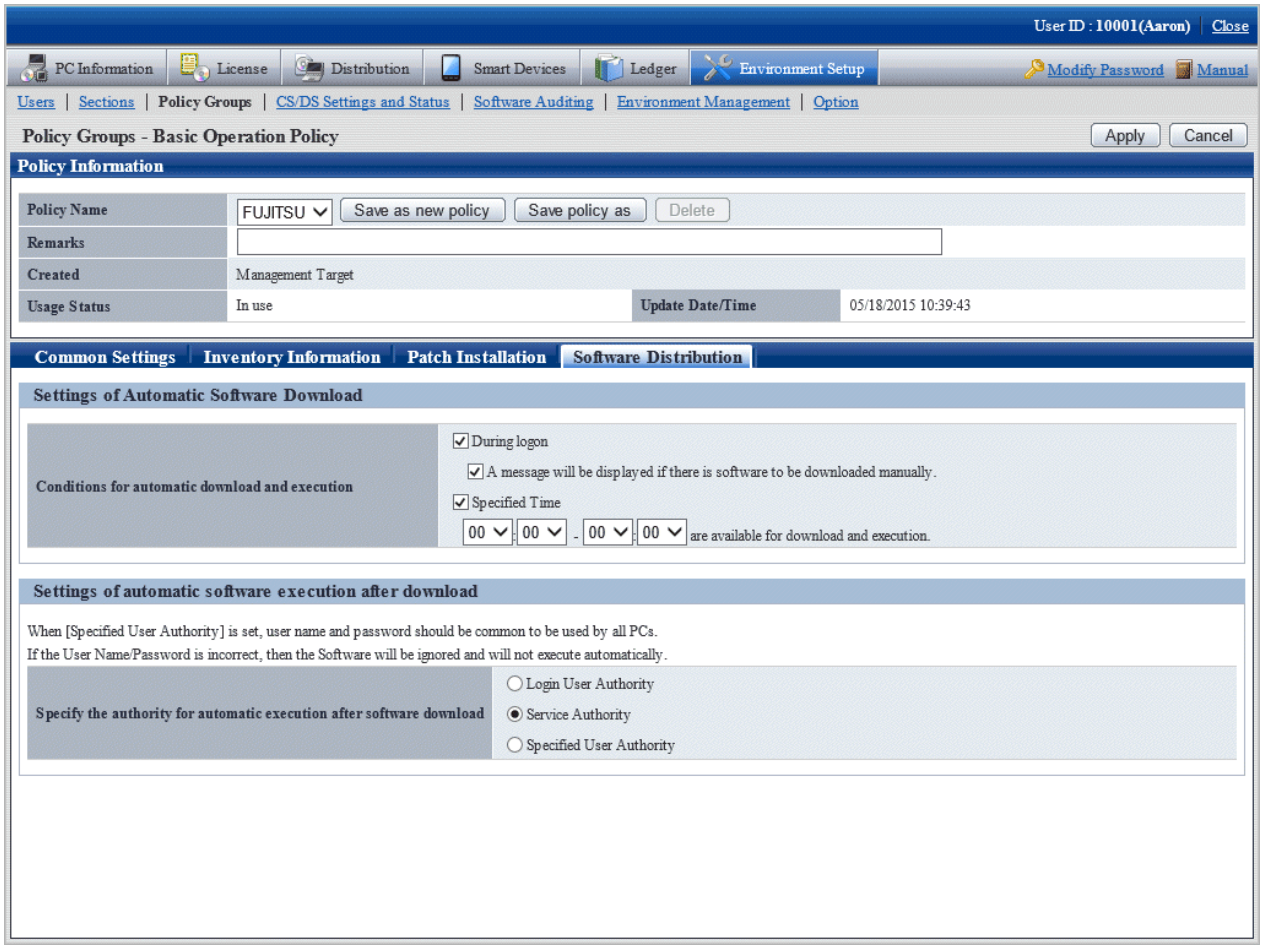
4. Click the link of policy name of the **Basic Operation Policy** tab.

   The following window will be displayed.



5. Click the **Software Distribution** tab.

   The following window will be displayed.



   Set the following items.

Item	Description
Conditions for automatic download and execution	- When set as **During logon**, confirm if there is any new software registered when logging on Windows. In addition, finish the following setup. - A message will be displayed if there is software to be downloaded manually. See below for the confirmation message displayed when there is manual software newly registered. **New software arrival. Display the software download window?** Confirmation message won't be displayed in case of automatic download. Display when there is new software for manual download. - Set as **Specified Time**, each CT starts software download for one round at any time point in the time frame specified. After the download starts, even the given time is surpassed, the download will continue till completion. The download will stop whenever an error occurs during download and will start again at the next time point. Confirm new arrival of software and software package in new arrival confirmation.

Item	Description
	In addition, confirmation of only one time carried out for new software arrival on CT. In case of reconfirmation of new software arrival, log on software again is necessary under the following circumstances or when the operation is ongoing. - Failed to download software - Software download window initiated
Specify the authority for automatic execution after software download	Specify limits of authority of automatic execution after software download - Logon User Authority - Service Authority - Specified User Authority - User ID: Specify with single-byte alphanumeric characters and characters within 256 characters. Value composed wholly of single-byte blank space not allowed. No need to specify domain name. Automatic execution will proceed according to user environment of Windows registered(log on domain, log on this time). - Password: Specify with single-byte alphanumeric characters and characters within 256 characters.

Note

- Automatic software download is based on the setup of **Specify the authority for automatic execution after software download**, perform the following operations.

  - Authority of service

    No window will be displayed on CT, software will be specified automatically.

  - Authority of logon user, specified limits of authority of user

    Software of this kind of authority will be downloaded automatically under the following circumstances.

    - When logging on Windows

    - PC standby this day, when resuming from standby the next day

    - When opening the software download window

    - User logged on Windows existing at the specified moment

    Automatic download will not proceed if there is no user logged on Windows at the specified moment.

    In addition, if there are users logged on Windows at the specified moment, dialog box of **Start software download** will be displayed once at the very beginning.

    After replay to message of the dialog box, software of **Logon User Authority** and **Specified User Authority** will be totally executed.

    In case of no replay to dialog box and no operation, the dialog box will be automatically closed and download canceled when the specified moment is up.

    In execution of the specified moment, unlike the software execution of logon Windows, the user won't necessarily see the window. Therefore, to prevent the user from executing the software without seeing the window, it's necessary to display the dialog box again when the executed software is displaying the window all the time while it has stopped half way.

- When setting **Service Authority** or **Specified User Authority** in **Specify the authority for automatic execution after software download**, as the needed limits of authority have been changed during software execution, it won't be possible to visit the network driver.

- When setting **Specified User Authority** in **Specify the authority for automatic execution after software download**, specify the user name with password in the specified **User name** textbox. When the user name with password setup is specified, it won't be possible to release and install software.
- For selection of multiple choice box of **A message will be displayed if there is software to be downloaded manually**, log on Windows, the notice dialog box will be displayed when the higher server has registered new software. Security patches installation won't be possible during display of the notice dialog box.

  Therefore, it's recommended not to select the multiple choice box of **A message will be displayed if there is software to be downloaded manually** when it's the unmanned PC to which the CT is imported.
- Set **Specified User Authority** in **Specify the authority for automatic execution after software download**, when referring to/updating the software of fixed information of the logging user, sometimes the execution will fail because that logging user is different from the executing user.
- It's the logging user's limits of authority when the download and execution is done from the software download window. Set with CustomPolicy.exe(policy change to user setup) when the limits of authority set on policy is used for execution.

6. Click the **Apply** button.

   Conditions of software distribution will be set.

8.2.3 Register Software Distribution to be Released

Log the software and file and other data on CS in the manner of software release. The logging software can be distributed to DS or CT.

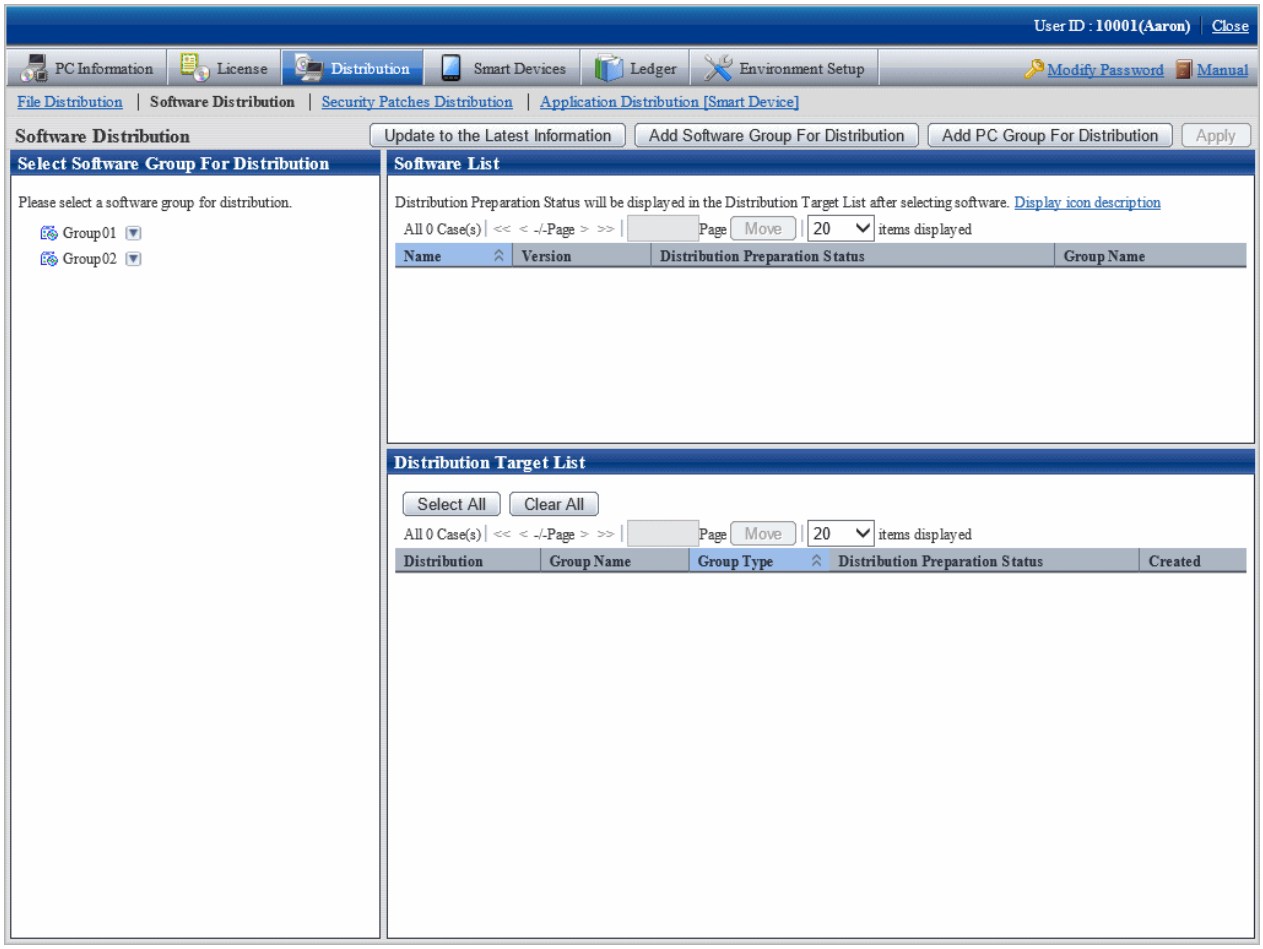
As to notes about software release to PC with Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012, refer to relevant contents of "8.2.3.1 Notes of Software Distribution to PC with Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012"

Register the software to be distributed.

The procedure is as follows.

1. Log on to the main menu, click **Distribution**, then click **Software Distribution**.

   The following window will be displayed.

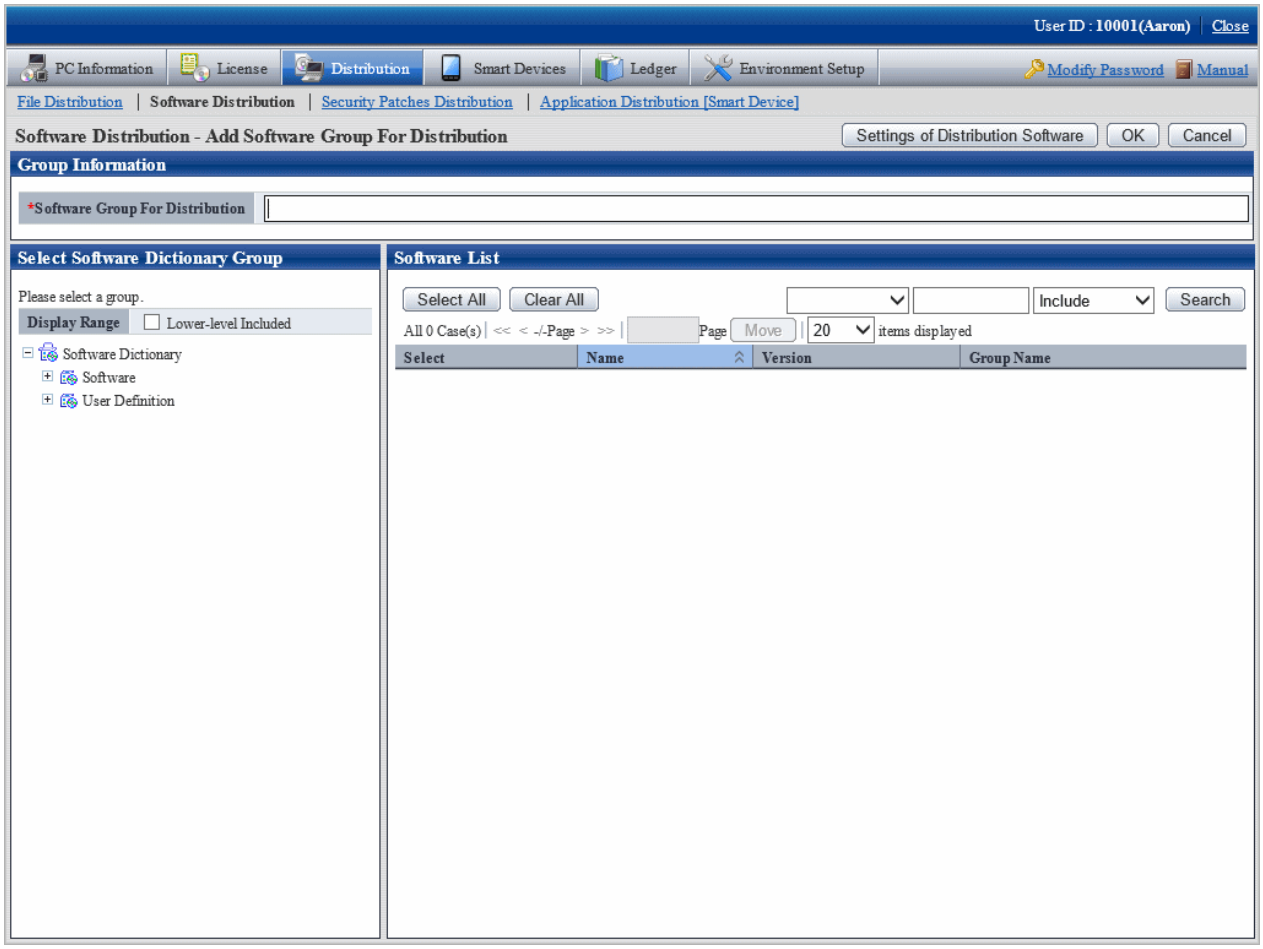


   See below for definition of the button names.

Button Name	Description
Update to the Latest Information button	Refresh to latest information
Add Software Group For Distribution button	Create software group to be distributed.
Add PC Group For Distribution button	Create of PC group for distribution.
Apply button	Save the state selected.

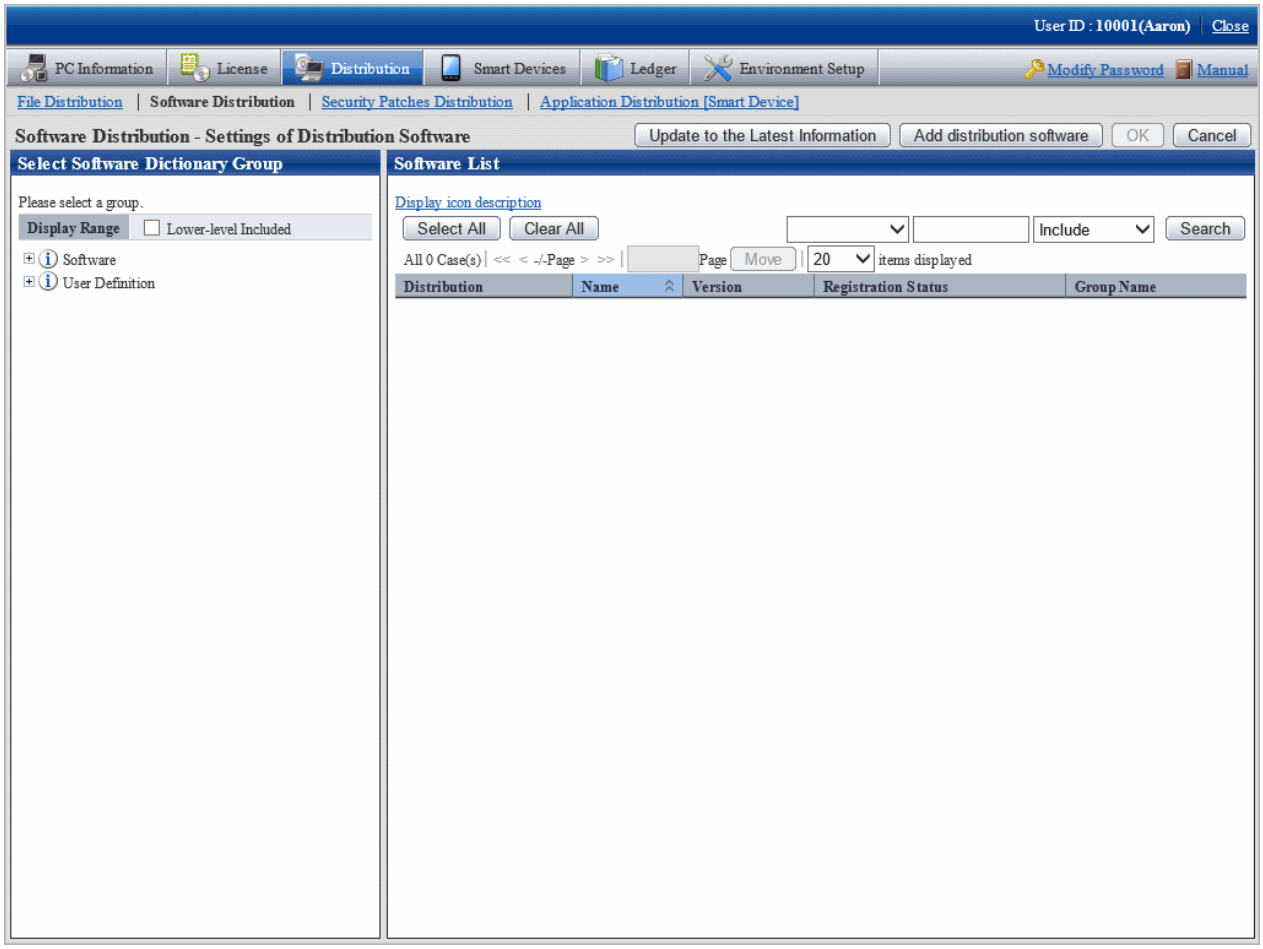
2. Click the **Add Software Group For Distribution** button.

   The following window will be displayed.



3. Click the **Settings of Distribution Software** button.

   The following window will be displayed.

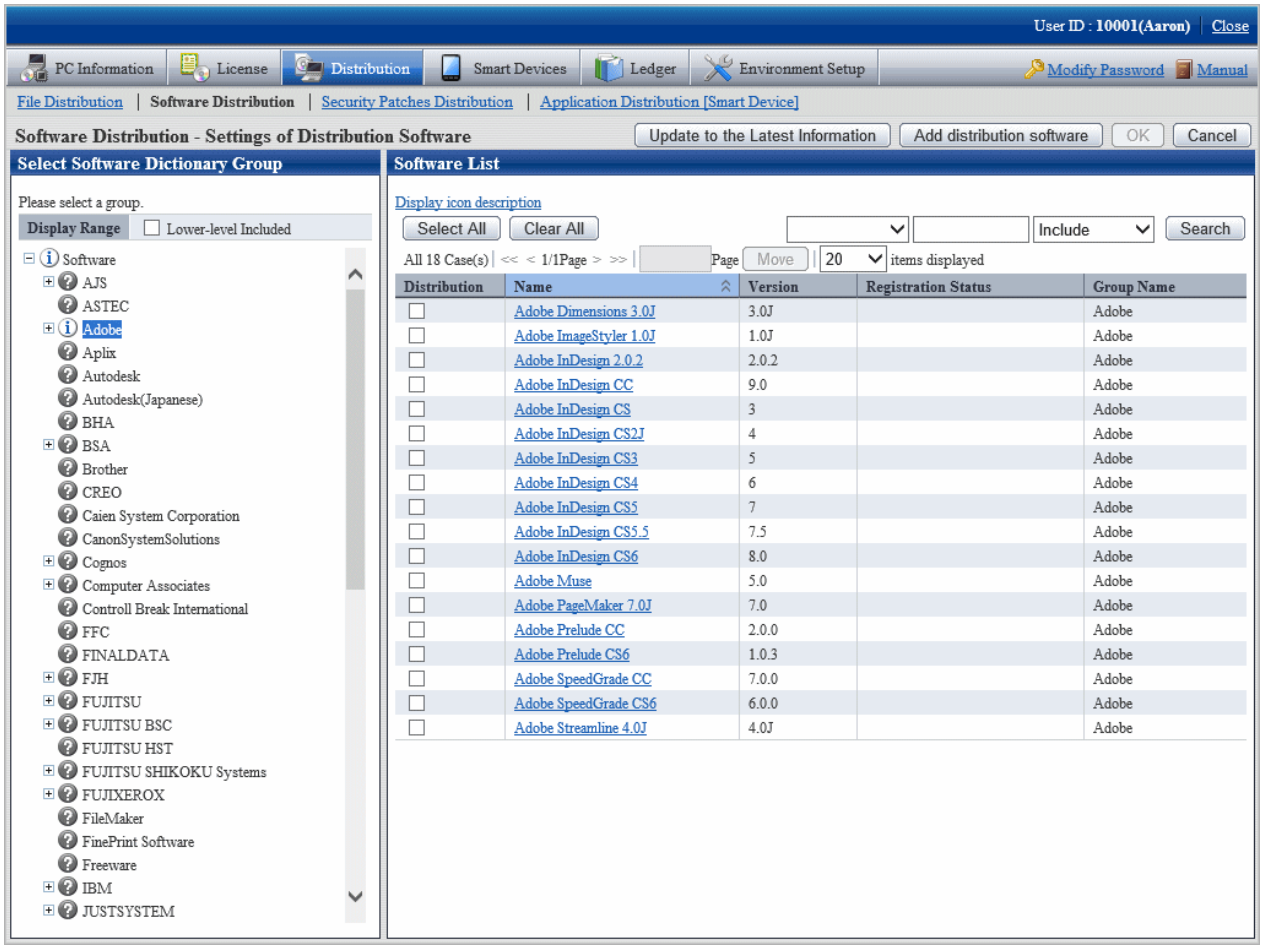


   The actions of each button are as follows.

Button name	Description
Update to the Latest Information button	Update to the latest information.
OK button	Save the specified settings.
Cancel button	Give up the specified settings.

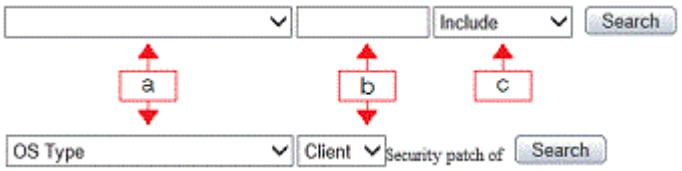
4. Select the directory under **Software** from the field on the left of the window.

   The selected software will be displayed in the field on the right of the window.



See below for explanation about the software list.

Item	Description

Search button	The display contents of the software list will be displayed accurately.
	 
	Select the object to be accurately displayed in "a". The selected objects are the respective project name, **OS name** and **OS type**. In addition, specify OS type only under the circumstances of security patches.
	Specify the conditions set in "a" of accurate display in "b" and "c".
	- When respective project name is selected in "a" or **OS name** is selected
	  - Character string of accurate display conditions is specified in "b". The character string can be specified as partially consistent.
	  In addition, if "a" is **OS name**, specify a character string excluding **Windows** or Edition in "b". (Even with designation of **Windows** and Edition won't narrow down the searching range)

Item	Description
	- Select **Including** or **Included** in "c". - When **OS type** is selected in "a" Select **Client end** or **Server** in "b".
Registration status	Logon status of software on CS can be grasped. : Registration completed : In Registration : Registration failed. (Note) Without icon, means software not registered.

Note: "Table 8.1 Message of registration status/distribution preparation status of software distribution" will be displayed.

Table 8.1 Message of registration status/distribution preparation status of software distribution

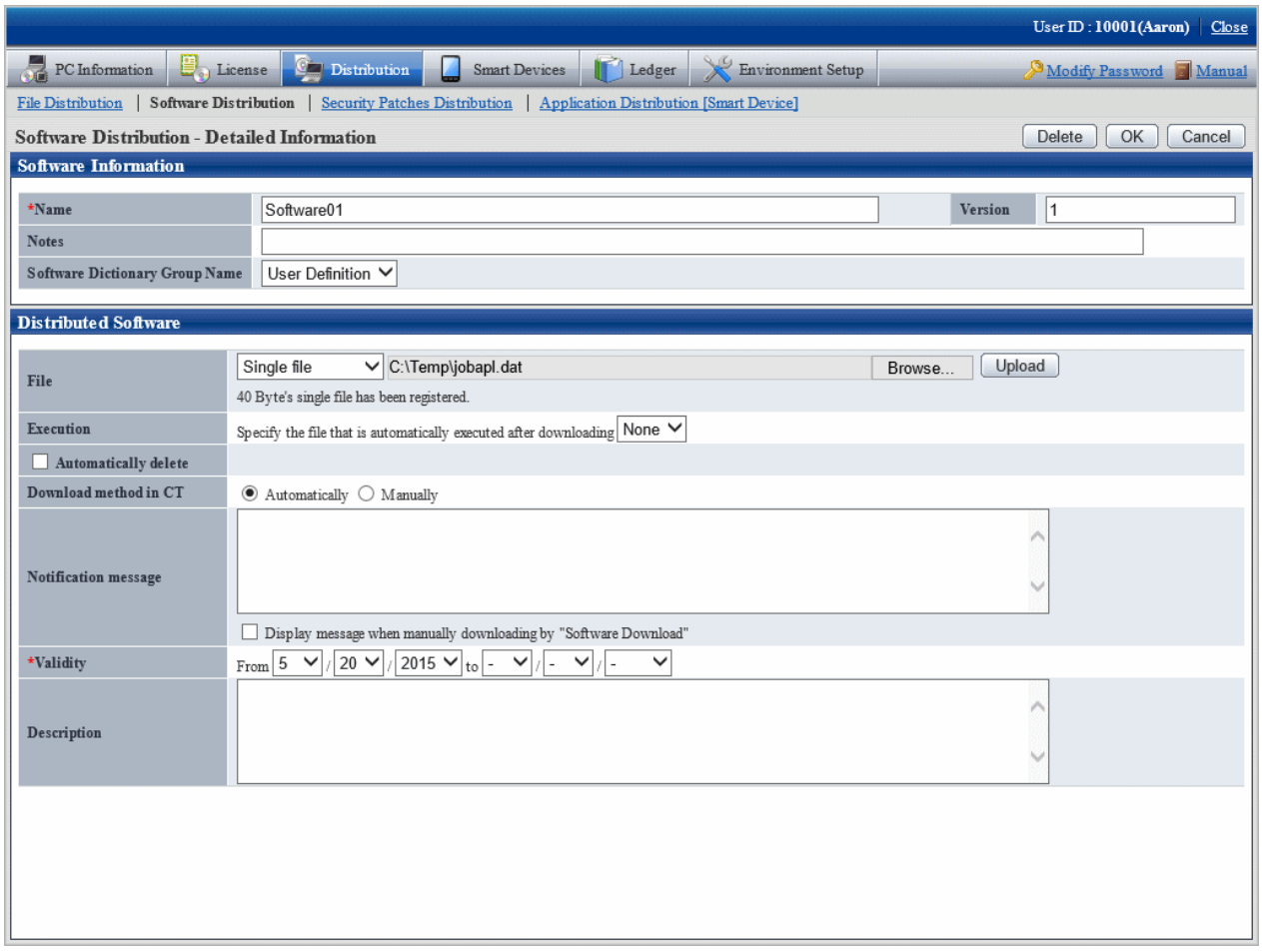
Measure	Description	Processing
canceled by service stopped	Registration processing was interrupted due to service stop	Register software again after deleting the error software.
failed to download software	Failed to download software on DS	Confirm the following contents on DS. - If there is sufficient remaining disk space of the directory specified in "Directory of saving software" (Note) - Is there any errors of disk volume If the problems stay after confirmation of the above, collect the log and contact the technicians.
failed to get software information from database	Failed to get software information from database, or failed to get software release object information from database	Confirm the following contents on CS. - Symfoware service initiated or not - System virtual memory sufficient or not - System in high load state or not - Disk volume mistaken or not After confirmation of the above, operate again from main menu. If the problems stay, collect the log and contact the technicians.
failed to register software	Failed to register software or download package	Confirm the following contents on DS. - Sufficient remaining space or not for disk where the specified directory belongs to in "Saving software directory"(Note) - Disk volume mistaken or not If the problems stay after confirmation of the above, collect the log and contact the technicians.
failed to store a software	Failed to store a software	Confirm the following contents on CS/DS. - Sufficient remaining space or not for disk where the specified directory

Measure	Description	Processing
		belongs to in "Saving software directory"(Note) - Disk volume mistaken or not If the problems stay after confirmation of the above, collect the log and contact the technicians.
upload file is not found	Upload file is not found	Confirm the following contents on CS/DS. - Software uploaded from main menu or not - Sufficient remaining space or not for disk where the specified directory belongs to in "Saving software directory"(Note) - Disk volume is mistaken or not After confirmation of the above, operate again from main menu. If the problem remains, collect the log and contact the technicians.

Note) Confirm with CustomPolicy.exe(policy change to user setup) for "Saving software directory".

5. Click the link of the software name to set the detailed information.

   The following window will be displayed.



6. Define the following information.

Software information

This item can only be set in the case of user defined software.

Item	Description
Name	For name of software to be distributed, enter up to 128 fullwidth characters or 256 halfwidth characters. This item cannot be omitted.
Version	Specify content using up to 32 fullwidth characters or 64 halfwidth characters for version.
Notes	Enter Remarks. Enter content within 128 multi-byte or 256 single-byte characters. (*1)
Software Dictionary Group Name	Select software dictionary group name to be added from the user definition.

*1: After you upgrade from V13.3.0 or earlier to V14.0.0 or later, information about the **Version** that was used in V13.3.0 or earlier is set in **Remarks** under **Software Information** in the distribution software settings.

Distributed Software

Item	Description
File (Note 1) (Note 3)	Register the software to be distributed. - Single file Designation of logon file. Specify here for logon one file. - Compressed file To be specified when logging on the compressed file. The registered compressed file will be automatically decompressed on CT. Specify the specified file in the list in the input field beside the list. Select **Compressed file** in the list, log on the server, check to see if the extension name is **Zip**. In addition, zip file with password protection cannot be registered. Click **Upload** button, the specified file will be registered the server. Click **Delete** button, the software registered will be canceled from the server. In the logon state, specify file again, click **Upload** button, then the logon will be covered.
Execution (Note 2)	After release, specify a file when you want to execute a file. - Specify the file that is automatically executed after downloading The executable file in the ones registered the server will be showed in the list. The files identified as executable have the following extension names. "exe", "bat", "msi", "vbs", "wsf" "No" will be displayed when there are no executable files or just after logon. In file execution after release, select the executable file, then set the following items. - Time needed for file execution from start to end. In file execution after release, select a value in 0-600 in unit of second for start to end of the specified file. Default input not allowed. - Space needed for execution(installation)

Item	Description
	For disk space needed for execution of the specified file after release, input a value within 30 digits(Unit: K characters). Specify an estimate value for software download on CT in this item.
Automatically delete	After software download on CT, select this item for automatic cancellation of the downloaded software. Set a value in 1-366(days) for how soon the software will be canceled after download. Default input of date is not allowed for automatic cancellation.
Download method in CT	Select if it's necessary to automatically download the software to be registered CT. - Automatically Automatic software download to CT - Manually Manual software download to CT
Notification message	Message displayed when CT is downloading software, designation of up to 2,048 fullwidth characters or 4,096 halfwidth characters. Using the software download window, the message can be displayed when downloading the selected software. No message will be displayed for automatic download.
Validity	Designation for checking/downloading software on CT to be limited in given time. The default start time is the date of software logon. Default input of start time is not allowed.
Description	For reference to the software attribution information when downloading on CT, input the information using up to 512 fullwidth characters or 1,024 halfwidth characters. Function, usage, software logon and other information can be input(file registered, file executed after download), attached information to software.

Note 1)

- For the registered software file/folder attribution(read only and etc), it cannot be maintained after distributed. Set the attribution again after download when it's needed to set file/folder attribution.
- 0 byte will be uploaded to upload the file in use. Be of 0 byte or not of the original file, when it shows 0 byte after upload, stop using the file and then upload.
- Don't upload file over 2GB. After upload, the browser won't be able to work.

Note 2)

- Saving directory of **Specify the file that is automatically executed after downloading**, when the release target is CS or DS, specify the **Saving software directory** in installation of CS or DS. When the distribution target is CT and in the case of **Automatically** for **Download method in CT**, it's <DTP installation directory>/contents directory. The Current directory of the software distribution will be set as target directory for software saving.
- The executable procedure in **Specify the file that is automatically executed after downloading** is for 32bit use. Whether it is 32bit or 64bit version for the distribution target of Windows, all startup will be done as per 32bit version without discrimination. The procedures initiated in **Specify the file that is automatically executed after downloading** shall be discriminated for the 64bit version.

Note 3)

Select **Compressed file**, considering the following in execution after distribution.

The folders shown in the following cases are Current ones in software execution on CT. therefore, finish the following record when executing EXE file from the package file.

- Example 1)

  <Structure of zip file>

  Excluding file folder compressed file.

  x.bat

  y.exe

  <Execution environment on CT>

  - After decompression

    <Target directory for software storage>\<Software name>_<Version> \x.bat

    < Target directory for software storage >\< Software name >_< Version >\y.exe

  - Current folder

    < Target directory for software storage >\< Software name >_< Version >

  < Example of recording patch file>

  y.exe

- **Example 2)**

  < Compositions of zip file >

  Excluding file folder compressed file.

  FolderA\x.bat

  FolderA\y.exe

  < Execution environment on CT >

  - After decompression

    < Target directory for software storage >\< Software name >_< Version >\FolderA\x.bat

    < Target directory for software storage >\< Software name >_< Version >\FolderA\y.exe

  - After decompression

    < Target directory for software storage >\< Software name >_< Version >

  < Example of recording patch package file >

  .\FolderA\y.exe

7. Click the **OK** button, saving the software registered.

   The allocation information shall be reflected to CS in the case of software distribution according to the allocated License. Information on license allocation is reflected in CS when you click **Start** > **Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Event Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Event Settings** for CS.

Steps to register again when registration failed

Take the following steps on CS if registration failure has been caused due to insufficient remaining disk space when registering the software from the main menu.

1. Make sure of sufficient remaining space needed for software registration.
2. Stop the ITBudgetMGR(INV) service.
3. Start the ITBudgetMGR(INV) service.
4. Register the software again from main menu.

8.2.3.1 Notes of Software Distribution to PC with Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012

According to different registered software, pay attentions to the following notes about automatic software download from PC with Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012.

- Make sure the programs of distribution/installation software are supported by Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012. If errors occur during software execution, the program will be considered as unable to execute on Windows Vista(R),, Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012. Confirm specifications of the software to be distributed.
- The upgrade window of authority(UAC) will be displayed when "setup" or "patch" is included in name of the procedures for software execution.
- Sometimes the upgrade window of authority(UAC) will be displayed when the specified user's authority are used for software execution. Use the service authority for software execution.
- When executing software with service authority and performing window display, the service "Interactive Services Detection" of Windows should be started.
- Operate when creating software without displaying window or restarting services.

8.2.4 Settings of Distribution Target

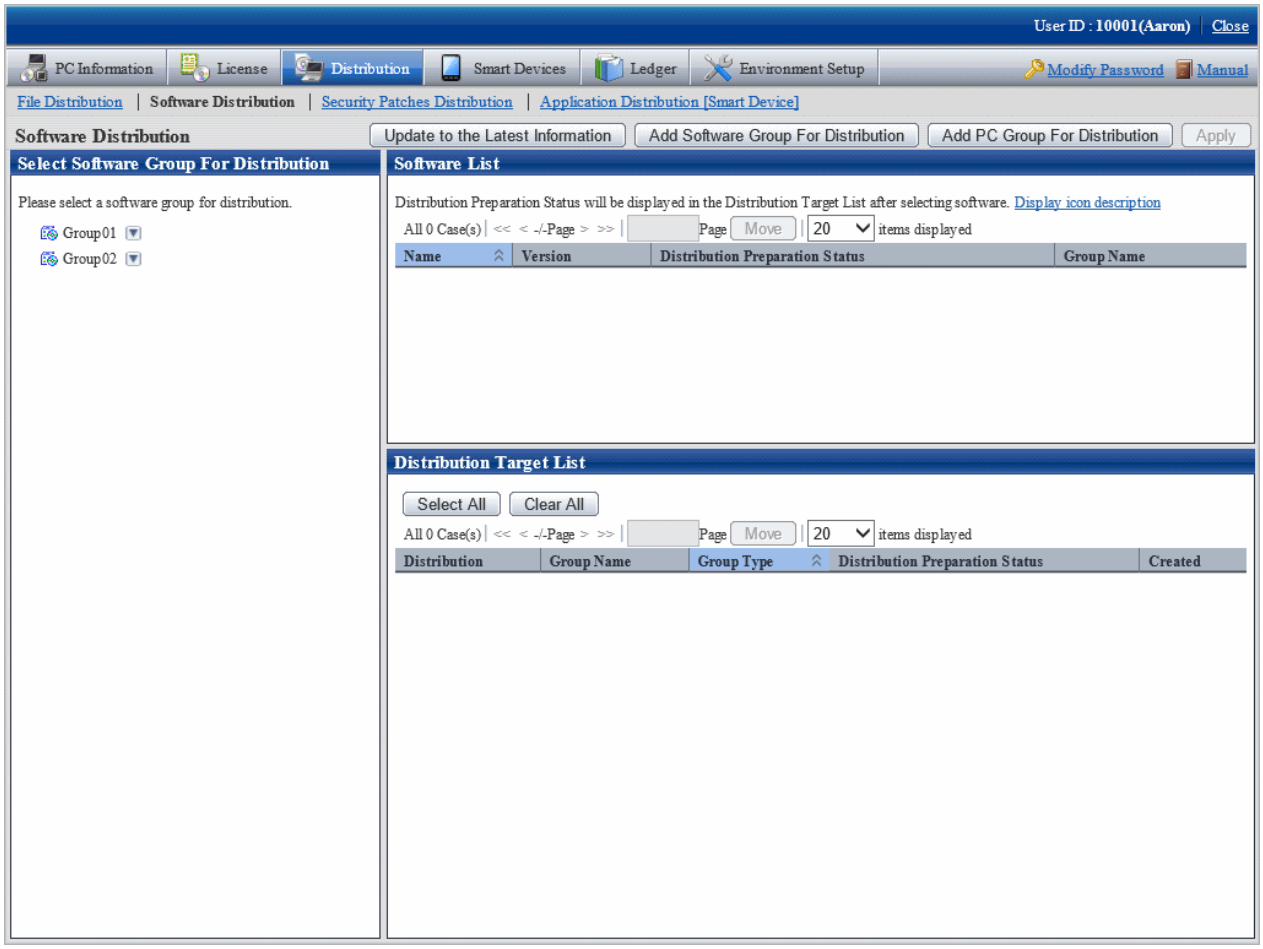
Set the software distribution target.

1. Create software Distribution Group
2. Create PC group for distribution
3. Connect the software group for distribution to the distribution target

The procedure is as follows.

1. Log on to the main menu, click **Distribution**, and then click **Software Distribution**.

   The following window will be displayed.



   See below for definition of each button in the window.

Button name	Description
Update to the Latest Information button	Update to the latest information of distribution preparation.
Add Software Group For Distribution button	Create software group to be distributed.
Add PC Group For Distribution button	Create PC group for distribution.
Apply button	Save the message that is displayed currently.

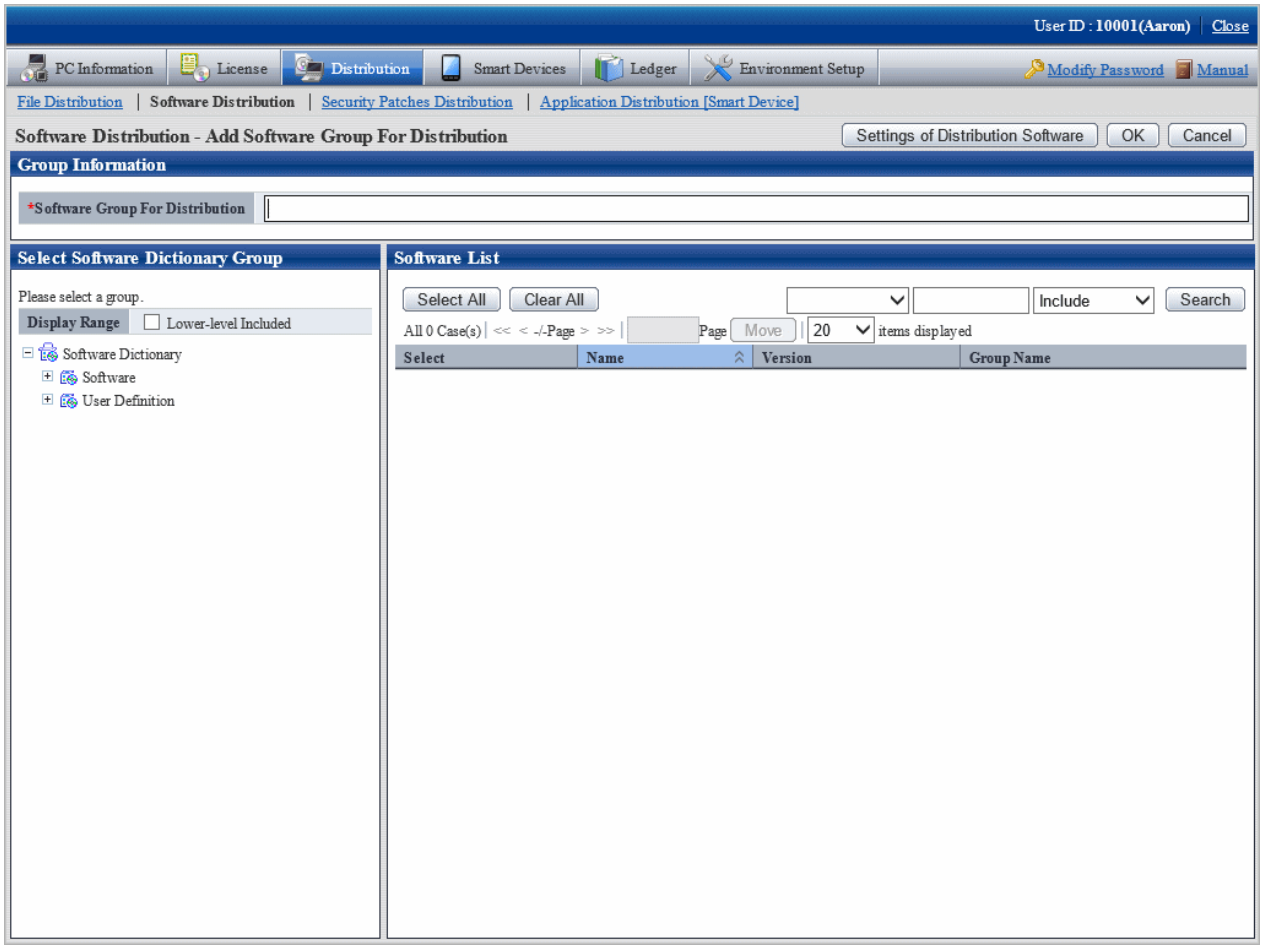
Add software group for distribution

Add software group for distribution.

The procedure is as follows.

1. Click **Add Software Group For Distribution** button in window of **Software Distribution**.

   The following window will be displayed.

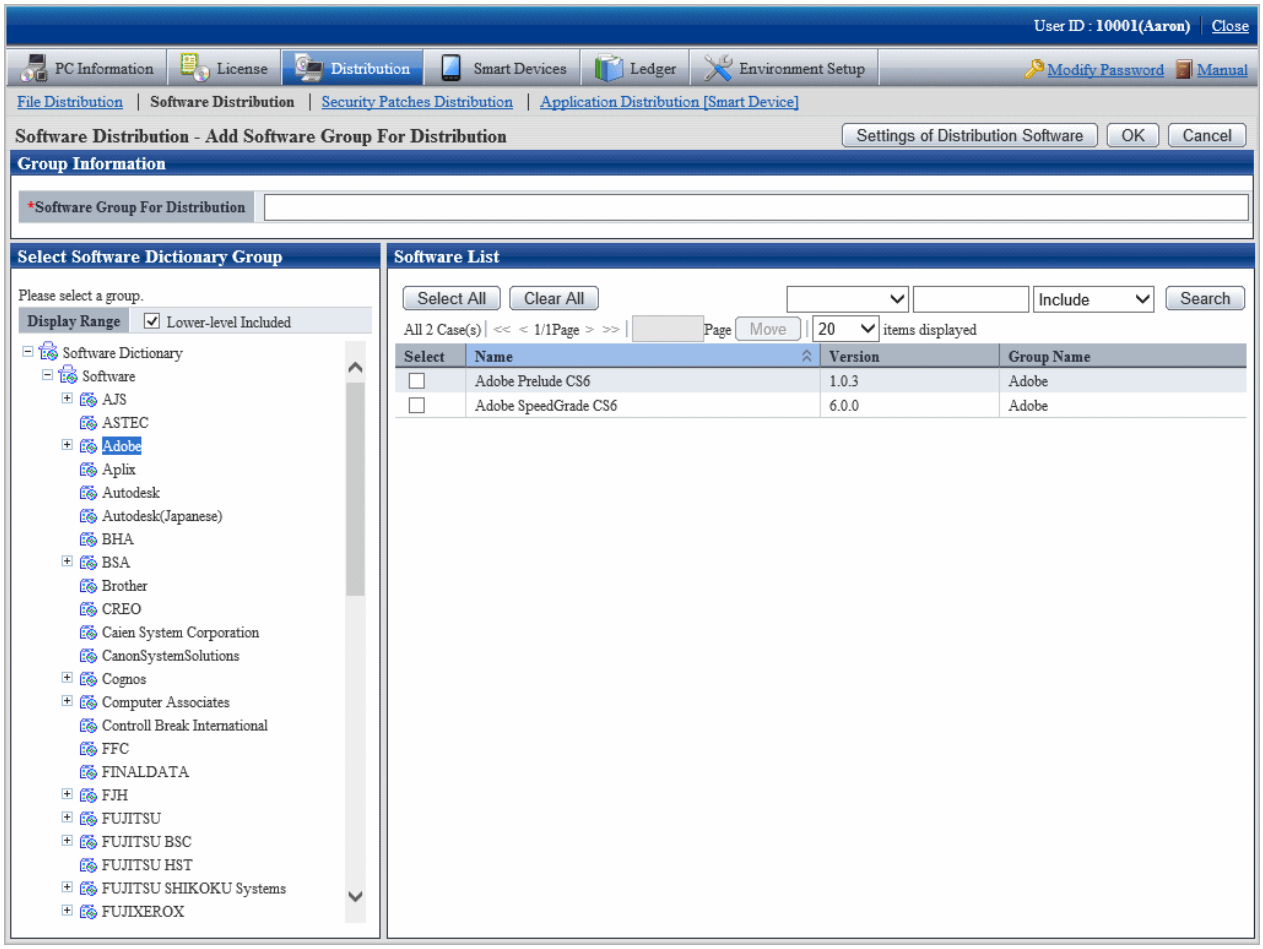


2. Input the following information.

Item	Description
Software Group For Distribution	Specify the name of software group for distribution. Maximum entry of the group name shall be 30 multi-byte or 60 single-byte characters. The specified characters shall be alphanumeric characters and the following single-byte symbols. ("-" "@" "." "(" ")" "[" "]" "{" "}" "<" ">" ":" ";")

3. Select software from the tree in the field on the left of the window.

   List of software will be displayed in the field on the right of the window.



4. Select software in the software group to be distributed for log on, click the **OK** button.

Point

Modify and delete software group for distribution

After addition of name of the software group for distribution, take the following steps to modify and delete the software group for distribution.

1. After addition of name of the software group for distribution, the software group for distribution will be display in **Select software group for distribution** in bottom left corner in the window. Move the cursor to in the field on the right to the software group name for distribution, the options of **Change** and **Delete** will be displayed.

   - **Modify**: select this option to modify the name of the software group for distribution, or just modify and delete the software registered the software group for distribution.

   - **Delete**: select this option to delete the software group for distribution.

2. After the setting has finished, click the **OK** button to finish.

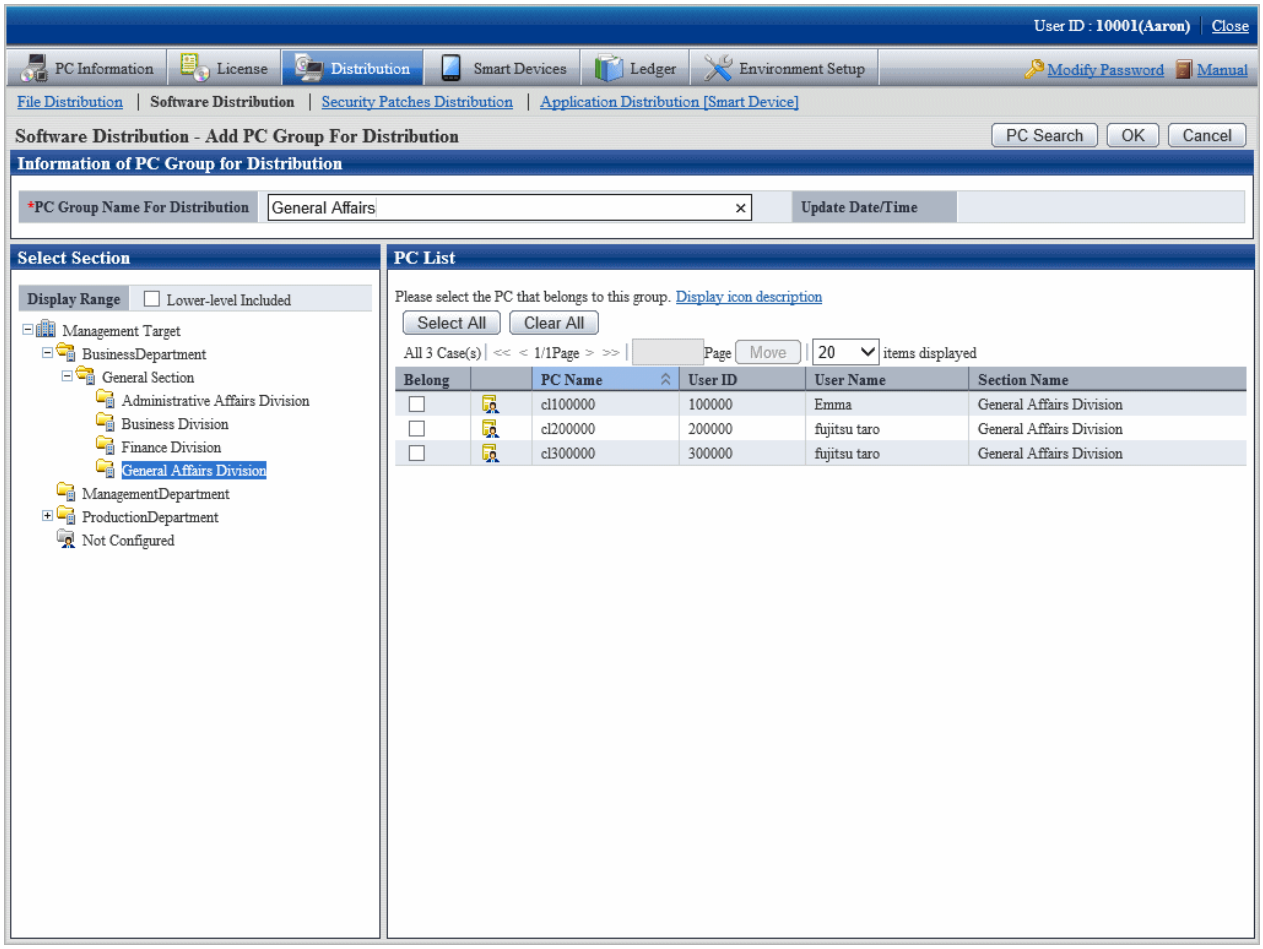
Add PC group for distribution

Select the PC of the software distribution target to perform group operations.

The procedure is as follows.

1. Click **Add PC Group For Distribution** in the **Software Distribution** window.

   The following window will be displayed.



   See below for definition of each button in the window.

Button name	Operation contents
PC Search	For PC search.
OK	Save setup of the PC group specified for distribution.
Cancel	No storage of content, return to the previous window.

2. Input information of PC group for distribution.

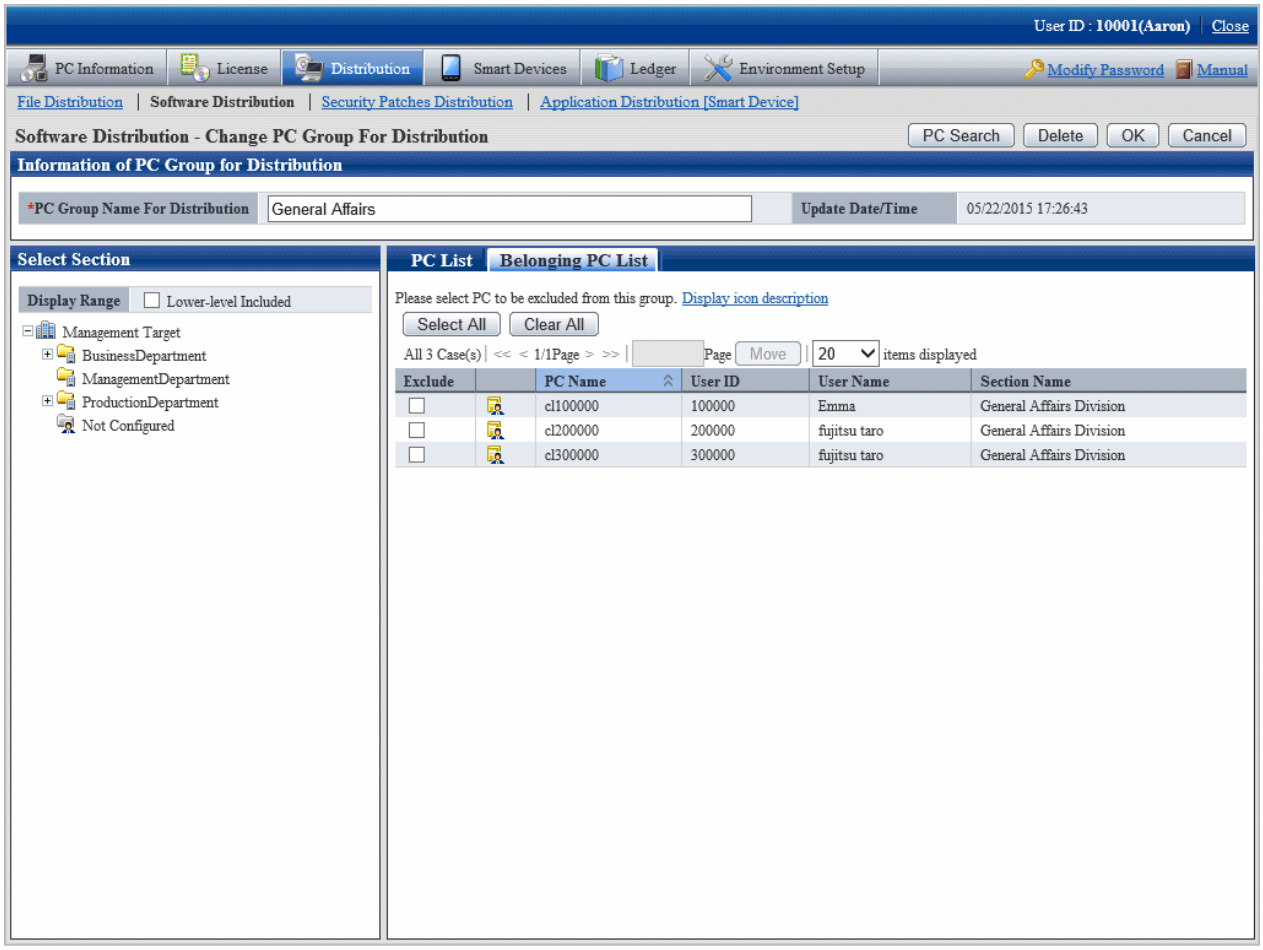
Item	Description
PC Group Name For Distribution	Divide the PC for distribution in groups and specify a name to the group. Maximum entry of the group name shall be 30 multi-byte or 60 single-byte characters. The specified characters shall be alphanumeric characters and the following single-byte symbols. "-" "@" "." "(" ")" "[" "]" "{" "}" "<" ">" ":" ";" It cannot be omitted.

3. Select the PC to be included in the PC group for distribution, click the **OK** button. But PC of CT command mode cannot be selected.

   The group will be added.

4. Select name of the PC group for distribution from **Distribution Target Lis**t to confirm the PC belongs to the PC group for distribution or change the setup content.

   The following window will be displayed.



   See below for definition of each button in the window.

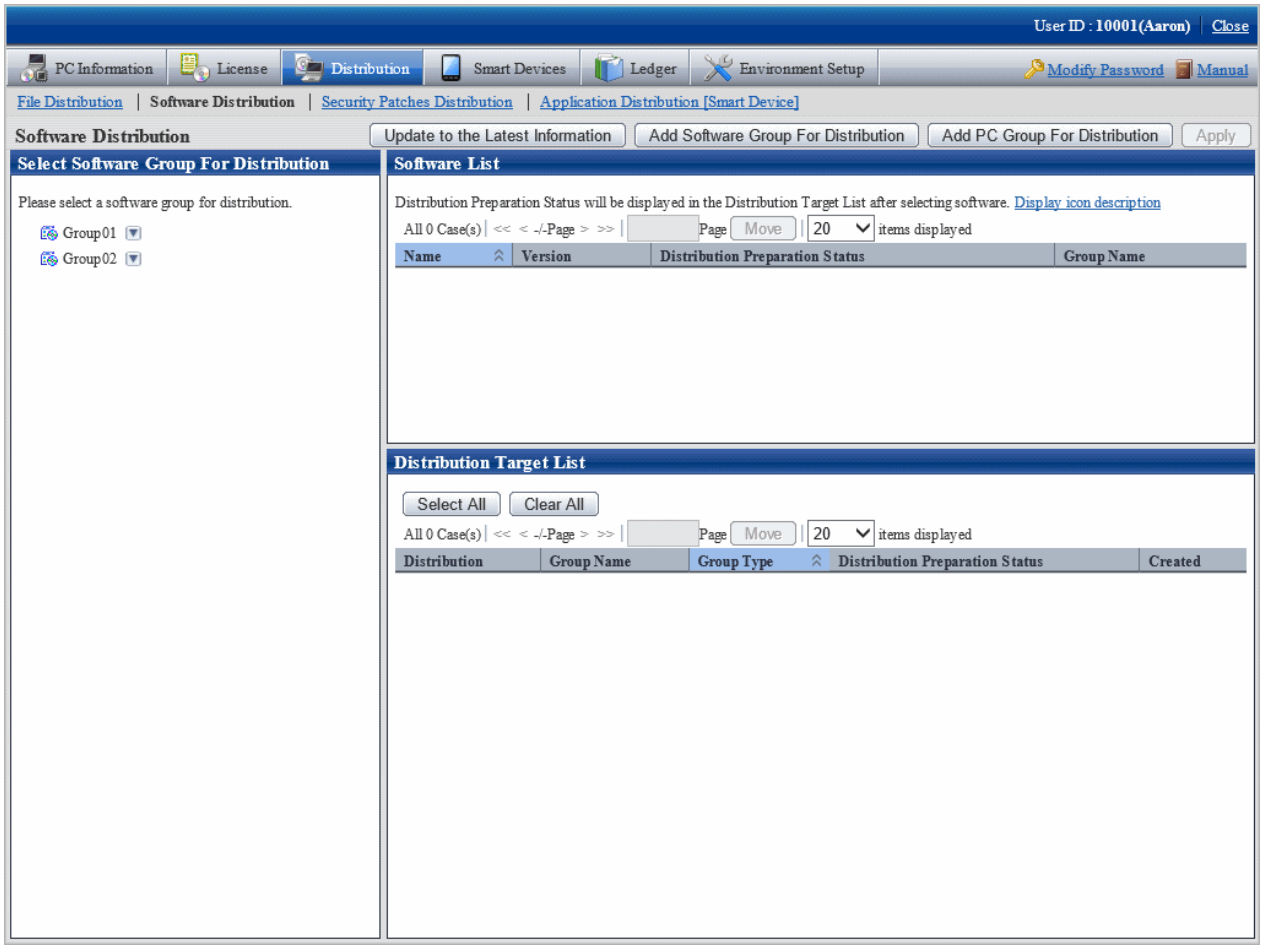
Button name	Operation content
PC Search	For PC search
Delete	Delete the specified PC group for distribution
OK	Save the setup of the PC group specified for distribution.
Cancel	No storage of the setup content, return to the previous window.

5. Change the setup content, click the **OK** button.

Connect the software suite for release to the release target

1. Select the software group to be distributed from the field on the left of the window of **Software Distribution**.

   The following window will be displayed.



2. Select CS/DS or group to be distributed from **Distribution Target List** in the field on the right of the window.

   See below for type definition of the distribution target.

Type	Description
CS	Specify this item when releasing to CT connected under CS.
DS	Specify this item when releasing to CT connected under DS.
Policy group	Specify this item when releasing to PC registered the policy group.
PC group for distribution	Specify this item when releasing to PC in the PC group logon for distribution.

3. Click **Apply** button.

8.3 Settings as Needed

Perform the following operations as needed for software distribution.

- Message display of software download

8.3.1 Message Display of Software Download

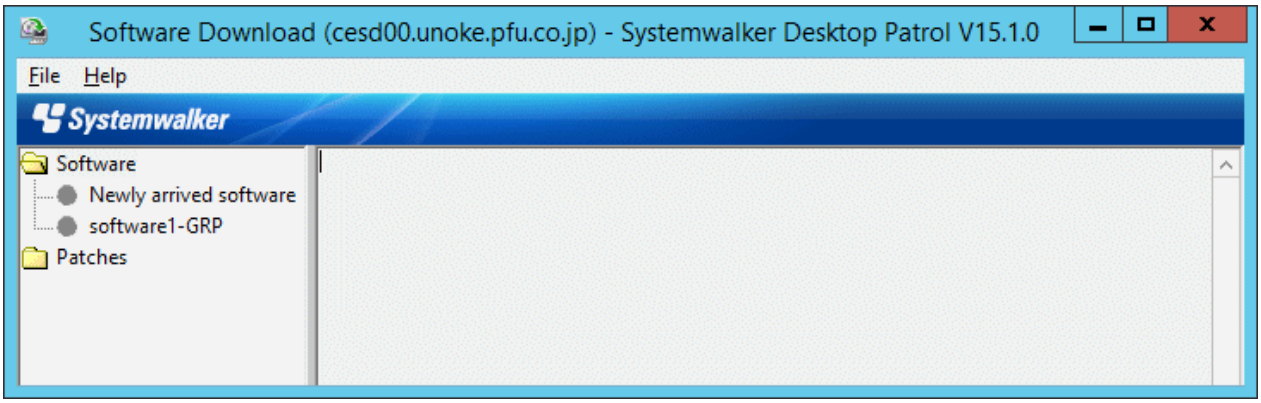
Contents including download instructions can be passed on to the client through the setup message in the **Software download** window on CT. Two kinds of information can be displayed.

- Message displayed in the software download window
- Message displayed when downloading the selected software

The following describes each message.

Message displayed in software download interface

Display the **Software Download** window on CT. Select **Software**, the message will be displayed in the field on the right of the window.



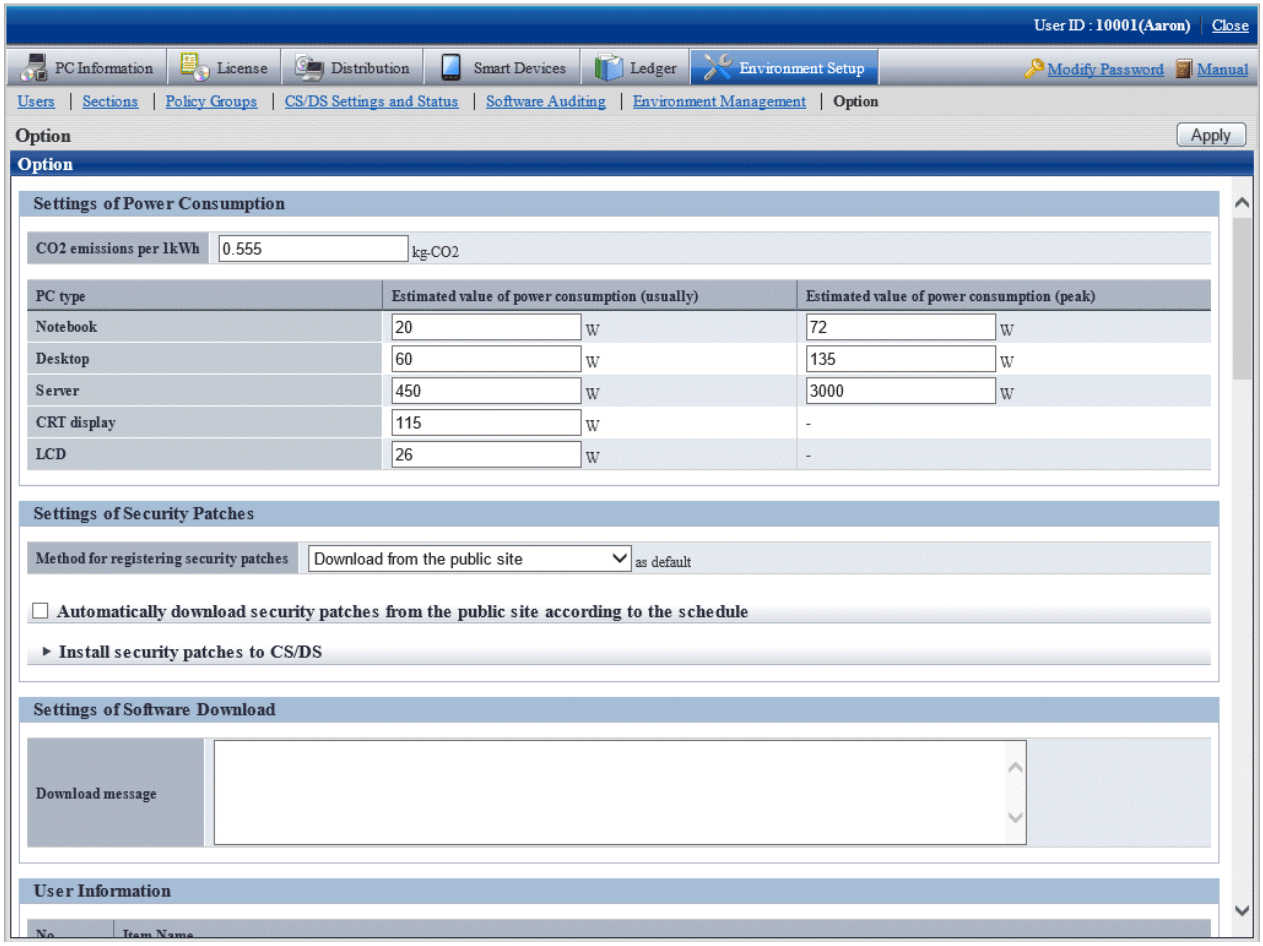
The procedure is as follows.

1. Log on to the main menu, click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **Option**.

   The following window will be displayed.



3. Enter **Download message** in **Settings of Software Download**.

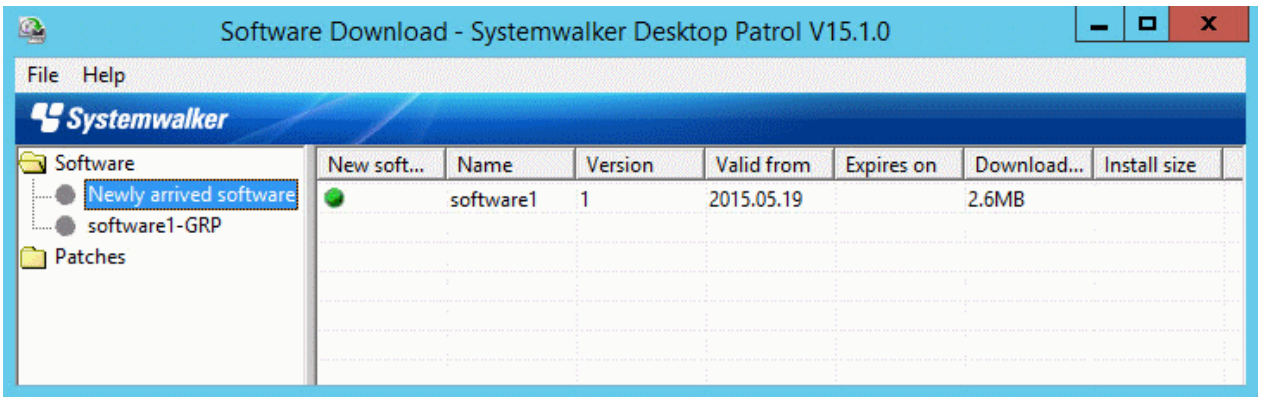
   Message will be displayed during software download on CT, contents of the message is specified to be up to 2,048 fullwidth characters or 4,096 halfwidth characters.

   Message specified here will be displayed in the software list when **Software** is selected in the software download window on CT.

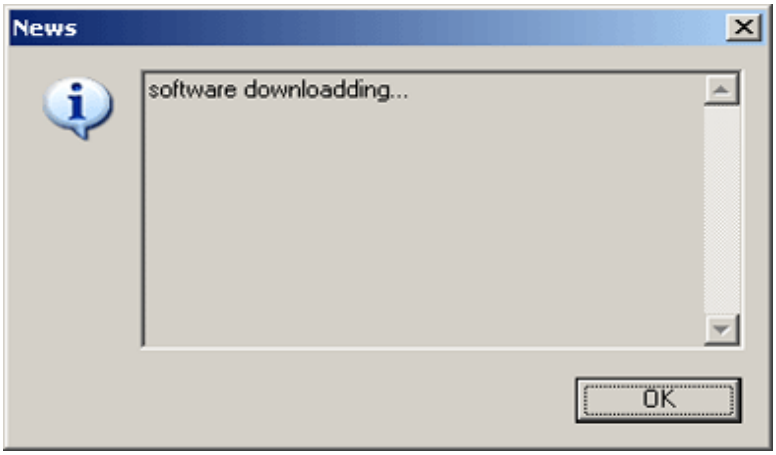
4. Click the **Apply** button.

Message displayed when downloading selected software

Display the **Software Download** window on CT.

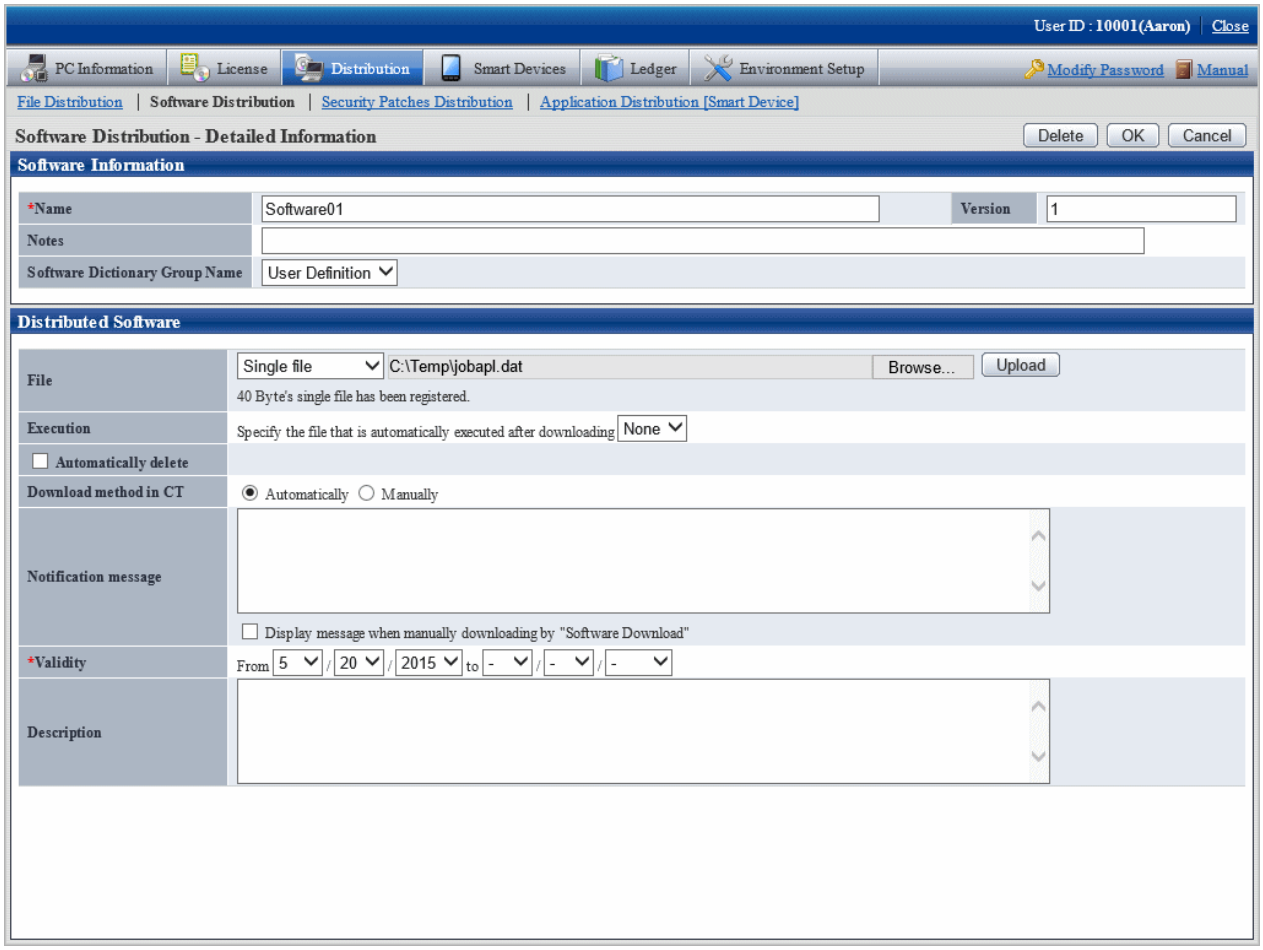


Select the software to be downloaded, the message will be displayed after selection of **File** > **Download** in the menu.



The procedure is as follows.

1. Register software referring to relevant contents in "8.2.3 Register Software Distribution to be Released".
2. In window of **Distribution** > **Software Distribution** > **Software Distribution - Detailed Information**, and set the display message.



3. Input message in **Notification message**, select **Display message when manually downloading by "Software Download"** .
4. Click the **OK** button.

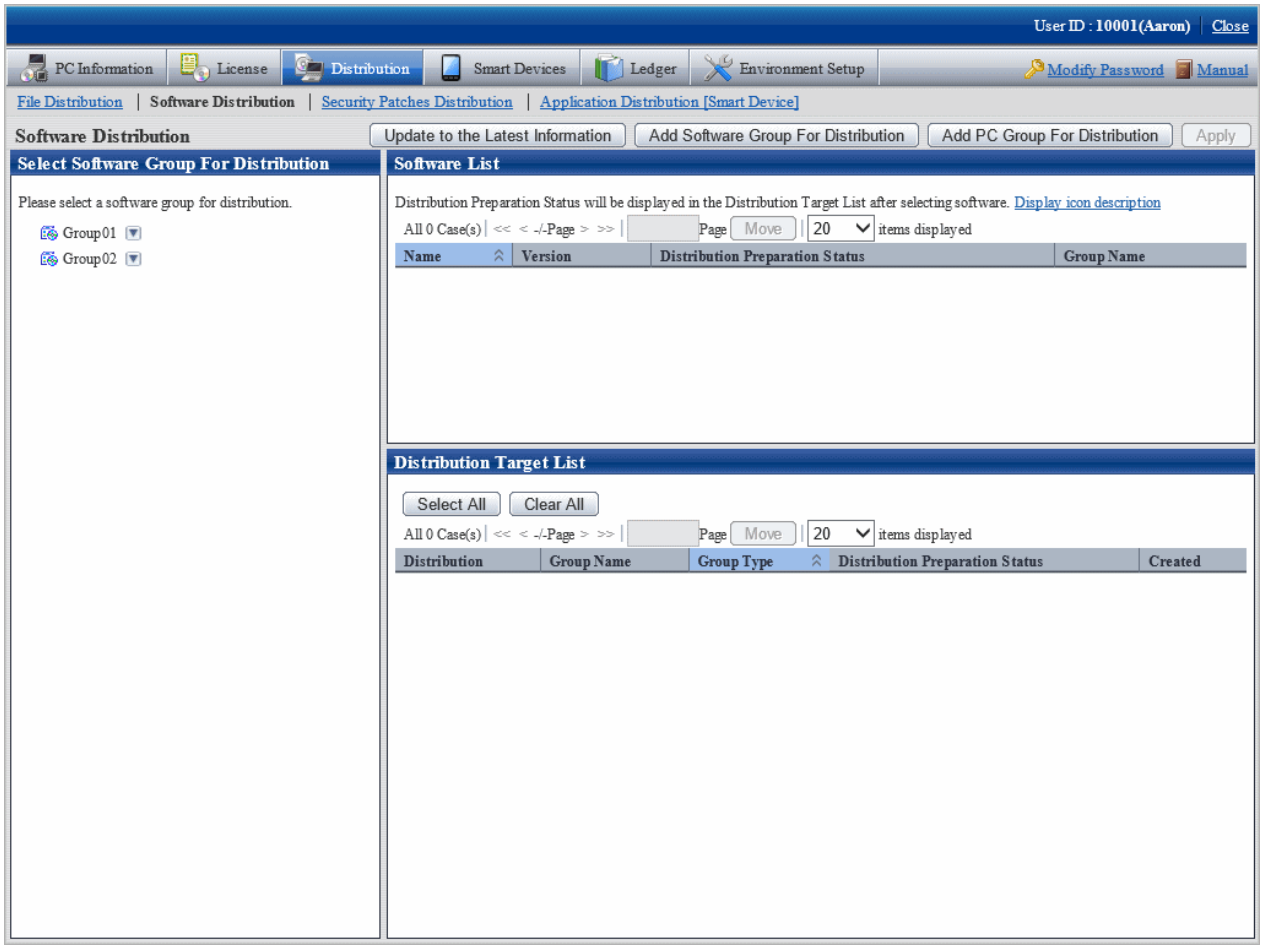
8.4 Operation

Whether the logon software has been distributed to each server normally can be confirmed through use of software distribution.

The procedure is as follows.

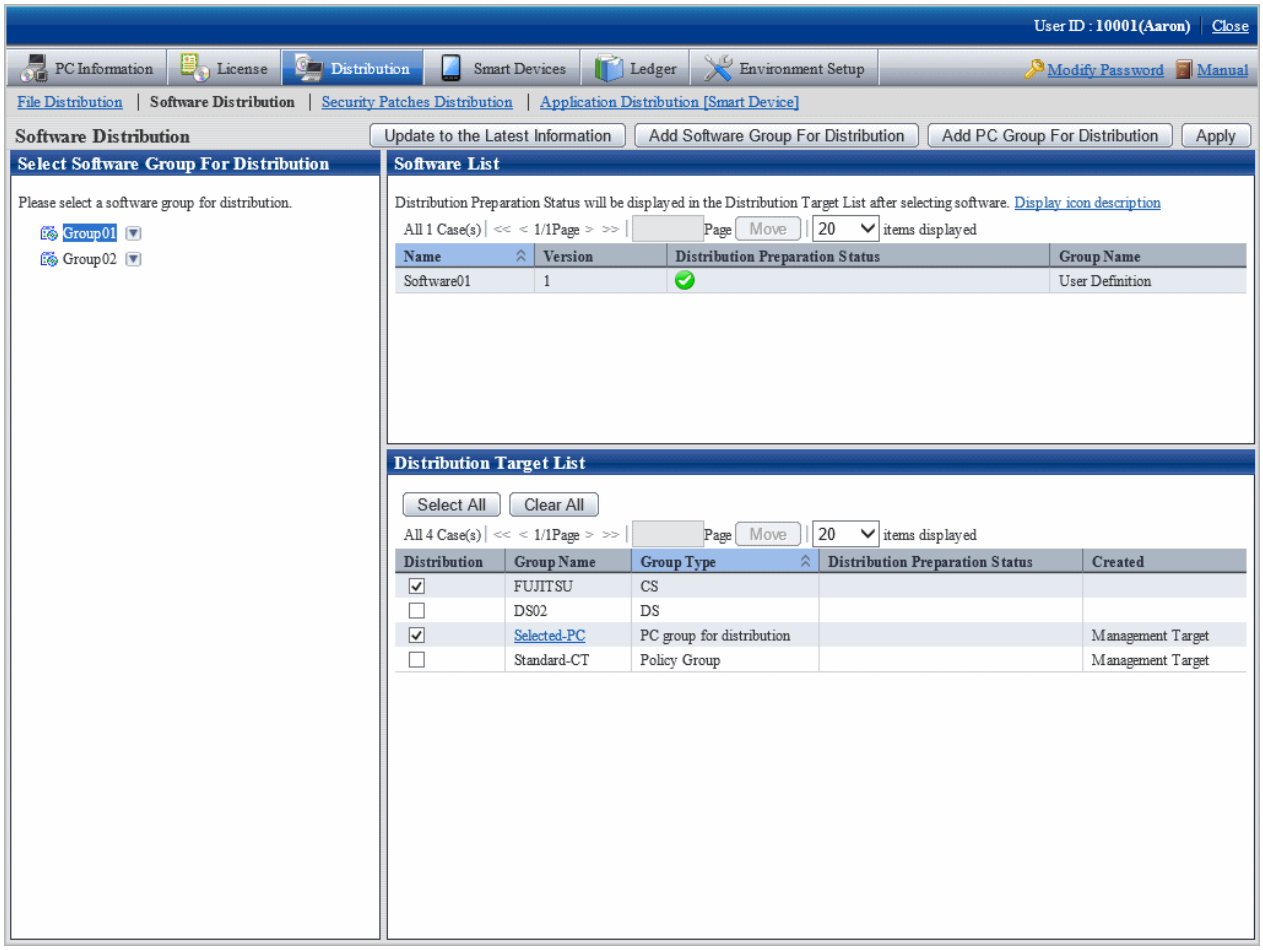
1. Log on to the main menu, click **Distribution** > **Software Distribution**.

   The following window will be displayed.



2. Select the software group for distribution from the field on the left of the window.

   The **Software List** and **Distribution Target List** will be displayed in the field on the right of the window.



3. Confirm distribution status by software in **Software List**.

   See below for definition of each icon in the **Distribution Preparation Status** column.

Icon	Description
	Distribution of correspondent software for distribution target completed.
	In distribution of correspondent software for distribution target.
	Distribution of correspondent software for distribution target failed.
None	Distribution target does not exist.

4. Confirm distribution status by the distribution target in **Distribution Target List**.

   The meaning of each icon in the **Distribution Preparation Status** column is as follows.

Icon	Description
	Distribution of correspondent software has completed.
	In distribution of correspondent software.
	Distribution of correspondent software failed.
None	No distribution target exists.

Chapter 9 Managing Smart Devices

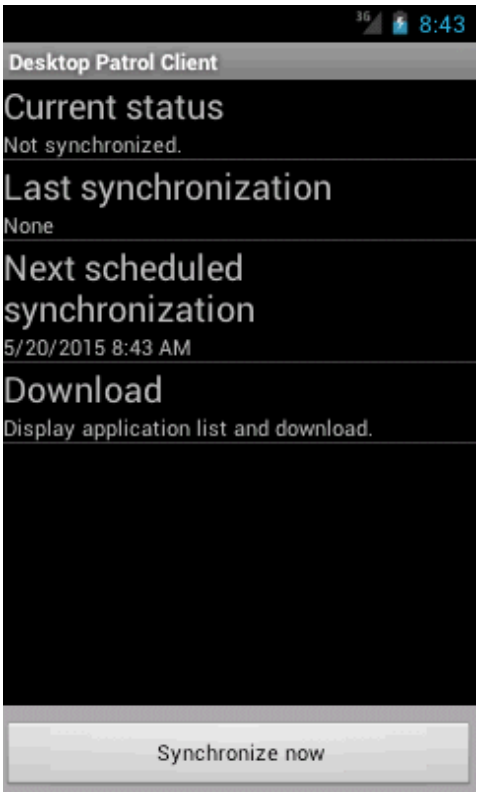
This chapter describes how to manage smart devices.

9.1 Synchronizing Inventory Information (Android Device Only)

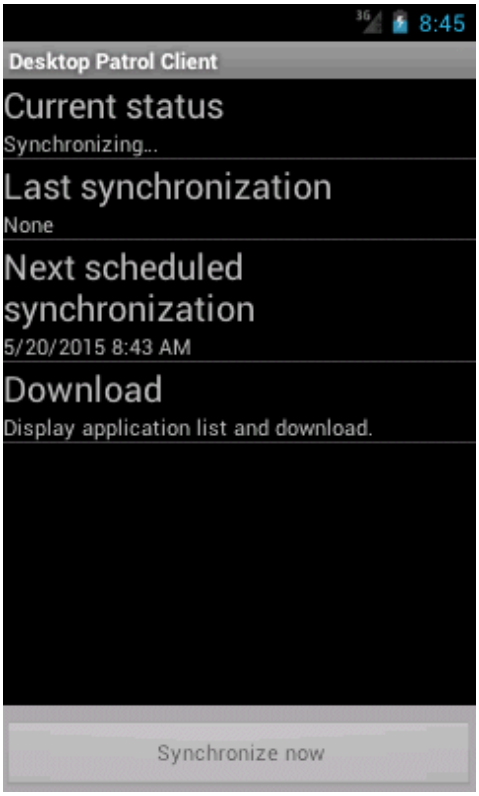
9.1.1 How to Synchronize the Inventory Information

The inventory information is synchronized automatically, however you can also choose to synchronize the inventory information at a time of your choosing.

- To synchronize the inventory information at a time of your choosing, tap **Synchronize now** button in the screen displayed when the smart device starts up.



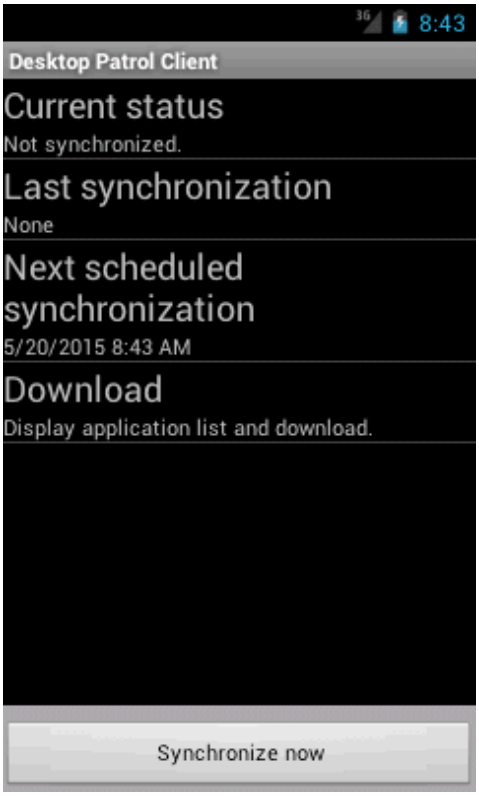
- During synchronization, the content displayed under the **Current status** changes. **Synchronize now** is grayed out and cannot be tapped.



9.1.2 Checking the Operational Status of the Smart Device CT

The operational status of the smart device CT can be checked using the window below.

- The operational status can be checked in the window that is displayed when the smart device CT starts up.



The display items are shown below:

Item	Description
Current status	The operational status of the smart device CT is displayed. During synchronization, this display changes. Refer to "Message List" in the *Systemwalker Desktop Patrol Reference Manual* for details.
Last synchronization	This item shows the date and time of the last synchronization with the Smartdevice Server (SS). If synchronization has not been performed, **None** will be displayed.
Next scheduled synchronization	The date and time of the next scheduled synchronization with the SS is displayed.
Download	When this item is tapped, a list of applications is displayed.
Synchronize now	When this button is tapped, synchronization with the SS will start.

9.2 Referencing Collected Inventory Information

You can reference the inventory information collected by a smart device from the main menu of Systemwalker Desktop Patrol. You can reference this information only when you are logged in as the system administrator or department manager.

The following information can be referenced:

- Smart device information
- Application information

Association of smart devices and user IDs

In the following cases, smart devices can be managed by a department based on user management information:

- If user IDs are specified on the smart devices (Android devices only)

  Refer to "Installing Smart Device CT (Android)" in the *Systemwalker Desktop Patrol Installation Guide* for details.

- If the manager has associated the smart devices and user IDs (iOS devices or Android devices)

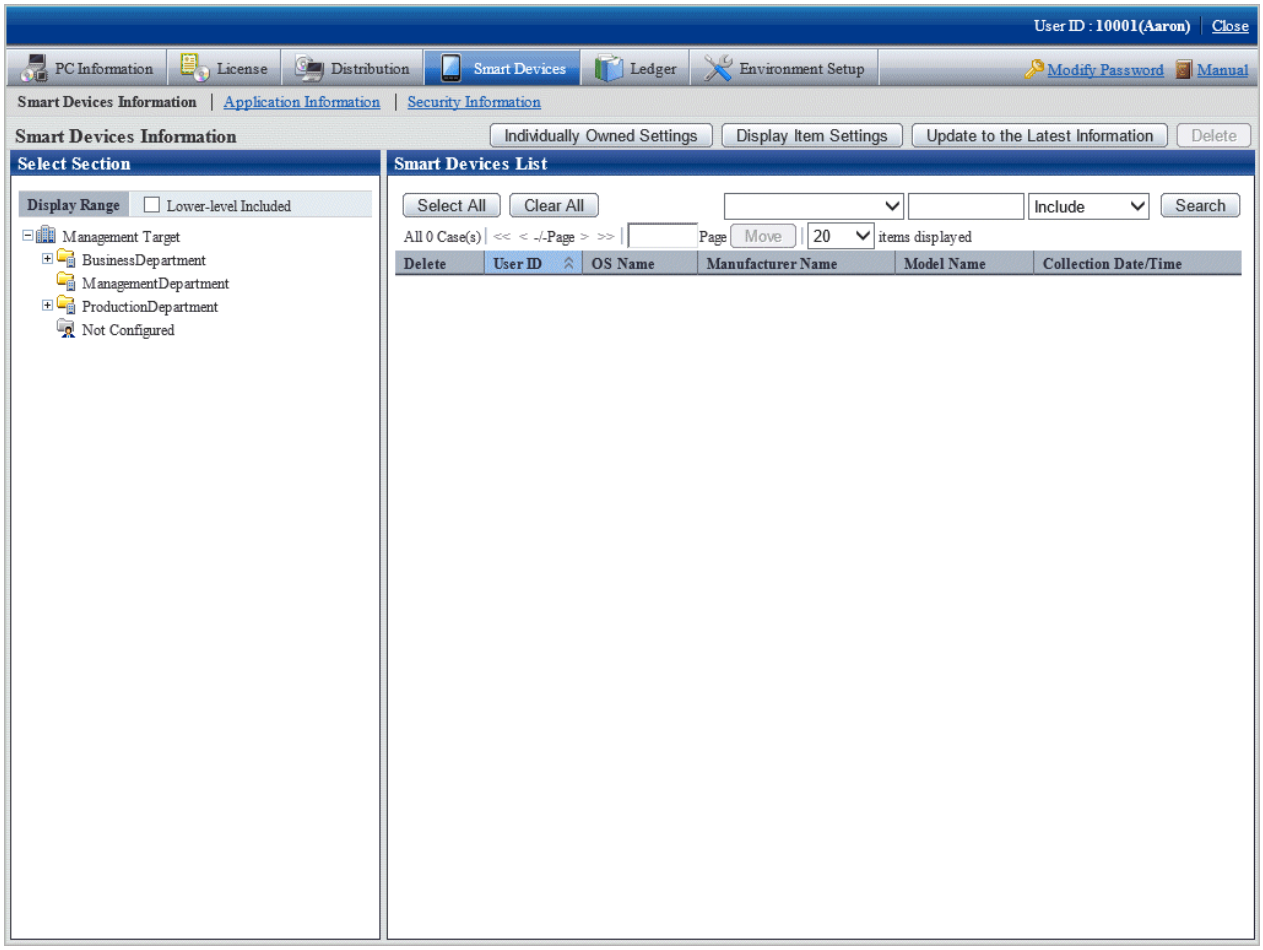
  Refer to "SWDTP_sdmap.exe (building smart device management information)" in the *Systemwalker Desktop Patrol Reference Manual* for details.

Point

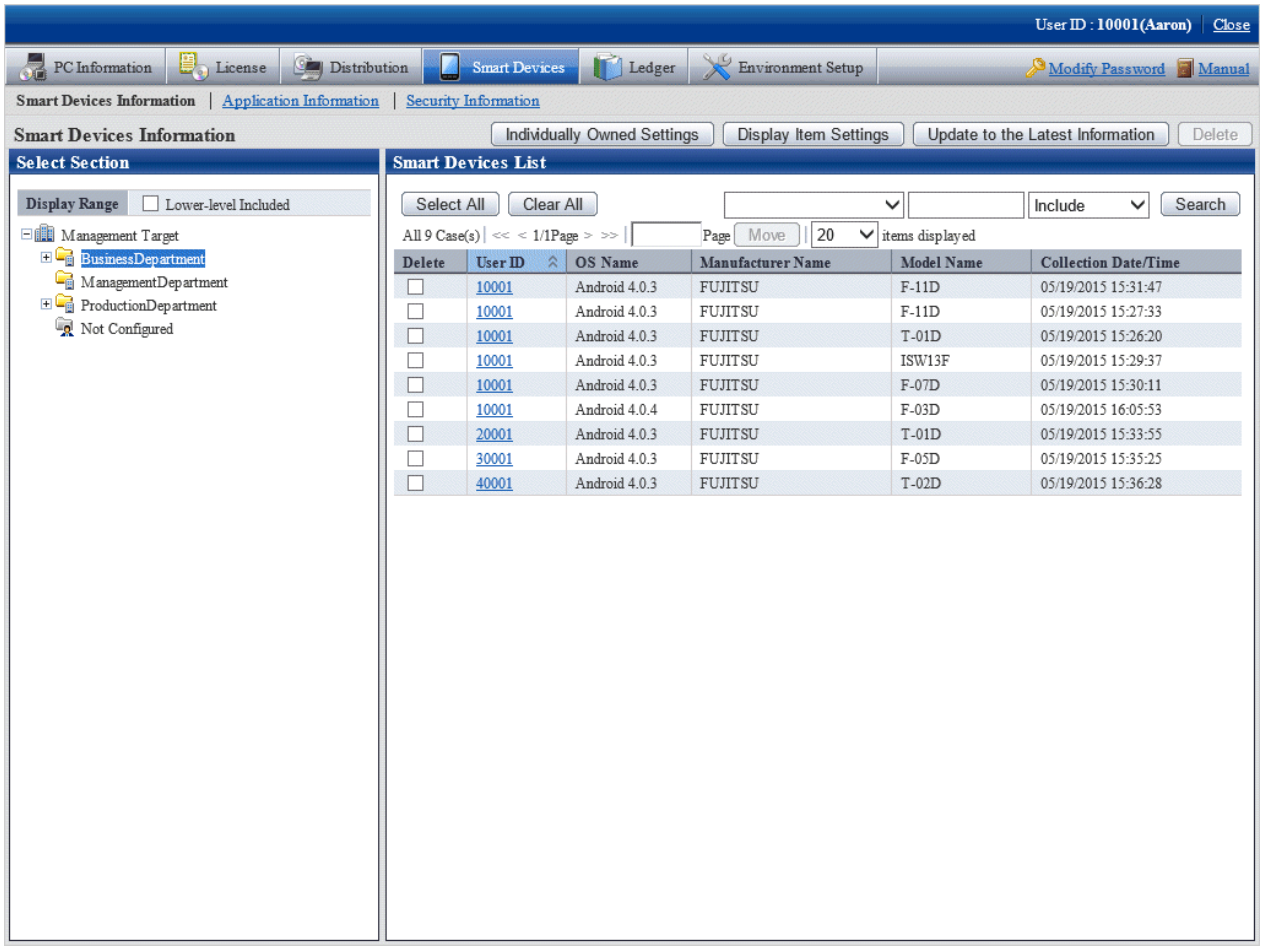
If user IDs are specified on the smart devices and the manager has associated the smart devices and user IDs, information on the smart devices and user IDs associated by the manager takes priority.

Smart device information

1. Log in to the main menu, then click **Asset Management** > **Smart Devices** to display the following window:



2. Select a department from the department tree in the left pane.
   The smart devices in the selected department are displayed in the right pane.



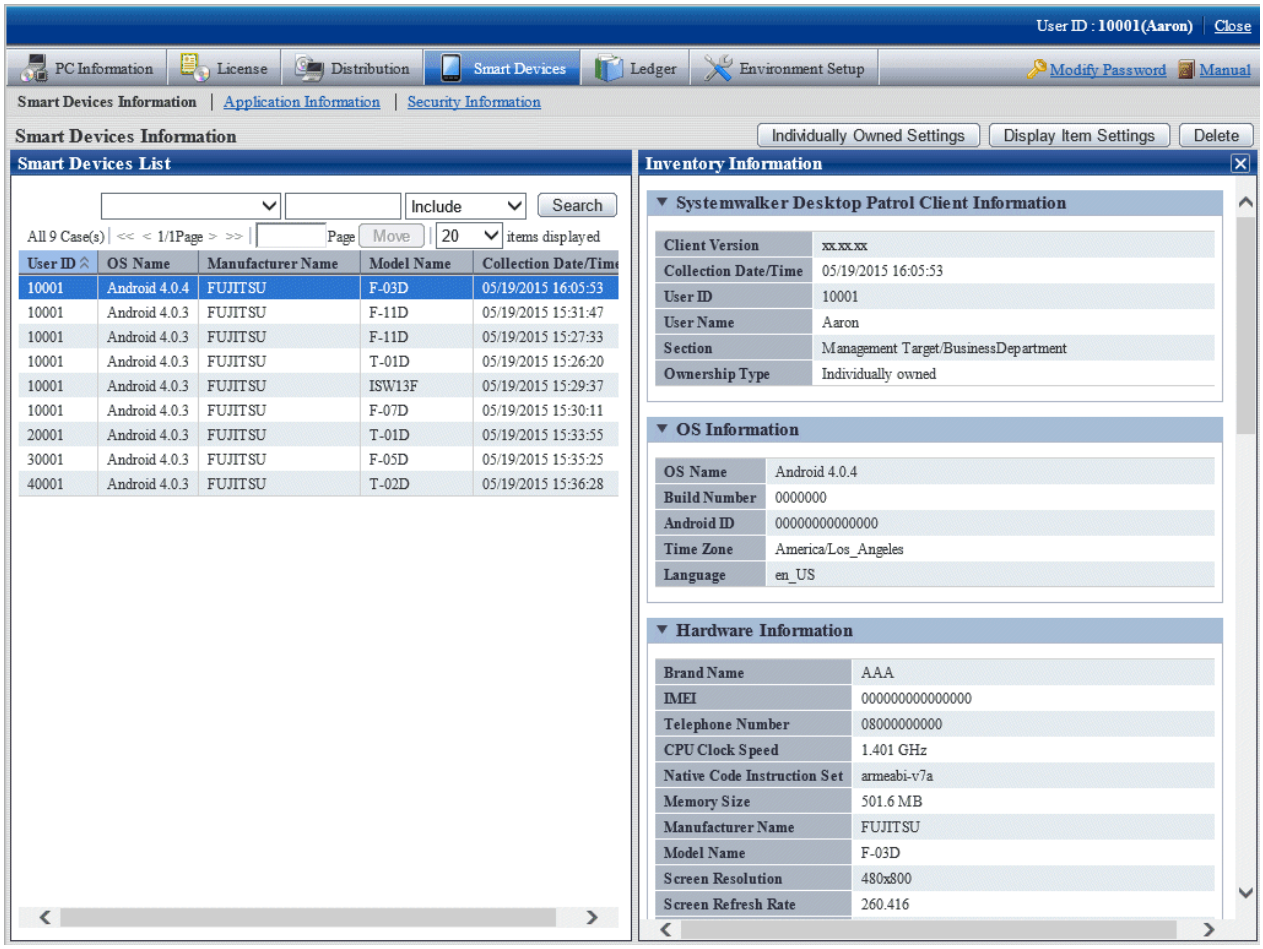
To delete smart device information, select the check box for the information to be deleted, and then click the **Delete** button at the top right hand side of the window.

Click the **Display Item Settings** button to change the items displayed in the list of smart devices and the order in which they are displayed.

If user IDs are specified on the smart devices, or if the manager has associated the smart devices and user IDs, the smart devices in the department to which the users belong are displayed in the right pane in accordance with user management information.

3. Click the user ID link in the list of smart devices.

   Detailed information for the selected user ID will be displayed in the field on the right. Click the **X** button to close the **Inventory Information** window.



The following inventory information collected from the smart device is displayed in the details window (the items marked "Y"):

Information	Item	Android	iOS	Description	Comments
Systemwalker Desktop Patrol Client Information	**Client Version**	Y		Version of the CT for smart devices	
	Collection Date/ Time	Y	Y	Collection date and time	
	User ID	Y	Y	User ID set on the smart device CT, or user ID associated with the smart device by the manager	If the user ID is omitted, this item becomes fixed as "MobileUser".
	User Name	Y	Y	User name for the user ID that is registered in user management	This item will be empty if the user ID is not registered in user management. This item can only be seen in the details window.
	Section	Y	Y	Section to which the user ID belongs	This item will be empty if the user ID does not belong to a section.

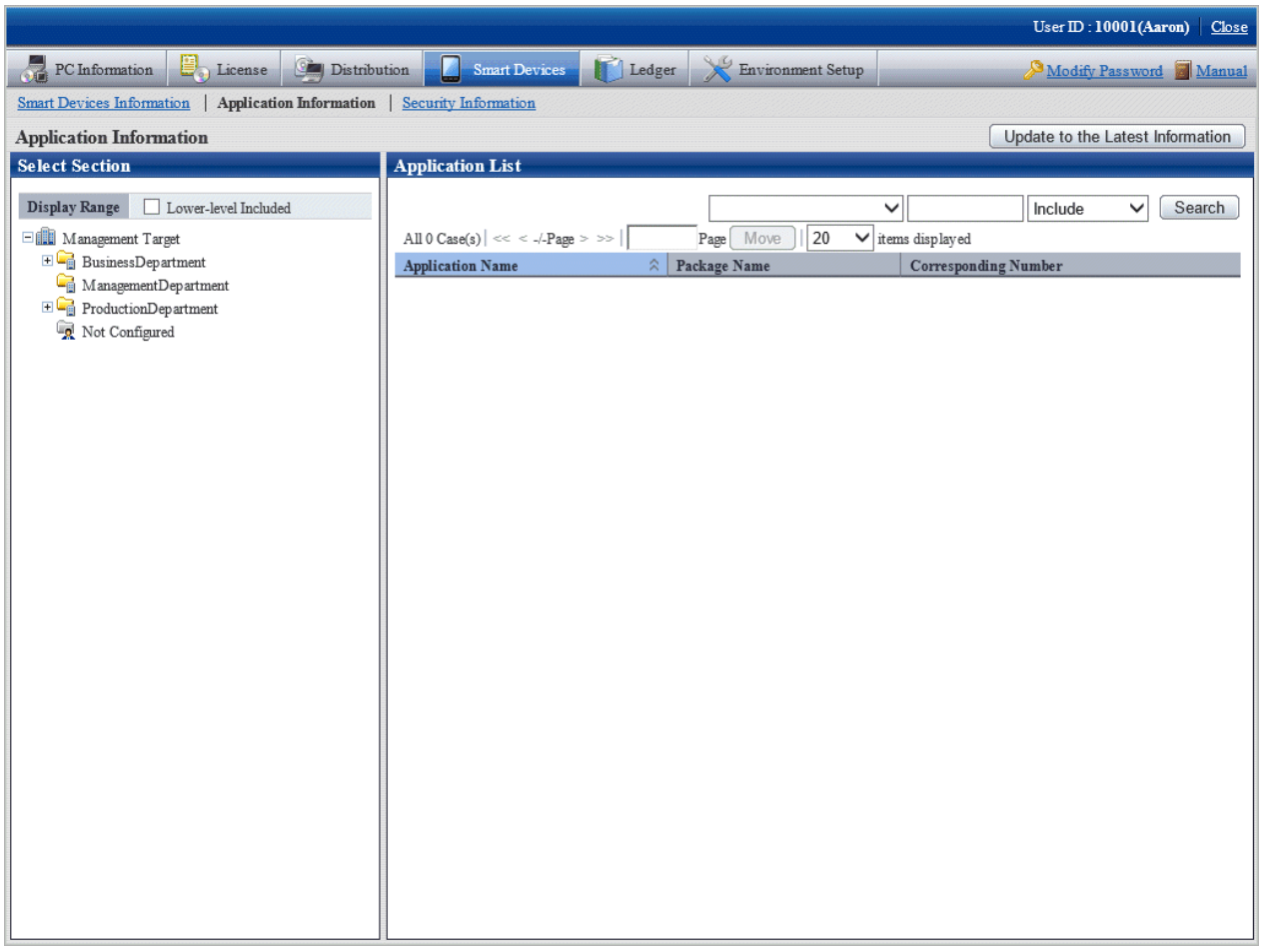
Information	Item	Andro id	iOS	Description	Comments
					This item can only be seen in the details window.
	Ownership Type	Y		Owner of the smart device (company owned device or individually owned device)	
OS Information	**OS Name**	Y	Y	OS type and version	
	Build Number	Y	Y	OS build number	
	Android ID	Y		ID of the device used for Google Play	
	Time Zone	Y		Country and region where the device is being used (time zone)	
	Language	Y		Language to use	
Hardware Information	**Brand Name**	Y		Carrier, manufacturer	
	IMEI	Y	Y	International Mobile Station Equipment Identity (number identifying the terminal)	
	Telephone Number	Y	Y	Telephone number without hyphens	
	CPU Clock Speed	Y		Clock rate	
	Native Code Instruction Set	Y		armeabi-v7a etc. in CPU-ABI order	
	Memory Size	Y		Memory size	
	Manufacturer Name	Y	Y	Name of the manufacturer	
	Model Name	Y	Y	Model name	
	Screen Resolution	Y		Screen resolution	
	Screen Refresh Rate	Y		Screen refresh rate	
	Total space on SD card	Y		The total volume of the SD card	
	Available space on SD card	Y		The available volume of the SD card	
	Device Name		Y	Device name	
	Model		Y	Model number of the device	
	Serial Number		Y	Serial number	
	UDID		Y	Unique Device Identifier. A code that identifies the device.	
	Total Capacity		Y	Total capacity. Measured in gigabytes.	
	Available Capacity		Y	Available capacity. Measured in gigabytes.	

Information	Item	Android	iOS	Description	Comments
	Modem Firmware Version		Y	Firmware version	
	ICCID		Y	ICC identification number for SIM	
	Bluetooth MAC		Y	Bluetooth MAC address	
Communication Information	**Carrier Name**		Y	Carrier name	
	Data Roaming		Y	Whether to perform data communication during roaming	
Wi-Fi Information	**Host Name**	Y		Host name	
	MAC Address	Y	Y	MAC address	
	IP Address	Y		IP address	IPv6 addresses are not displayed.
	Subnet Mask	Y		Subnet mask	
	Default Gateway	Y		Default gateway	
	DHCP Server	Y		DHCP server	
	DNS Server 1	Y		DNS server 1	
	DNS Server 2	Y		DNS server 2	
Account Information	**Account Type**	Y		Type corresponding to the account name	These items can only be seen in the details window.
	Account Name	Y		Name of the account registered on the terminal (normally a Gmail address)	
Application Information	**Application Name**	Y	Y	Application name	These items can only be seen in the details window.
	Package Name	Y	Y	Package name	
	Version	Y	Y	Version	
Security Information	**Screen Lock Type**	Y		Method of releasing the device lock	
	Idle Time until Screen Lock	Y		Time that the device remains idle before being locked	
	Enable Password	Y		Activation of the password lock policy	
	Password Length	Y		Number of characters required in the password	
	Password Complexity	Y		Complexity of the password	
	Storage Encryption	Y		Implementation of storage encryption	
	Automatic Setting of Date and Time	Y		Use the time provided by the network	
	Automatic Setting of Time Zone	Y		Use the time zone provided by the network	
	Root Device	Y		Whether illegally modified by rooting	

Information	Item	Android	iOS	Description	Comments
	USB Debug	Y		Activation of USB debugging feature	
	Passcode		Y	Whether a passcode is set	

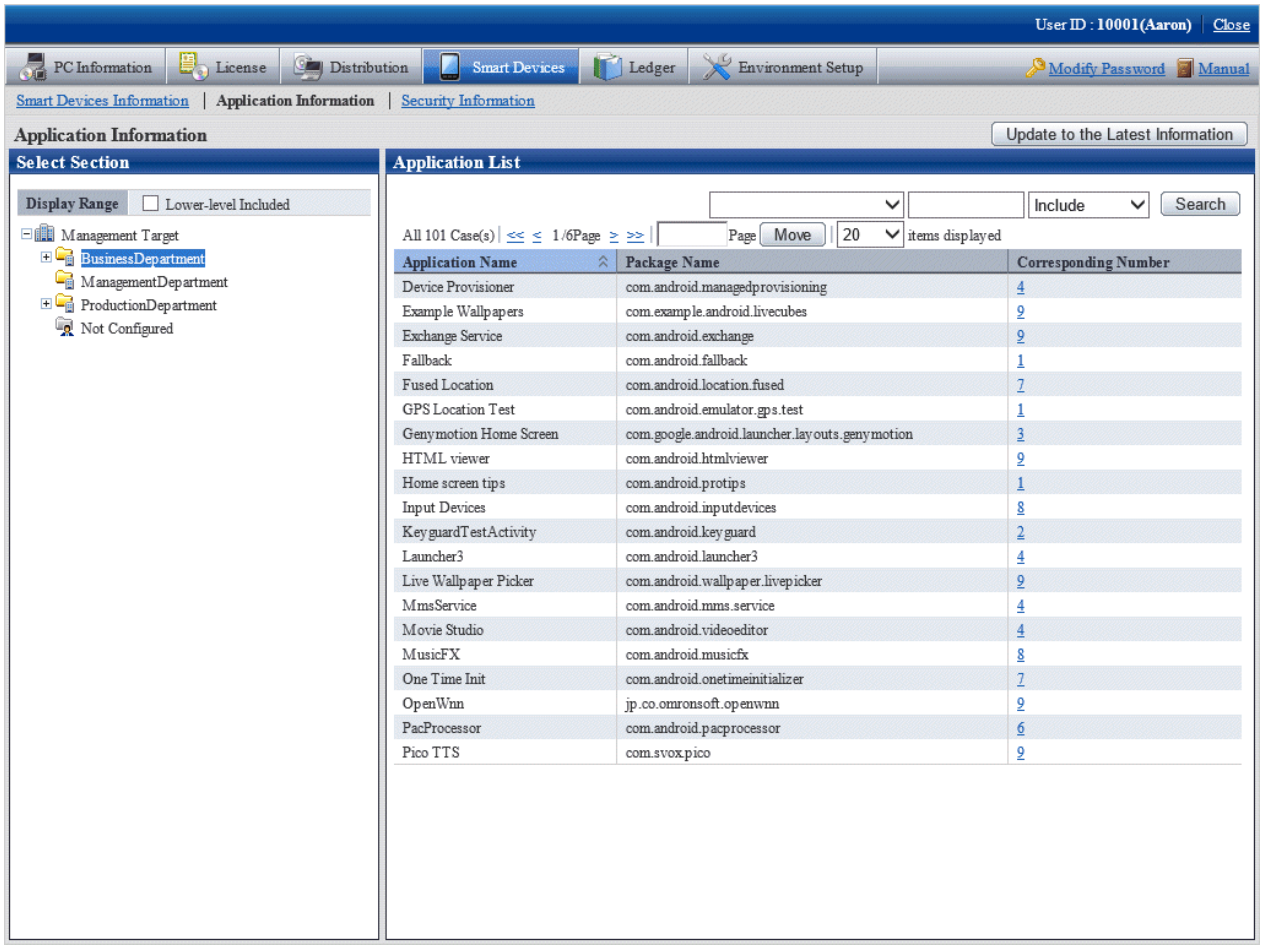
Application information

1. Click **Application Information** in the submenu to display the following window:



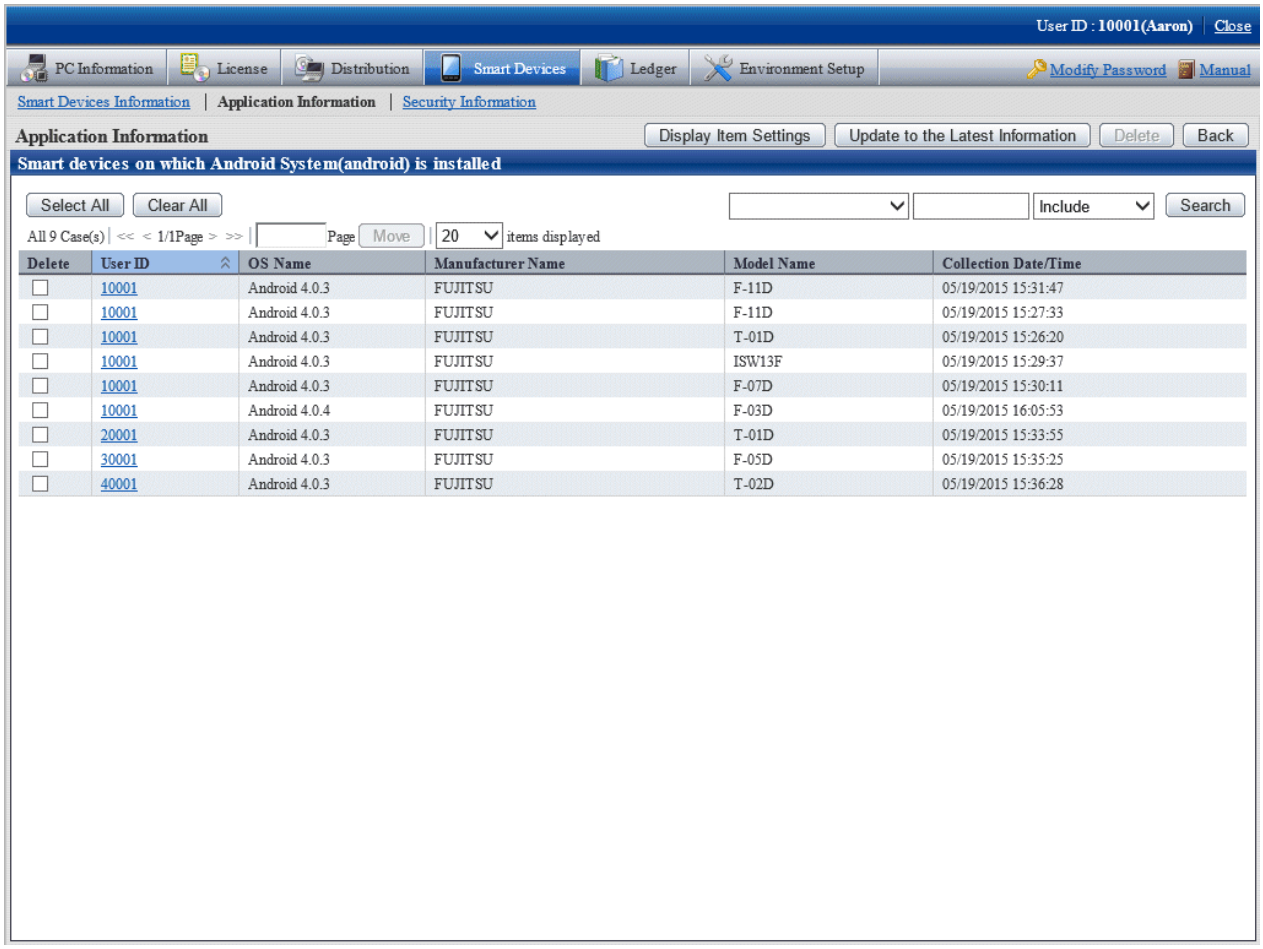
2. Select a department from the department tree in the left pane.

   Application information for the smart devices in the selected department is displayed in the right pane.



3. Click a link in the **Corresponding Number** column.

   A list of smart devices with the relevant application installed is displayed.



9.3 Referencing Collection Information in Security Settings

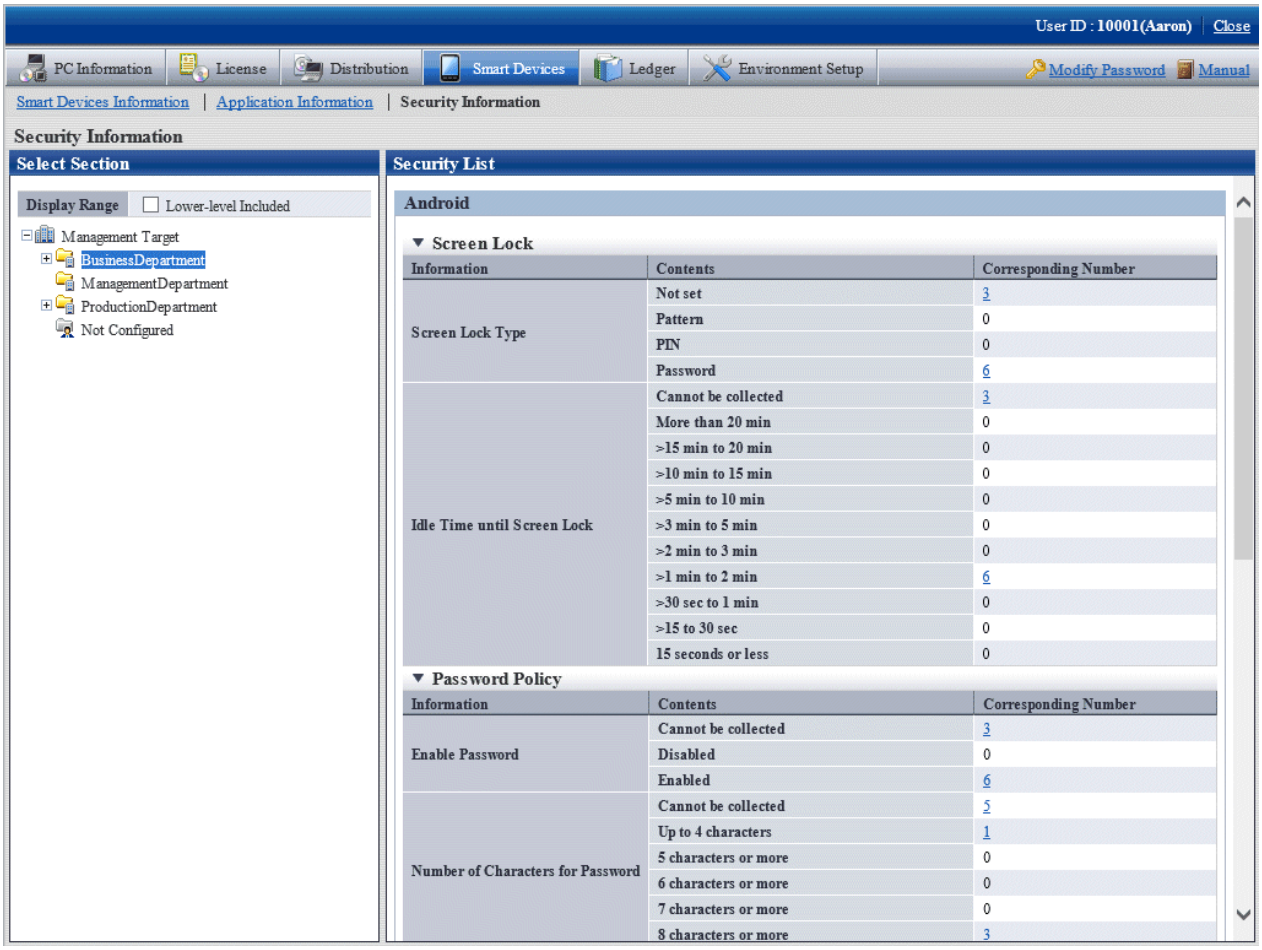
You can reference collection information in security settings.

The procedure is as follows:

1. Log in to the main menu, and click **Assets Management** > **Smart Devices**.

   The **Smart Devices Information** window will be displayed.

2. In the submenu, click **Security Information**. The window shown below will be displayed.
   If you selected a department from the department tree in the left pane, security information for the smart devices in the selected department is displayed in the right pane.



The items displayed in the screen are as follows.

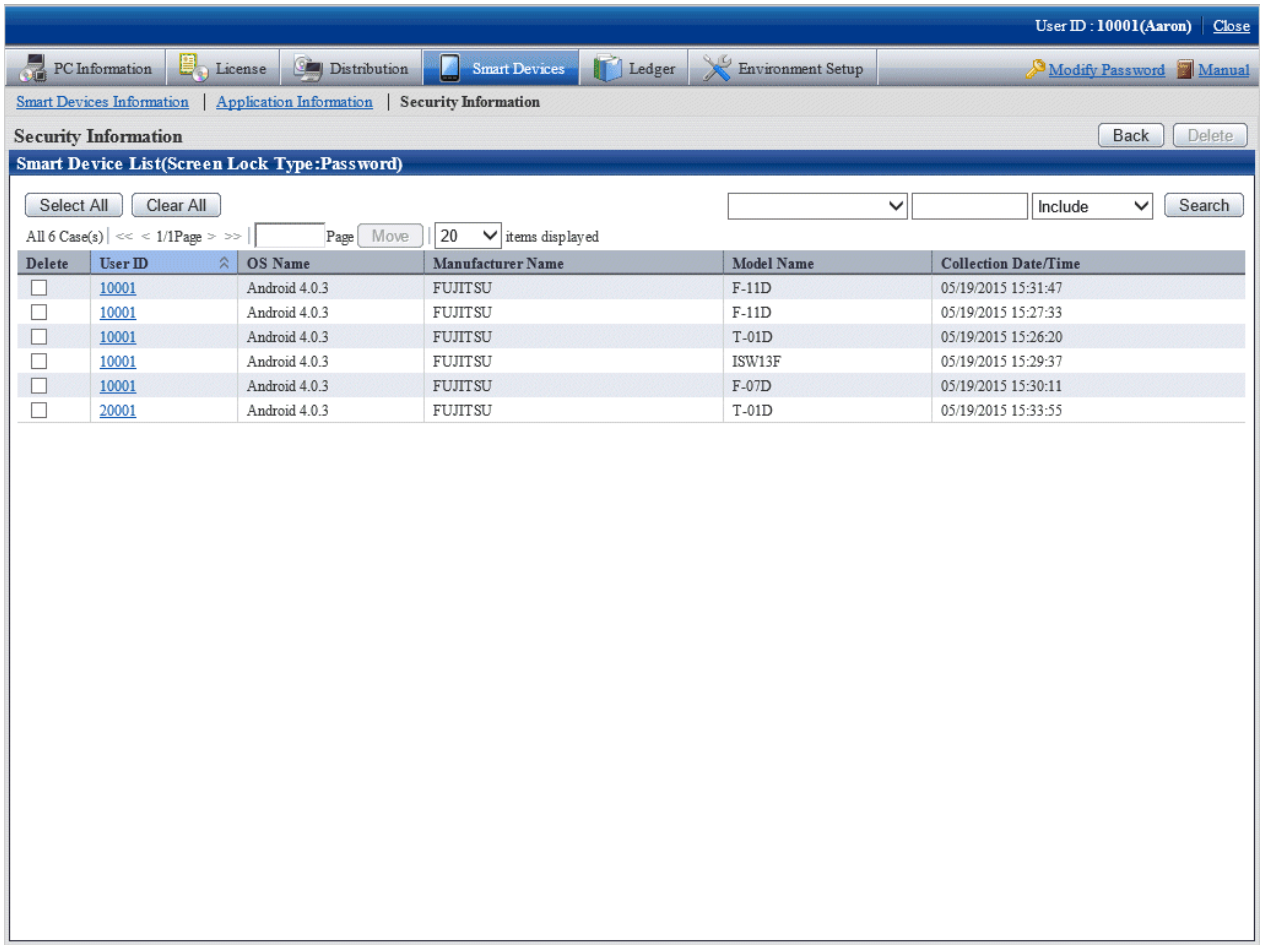
Item		Description
Android	**Screen Lock Type**	Indicates the number of smart devices with each of the following settings for the lock release method when the smart devices have been locked: - **Not set** - **Pattern** - **PIN** - **Password**
	Idle Time until Screen Lock	Indicates the number of smart devices with each of the following settings for the time that the smart device remains idle before being locked: - **Cannot be collected** - **More than 20 min** - **>15 min to 20 min** - **>10 min to 15 min** - **>5 min to 10 min**

Item		Description
		- **>3 min to 5 min** - **>2 min to 3 min** - **>1 min to 2 min** - **30 sec to 1 min** - **>15 to 30 sec** - **15 seconds or less**
	Enable Password	Indicates the number of smart devices with each of the following settings for activation of the password lock policy: - **Cannot be collected** - **Disabled** - **Enabled**
	Number of Characters for Password	Indicates the number of smart devices with each of the following settings for the number of characters required in the password: - **Cannot be collected** - **Up to 4 characters** - **5 characters or more** - **6 characters or more** - **7 characters or more** - **8 characters or more**
	Password Complexity	Indicates the number of smart devices with each of the following settings for the complexity of the password: - **Cannot be collected** - **Letters** - **Alphanumeric characters** - **Alphanumeric characters and symbols**
	Automatic Setting of Date and Time	Indicates the number of smart devices with each of the following settings indicating whether to use the time provided by the network: - **Cannot be collected** - **Manual** - **Automatic**
	Automatic Setting of Time Zone	Indicates the number of smart devices with each of the following settings indicating whether to use the time zone provided by the network: - **Cannot be collected** - **Manual** - **Automatic**
	Storage Encryption	Indicates the number of smart devices with each of the following settings indicating whether storage encryption is implemented:

Item		Description
		- **Cannot be collected** - **Not encrypted** - **Encrypted**
	Root Device	Indicates the number of smart devices with each of the following settings indicating whether the device has been illegally modified by rooting: - **Cannot be collected** - **Rooted** - **Not rooted**
	USB Debug	Indicates the number of smart devices with each of the following settings indicating whether the USB debugging feature has been activated: - **Cannot be collected** - **Enabled** - **Disabled**
iOS	**Passcode**	Indicates the number of smart devices with each of the following settings indicating whether a passcode is set: - **Cannot be collected** - **Not set** - **Set**

3. In the **Security Information** list, click the **Corresponding Number** link you want to view.

   The window shown below will be displayed. This window lists the smart devices for which **Not set** is specified for **Screen Lock Type**.



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

A device owner can change the device ownership form to individual ownership by clearing **Company owned device** on the smart device CT. After a smart device has been changed to individual ownership, inventory information (such as telephone numbers and account information) will be collected if the system administrator has selected that option.

The inventory collection items available for selection by the system administrator are as follows.

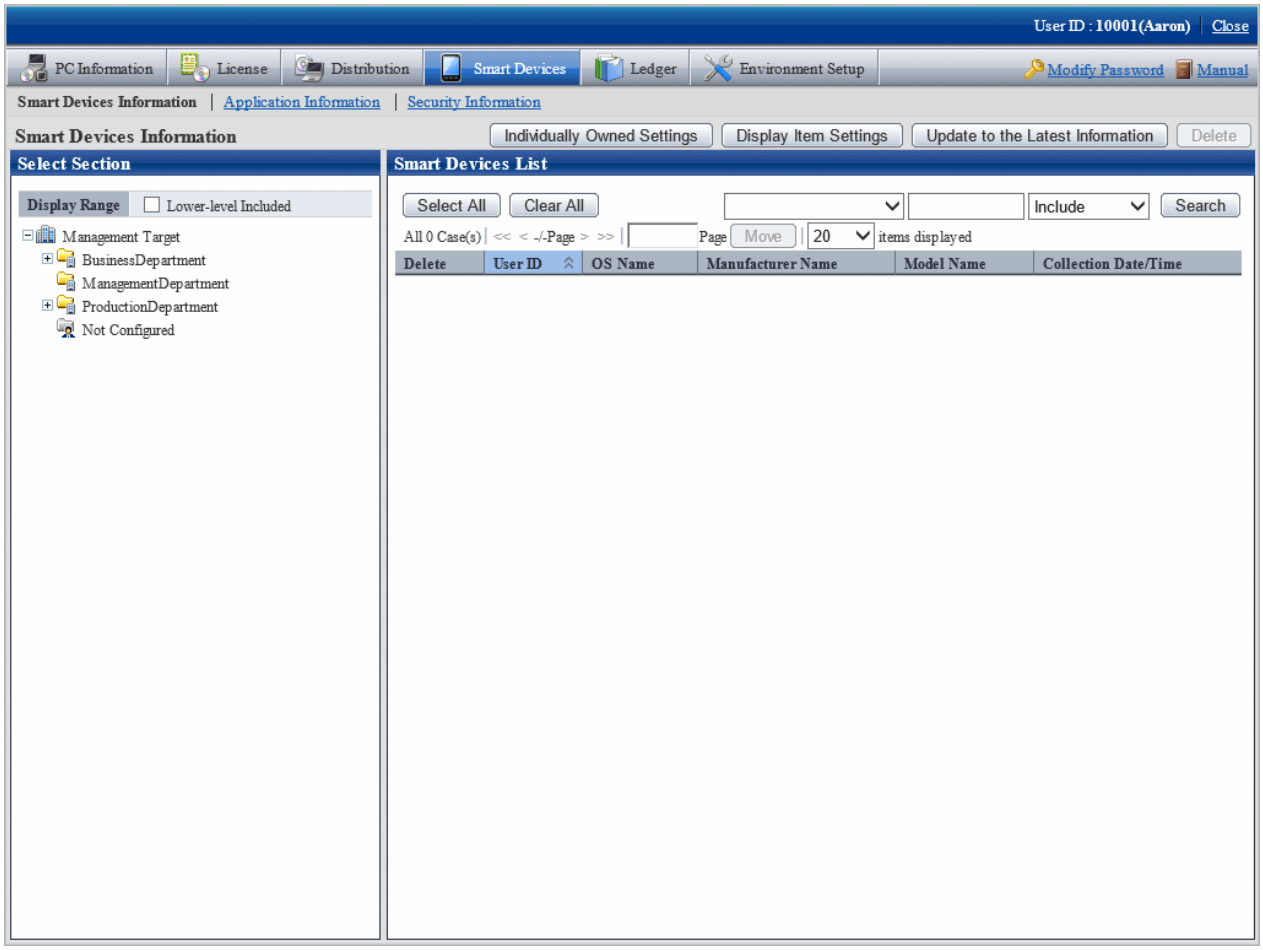
Type	Item
OS Information	**Build Number**
Hardware Information	**Brand Name**
	Telephone Number
	CPU Clock Speed
	Native Code Instruction Set
	Memory Size
	Screen Resolution
	Screen Refresh Rate

Type	Item
	Total space on SD card
	Available space on SD card
Wi-Fi Information	**Host Name**
	IP Address
	Subnet Mask
	Default Gateway
	DHCP Server
	DNS Server 1
	DNS Server 2
Account Information	**Account Type**
Application Information	**All applications**
	Distribution applications only

Procedure

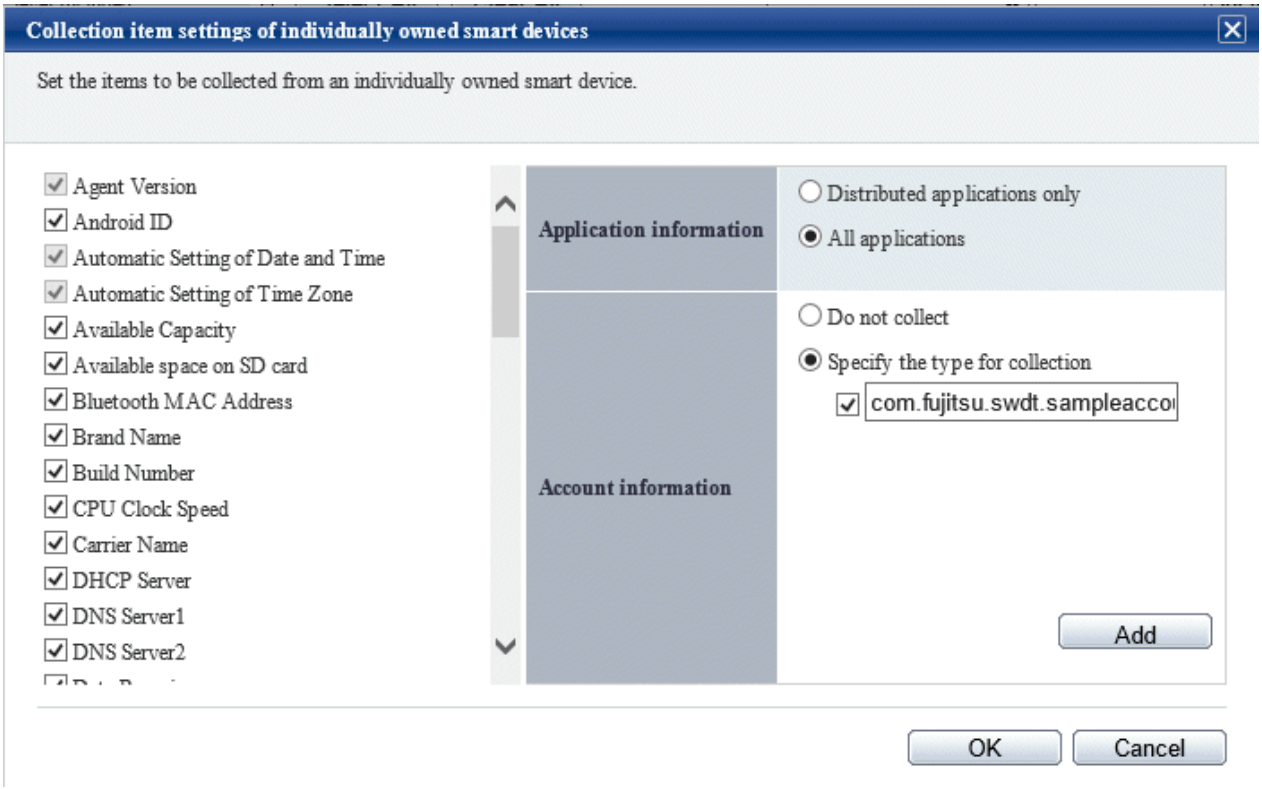
1. Log in to the main menu, and click **Assets Management** > **Smart Devices**.

   The **Smart Devices Information** window will be displayed.



2. Click **Individually Owned Settings**.

   The window shown below will be displayed.



3. Set the items to be collected.

Item	Description
-	Select the items to be collected from an individually owned smart device. Unselectable items are disabled. Initially, all selectable items are unselected. Changes to these settings are reflected the next time inventory collection is performed. Until that time, the window will display the inventory information collected in accordance with the settings that were valid when inventory collection was performed on the smart device.
Application Information	Select one of the following: The initial value is **Distribution applications only**. - **Distribution applications only** Only application information that was distributed by the application distribution feature is collected. If you change from **All applications** to **Distribution applications only**, the new setting will be reflected the next time inventory collection is performed. Until inventory collection, application information other than distribution applications may be displayed in inventory information. - **All applications** All application information is collected. If you change from **Distribution applications only** to **All applications**, the new setting will be reflected the next time inventory collection is performed. Until inventory collection, application

Item	Description
	information other than distribution applications may be displayed in inventory information.
Account Information	Select one of the following. The initial value is **Do not collect**. - **Do not collect** Account information is not collected. If you change from **Specify the type for collection** to **Do not collect**, the new setting will be reflected the next time inventory collection is performed. Until inventory information is reflected, collected account information may be displayed in inventory information. - **Specify the type for collection** Only the specified account type is collected. Select the type to be collected. You can add a type that is not in the list by clicking **Add**. The displayed account types include those collected as inventory information and those added by using **Add**. Account types collected as inventory information cannot be changed or deleted. The following explains how to add an account type and change the collection settings: - Clicking **Add** adds an entry column. Using up to 512 halfwidth characters, enter the account type to be specified. If you do not enter anything, the entry column will automatically be deleted. - To temporarily stop collecting account information of a specific account type, clear the check box for the relevant account type. - To stop collection altogether for a specific account type, you can delete the account type from this setting by deleting the string from the entry column. After you delete an account type, a confirmation dialog box will be displayed when you operate other items or buttons. Click **OK** to delete the relevant account type. If you click **Cancel**, the value is restored. - You cannot specify the same value for multiple account types. If you do specify the same value multiple times and click **OK**, a message will be displayed. Change or delete the value, and then click **OK**. The change to the selected account types or the account types configured in this setting will be reflected the next time inventory collection is performed. Until inventory information is reflected, information of the relevant account type will be displayed in inventory information. If you change from **Do not collect** to **Specify the type for collection**, the new setting will be reflected the next time inventory collection is performed. Until that time, account information may not be displayed in inventory information.

Chapter 10 Distributing Applications to Smart Devices

This chapter explains how to distribute applications to smart devices.

In this chapter, the term "distribute" includes all steps up to and including installation of applications on a smart device.

Note

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

10.1 Procedure

The main menu enables you to configure distribution settings and distribute applications to smart devices.

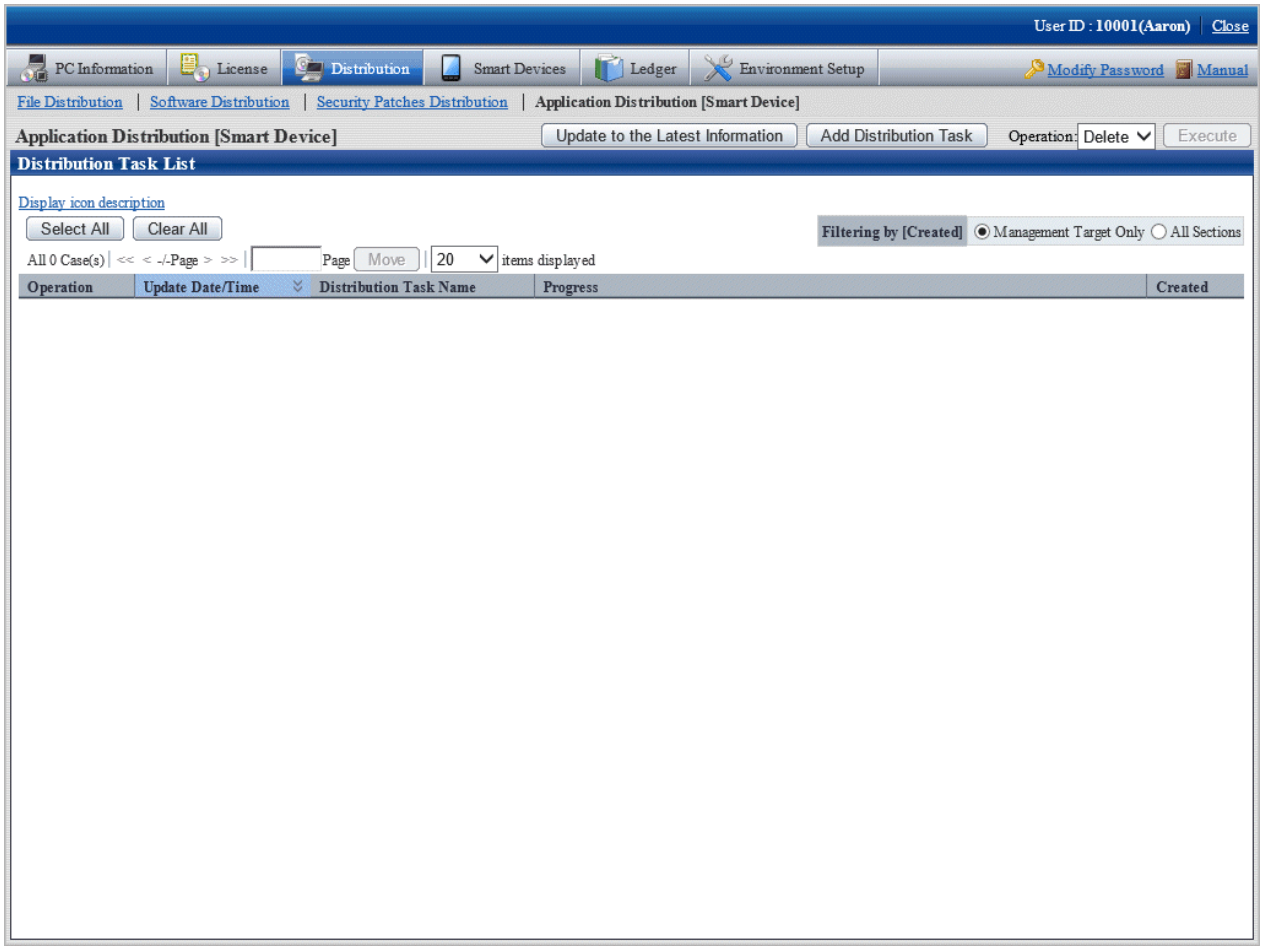
Distribution settings are configured per distribution task. A distribution task is a combination of the application to be distributed and the smart device you are distributing the application to.

10.2 Setup and Distribution

Use the following procedure to set up application distribution and distribute an application.

1. Log in to the main menu.
2. Click **Asset Management** > **Distribution** > **Application Distribution [Smart Device]**.

   The initial window of **Application Distribution [Smart Device]** is displayed.



   The following table explains the buttons:

Button name	Description
Update to the Latest Information	Refreshes the information so that the latest information will be shown.
Add Distribution Task	Adds a task for distributing an application.
Operation / **Execute**	Enabled when a check box in **Distribution Task List** is selected. When you select an operation from the operation list for the distribution task whose check box you selected and then click **Execute**, processing is performed for the distribution task. If you select multiple distribution tasks and operation fails for a specific task, perform that operation for all tasks. The list of operations is as follows: - **Delete** Deletes a distribution task from CS. You cannot delete a task that is being distributed. - **Start** Starts distribution for tasks that have not started to be distributed, have stopped, or have ended abnormally. - **Stop** Stops distribution of a task that is being distributed.

The following table explains the **Distribution Task List** items:

Item	Description
Operation (check box)	Select the check box for the distribution task for which you want to perform the delete or other process.
Update Date/Time	Displays the date and time at which the distribution task was registered or updated.
Distribution Task Name	Displays the name of the distribution task. You can view detailed information on the distribution task by clicking the distribution task name.
Progress	Displays the progress of the distribution task. The color of the bar graph indicates the progress percentage. - Green Indicates the percentage that has been distributed normally. - Red Indicates the percentage that has failed to be distributed. - Gray Indicates the percentage that has not finished being distributed. The meaning of each icon is as follows: : Distributed normally. : Distribution ended abnormally. : Distribution has not started. : Distribution is in progress.

Item	Description
	: Distribution has stopped. The total calculated from "number of applications x smart devices targeted for distribution" is displayed as a number next to the icon. The breakdown is as follows: - Total *n* Number of applications to be distributed. - Normal *n* Indicates the number of applications that finished being distributed normally. - Abnormal *n* Indicates the number of applications that failed to be distributed. Click the distribution task name and check the **Detailed Status** tab for details of why distribution failed. - Distributing *n* Indicates the number of applications being distributed. - Not distributed *n* Indicates the number of applications that have not been distributed.
Created	Indicates the department to which the manager who created the distribution task belongs. If the system administrator created the distribution task, this is fixed as "Management Target".
Filtering by [Created]	You can use the **Created** item to filter the content of **Distribution Task List**. The content displayed in **Distribution Task List** depends on the privileges of the user logged in to the main menu. - With system administrator privileges - **Management Target Only** Displays only the distribution tasks for which **Created** is "Management Target". - **All Sections** Displays all distribution tasks, regardless of their **Created**. - With department manager privileges - **Affiliated Section Only** Displays only the distribution tasks created in the department to which the logged in user belongs. - **All Sections for Viewing** Displays the distribution tasks created in the department to which the logged in user belongs and distribution tasks created in all lower levels.

Point

Maximum number of tasks to be managed

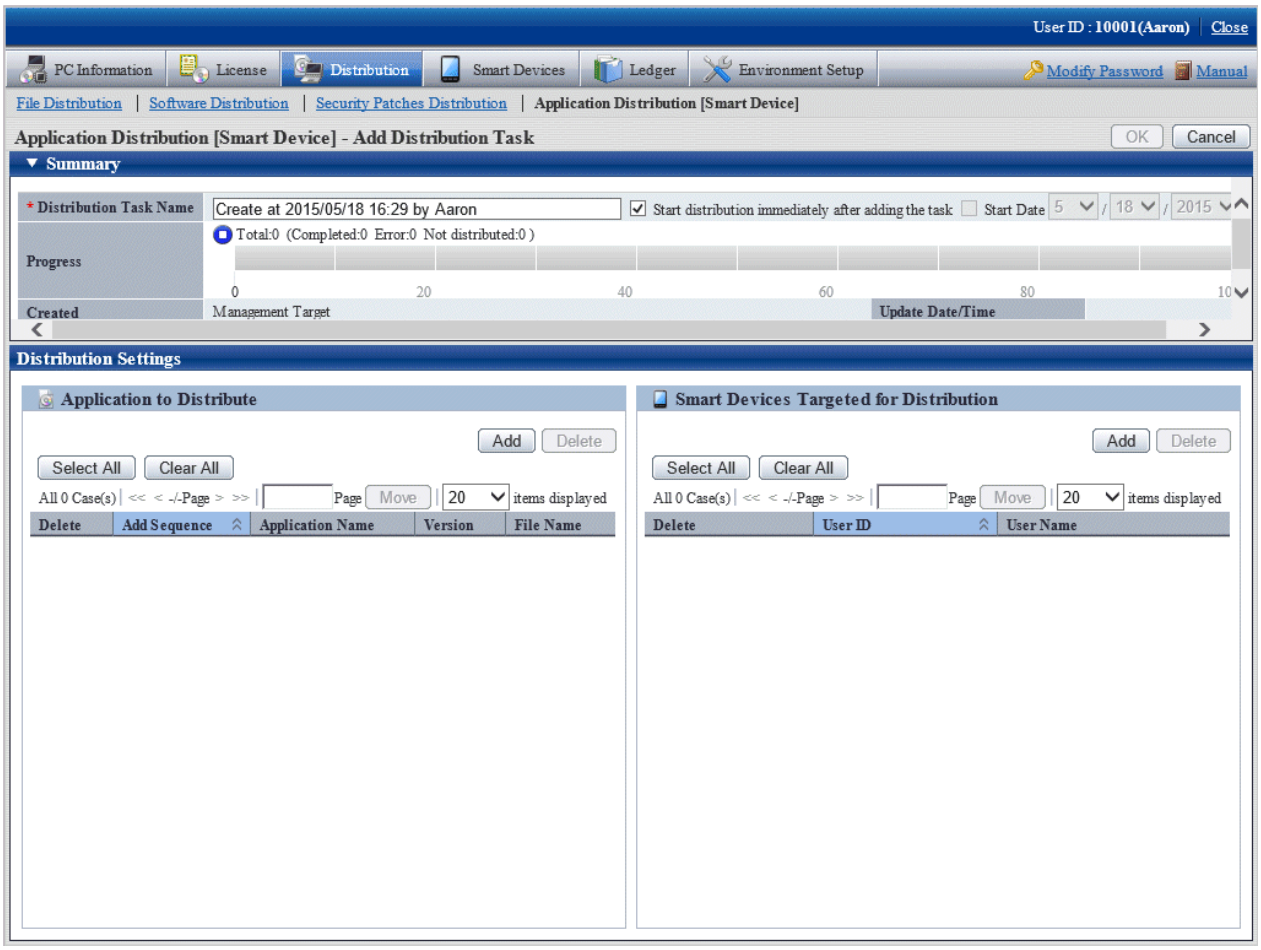
Up to 100 tasks can be managed on a system.

Tasks are not deleted automatically, so delete tasks that completed normally and are no longer required for operations.

When the number of tasks on a system reaches 100, you cannot add a distribution task by clicking the **Add Distribution Task**.

3. Click the **Add Distribution Task** button.

   The **Application Distribution [Smart Device] - Add Distribution Task** window will be displayed.



The following table explains the setting items of this window:

Item	Description
OK	Registers or updates the settings and navigates the display to **Distribution Task List**. This button is enabled when at least one application to be distributed and at least one smart device targeted for distribution have both been registered.
Cancel	Navigates the display to **Distribution Task List** without registering or updating the settings.
Distribution Task Name	Specify the name of the task to be distributed, using up to 30 fullwidth characters or 60 halfwidth characters. By default, the creation date and time and the name of the creating user are displayed. This item is required. - **Start distribution immediately after adding the task** Distribution will start after you select this item and click **OK**. To perform distribution preparation only, clear this item and click **OK**. - **Start Date** Selecting this item enables you to select the date for starting distribution. If the date is the current date or in the past, distribution will start as soon as you click **OK**.

Item	Description
Progress	Displays the progress of the distribution task. The content is the same as in the **Distribution Task List** window.
Created	Indicates the department to which the manager who created the distribution task belongs. The content is the same as in the **Distribution Task List** window.
Update Date/Time	Displays the date and time at which the distribution task was registered or updated.

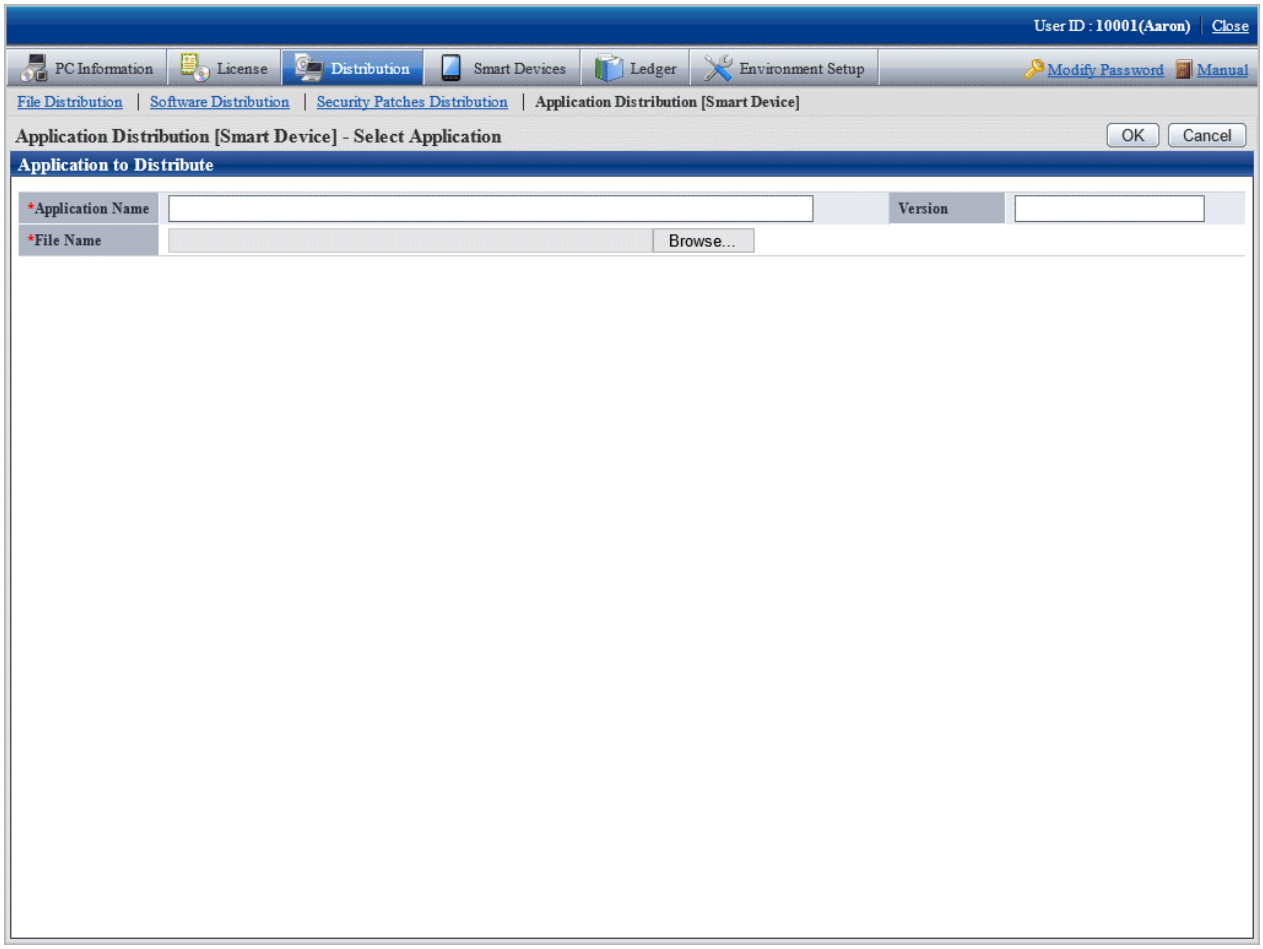
The following table explains the content of **Application to Distribute** in the **Distribution Settings** tab:

Item	Description
Add	Adds an application to be distributed. The display then navigates to the **Select Application** window. This button is not displayed for a task that has started to be distributed.
Delete	Deletes an application. This button is enabled when you select **Delete**. It is not displayed for a task that has started to be distributed.
(Check box)	To delete an application, select the application to be deleted.
Add Sequence	Displays the sequence in which applications were added.
Application Name	Displays the application name specified by the manager.
Version	Displays the version of the application.
File Name	Displays the selected file name.

The following table explains the content of **Smart Devices Targeted for Distribution** in the **Distribution Settings** tab:

Item	Description
Add	Adds a smart device to be targeted for distribution. The display then navigates to the **Select Smart Device** window. This button is not displayed for a task that has started to be distributed.
Delete	Deletes a smart device. This button is enabled when you select **Delete**. It is not displayed for a task that has started to be distributed.
(Check box)	To delete a smart device, select the smart device to be deleted.
User ID	Displays the user ID of the user who is using the smart device.
User Name	Displays the user name of the user who is using the smart device.

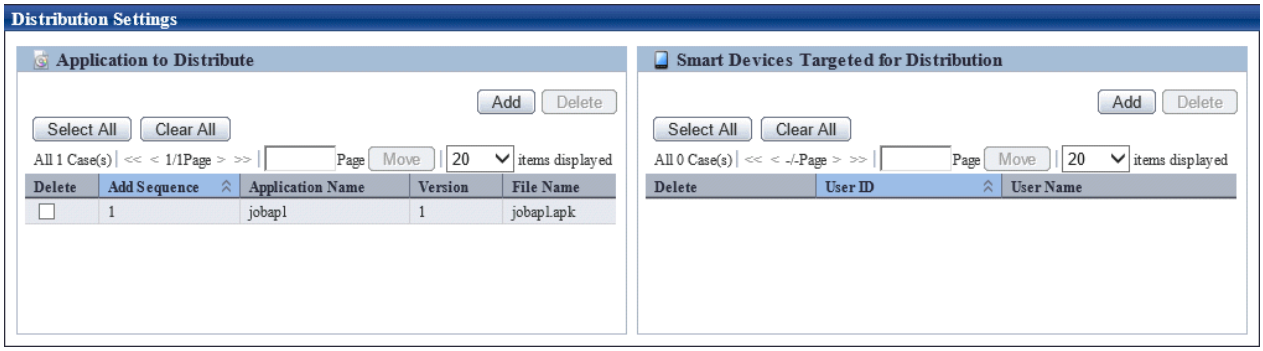
4. Select the application to distribute.
   Clicking **Add** for **Application to Distribute** in the left pane of the **Distribution Settings** tab displays the **Select Application** window.



The following table explains the setting items of this window:

Item	Description
OK	Registers the application and navigates to the **Select application** window.
Cancel	Navigates to the previous window without registering the application.
Application Name	Enter the application name. You can use up to 128 fullwidth characters and 256 halfwidth characters.
Version	Enter version information. You can use up to 16 halfwidth characters.
File Name	Click **Browse** and select the application to be distributed.
Browse	Starts the file selection window.

When you register an application and click **OK**, the application to be distributed is added to the list.



If you accidentally register an application, select the application you want to delete from the list and click **Delete**.

Point

Number of applications registered in one task

You can register up to 10 applications in one task.

When the number of applications exceeds 10, split the task.

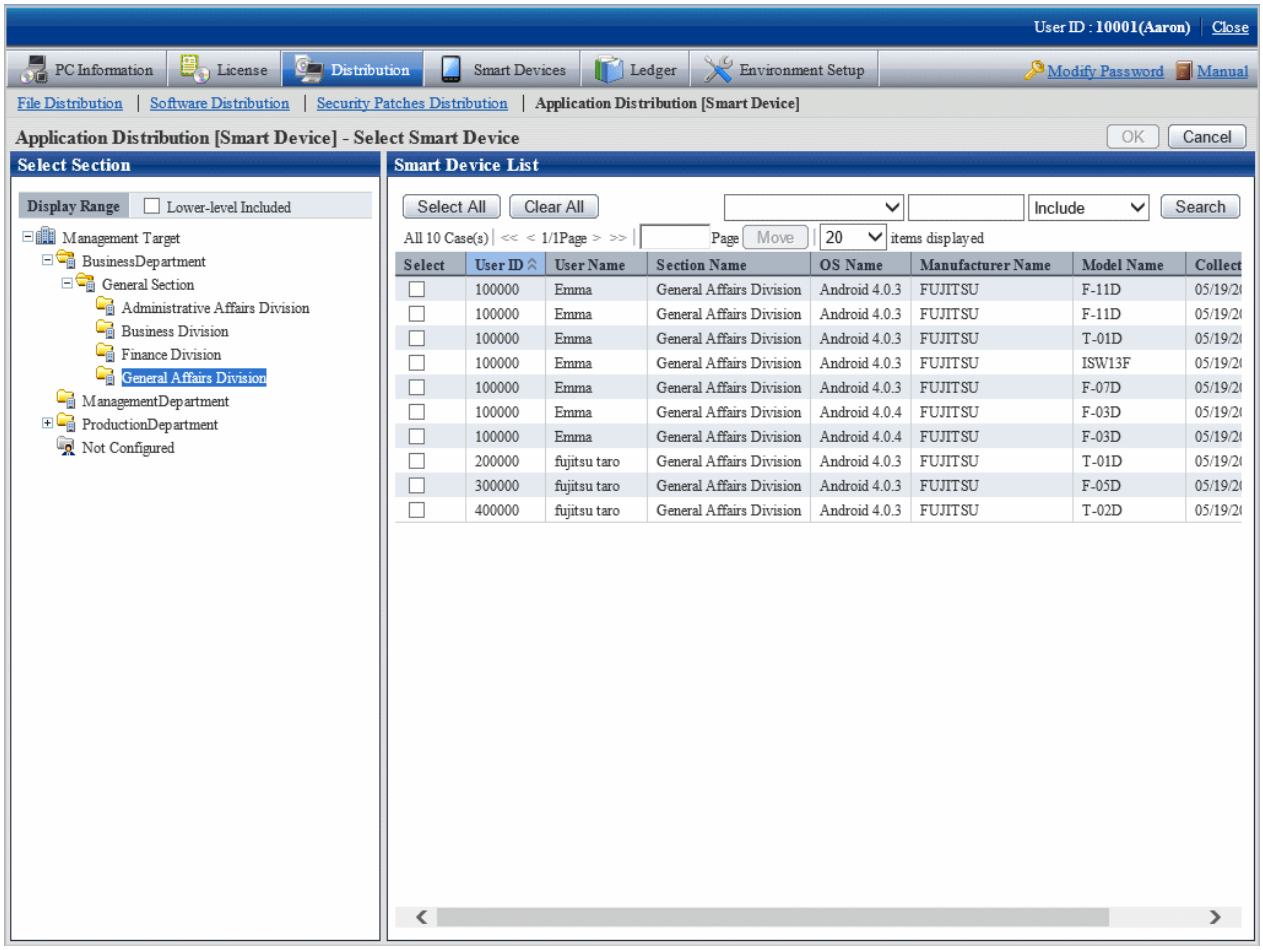
Point

About registering applications

- To distribute an application to an Android device, register the apk file.
- To distribute an application to an iOS device, compress the ipa file and manifest file to zip format before registering them.
- When registering applications, the apk file and the zip file cannot coexist.
- If a smart device is registered in a task
  - If an Android device is registered, you can register only apk files.
  - If an iOS device is registered, you can register only zip files.

5. Click **Add** for **Smart Devices Targeted for Distribution** in the bottom right pane of the window.

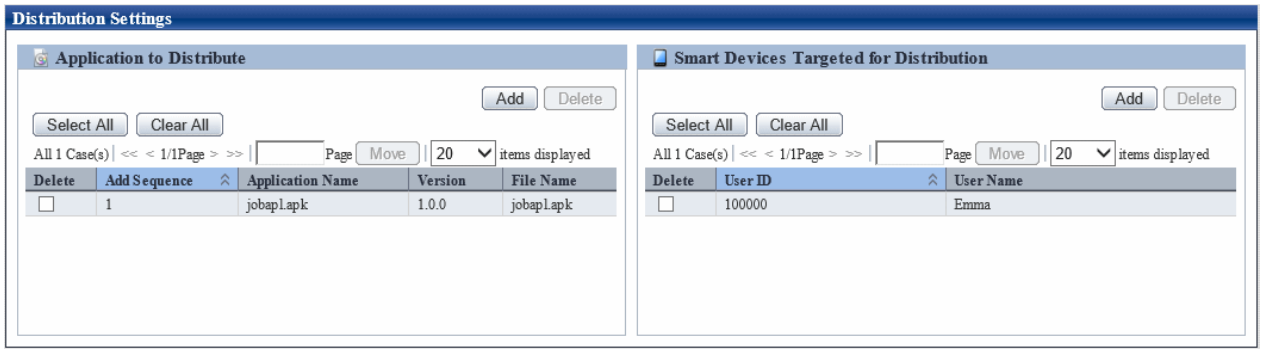
   The **Select Smart Device** window will be displayed.



The following table explains the setting items of this window:

Item	Description
Search	Filters the list based on whether a specific string is included in a specific column.
OK	Adds the selected smart device and navigates to the previous window.
Cancel	Navigates to the previous window without adding the smart device.
(Check box)	Select the smart device to be added.
User ID	Displays the user ID of the user who is using the smart device.
User Name	Displays the user name of the user who is using the smart device.
Section Name	Displays the name of the department to which the user who is using the smart device belongs.
OS Name	Displays the OS of the smart device.
Manufacturer Name	Displays the name of the smart device manufacturer.
Model Name	Displays the model name of the smart device.
Collection Date/Time	Displays the inventory collection date and time.

In the **Select Smart Device** window, select the smart device to be targeted for distribution, select the check box, and click **OK**. The smart device targeted for distribution will be added to the list.



Point

Number of smart devices registered in one task

You can register up to 500 smart devices in one task.

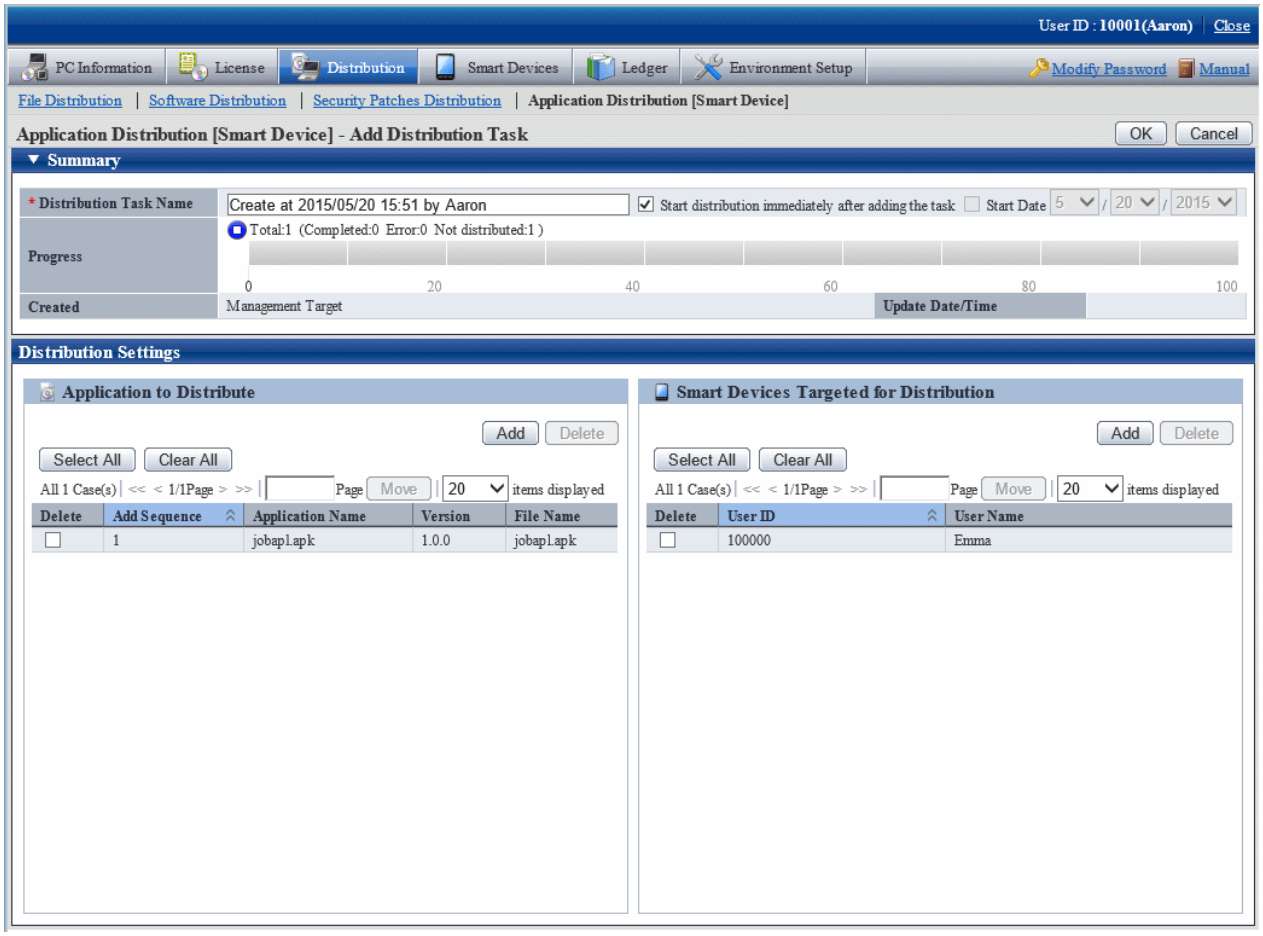
When the number of smart devices exceeds 500, split the task.

Point

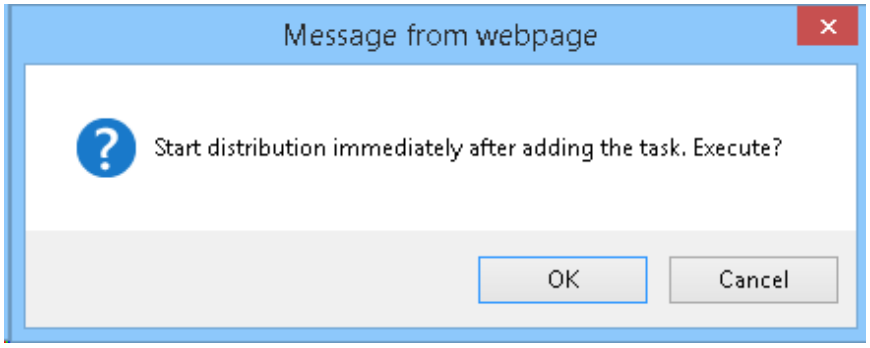
Smart devices that can be registered

- If an application has been registered in a task, you can register the following smart devices:
  - If an apk file is registered, you can register only an Android device.
  - If a zip file is registered, you can register only an iOS device.

6. If the settings are correct, click **OK**.



If **Start the distribution immediately after adding the task** is selected, click **OK**. The following message box will be displayed:



Click **OK** to add the distribution task and start distribution of the application.

If you click **Cancel**, distribution of the application does not start.

10.3 Operation

This section explains the following operation items for distributing applications:

- Checking distribution results
- Stopping distribution
- Performing distribution again
- Distributing ready distribution tasks

- Checking the content of registered distribution tasks
- Changing the content of registered distribution tasks
- Deleting unnecessary distribution tasks

10.3.1 Checking Distribution Results

You can check distribution results in the initial window of **Application Distribution [Smart Device]**.

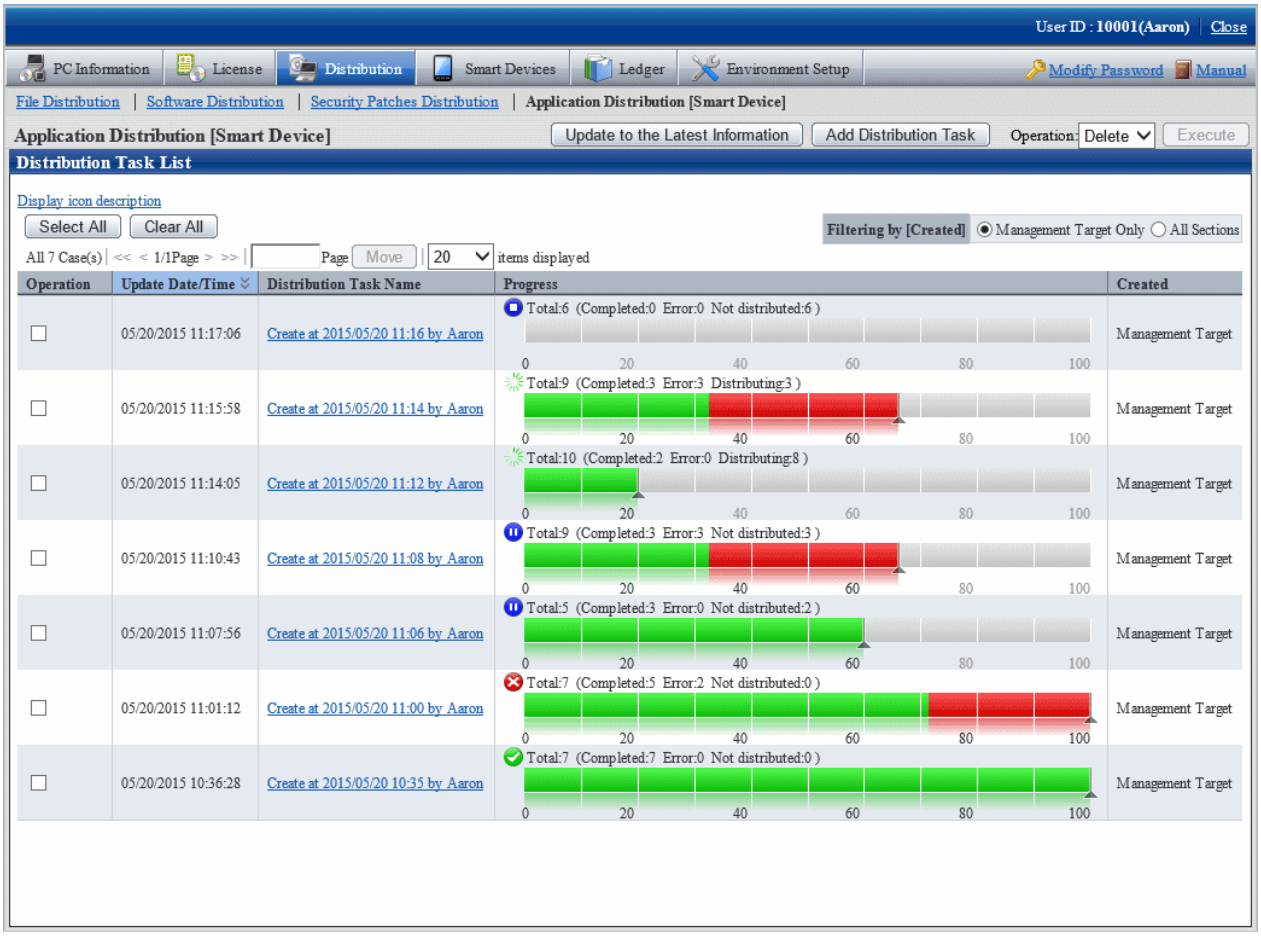
Note

- If no distribution result is reported within seven days of the last "Start" or "Stop" operation for the distribution task, distribution will be regarded as having ended abnormally.
- If you install an application on a smart device and the distribution result indicates that the distribution was successful, the distribution result does not change even if you uninstall the application.
- If an application whose distribution result indicates that distribution was successful is uninstalled from a smart device, the distribution result does not change even if you reinstall the application.
- Android allows you to install an application any number of times on a smart device before the distribution task is deleted.

The following explains the distribution results window:

When all distribution is completed and successful

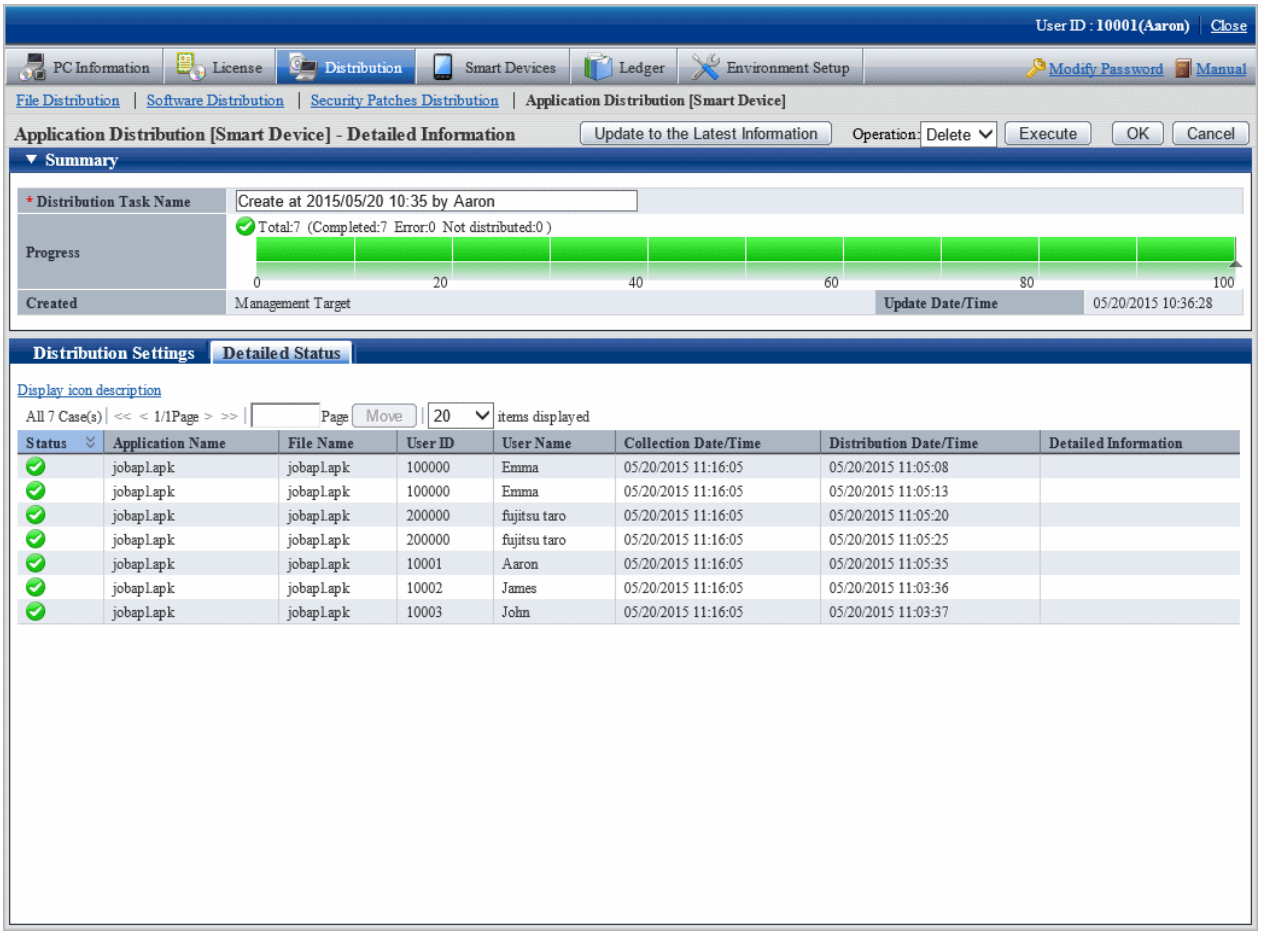
The icon is .



No particular operation is required after confirmation.

To check the details, click the link of the distribution task name.

You can check detailed information on the distribution result for the distribution task in the **Application Distribution [Smart Device] - Detailed Information** window.



The following table explains the setting items of this window:

Item	Description
Update to the Latest Information	Refreshes the information so that the latest information will be shown.
Operation / **Execute**	When you select an operation from the operation list for the distribution task and then click **Execute**, processing is performed for the distribution task. The list of operations is as follows: - **Delete** Deletes a distribution task. You cannot delete a task that is being distributed. To delete a task that is being distributed, stop it before deleting it. - **Start** Starts distribution of a task whose distribution has stopped. If you selected a task that is being distributed, it continues being distributed and processing ends normally. - **Stop**

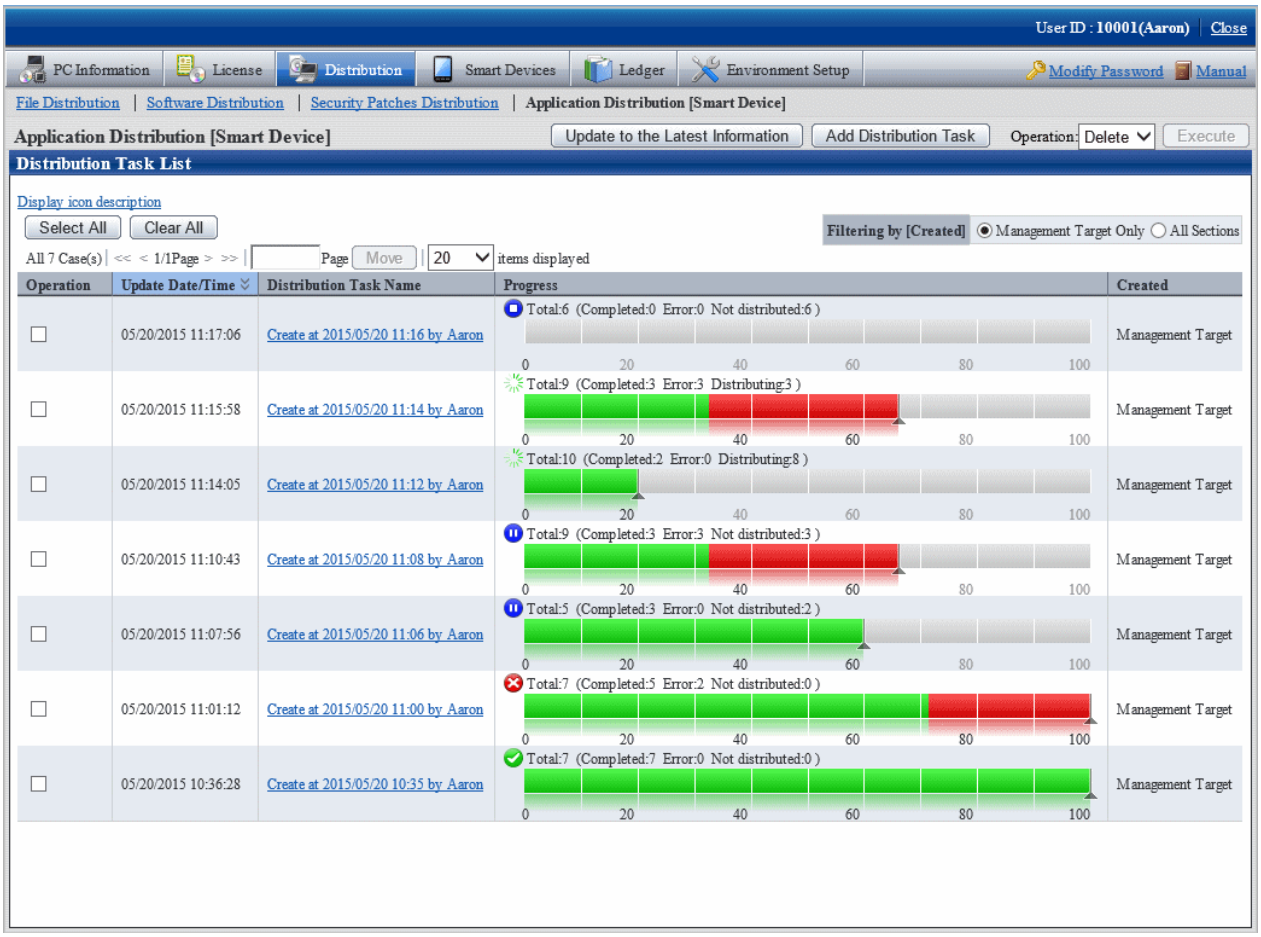
Item	Description
	Stops distribution of a task that is being distributed. If you selected a task that is stopped, it remains stopped and processing ends normally.
OK	Updates the settings and navigates the display to **Distribution Task List**.
Cancel	Navigates the display to **Distribution Task List** without updating the settings.
Distribution Task Name	Displays the name of the distribution task. The content is the same as in **Distribution Task List**.
Progress	Displays the progress of the distribution task. The content is the same as in **Distribution Task List**.
Created	Indicates the department to which the manager who created the distribution task belongs. The content is the same as in **Distribution Task List**.
Update Date/Time	Displays the date and time at which the distribution task was registered or updated. The content is the same as in **Distribution Task List**.

The following table explains the content of the **Detailed status** tab:

Item	Description
Status	Same as the icon displayed for **Progress** in the **Distribution Task List** window.
Application Name	Displays the name of the application to be distributed.
File Name	Displays the file name of the application to be distributed.
User ID	Displays the user ID of the user who is using the smart device targeted for distribution.
User Name	Displays the user name of the user who is using the smart device targeted for distribution.
Collection Date/Time	Displays the inventory collection date and time.
Distribution Date/Time	Displays the distribution date and time.
Detailed Information	Displays details of the error if distribution fails.

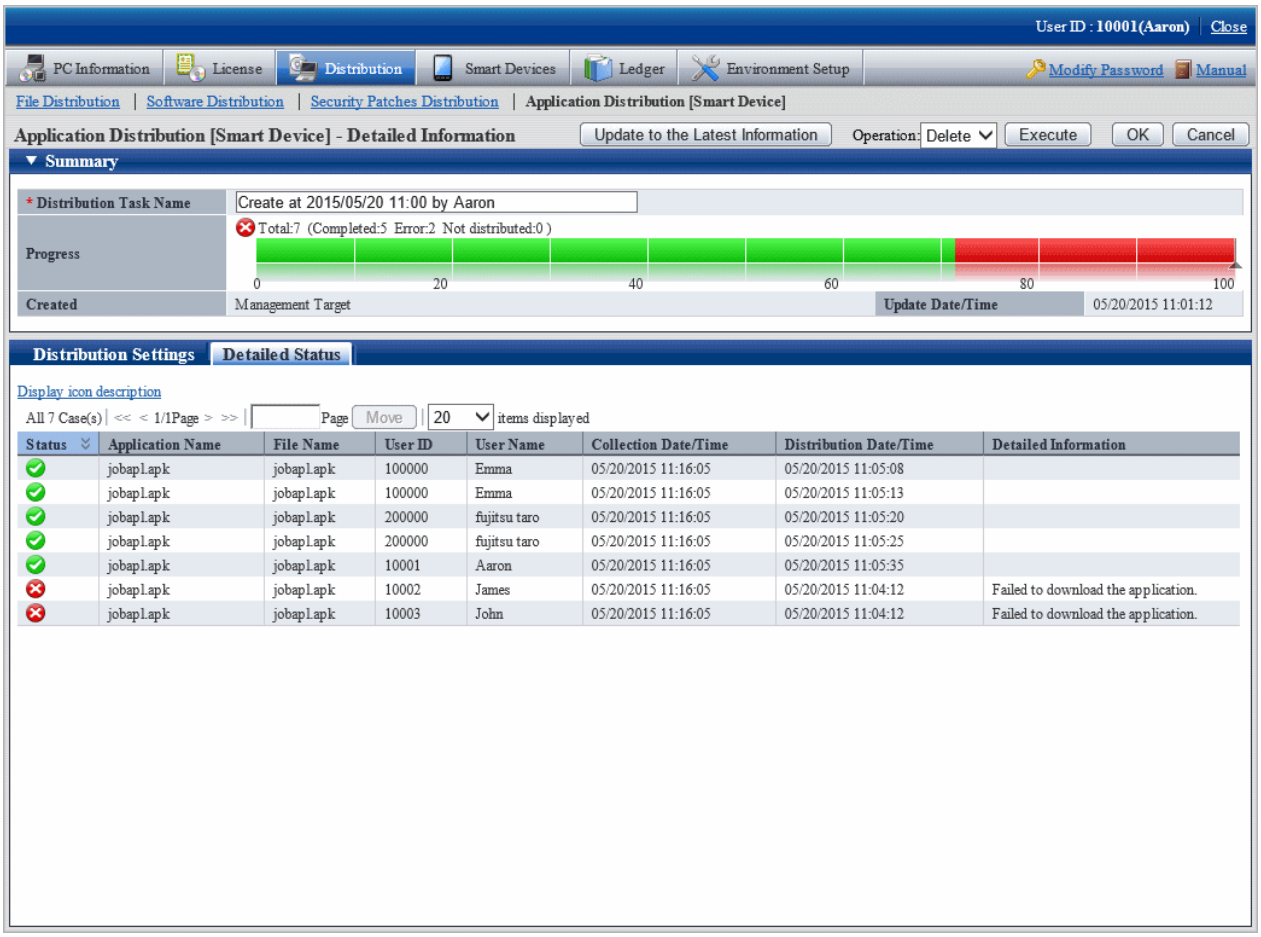
When all distribution is completed but some distribution fails

The icon is .



To view detailed information, click the link of the distribution task name.

You can check detailed information on the distribution result for the distribution task in the **Application Distribution [Smart Device] - Detailed Information** window.



The **Detailed status** tab in the bottom pane of the window enables you to check which application failed to be distributed to which smart device.

Check the error details displayed in the **Detailed Information** column and ensure that distribution to the relevant smart device is possible.

The following table lists the error details displayed in the **Detailed Information** column:

OS type	Detailed information
Android	Failed to access external storage. Failed to download the application. Failed to install the application. No response.
iOS	Failed to download the application. No response.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for detailed information on the errors.

10.3.2 Stopping Distribution

You can stop distribution for a smart device for which distribution has not been completed.

Note

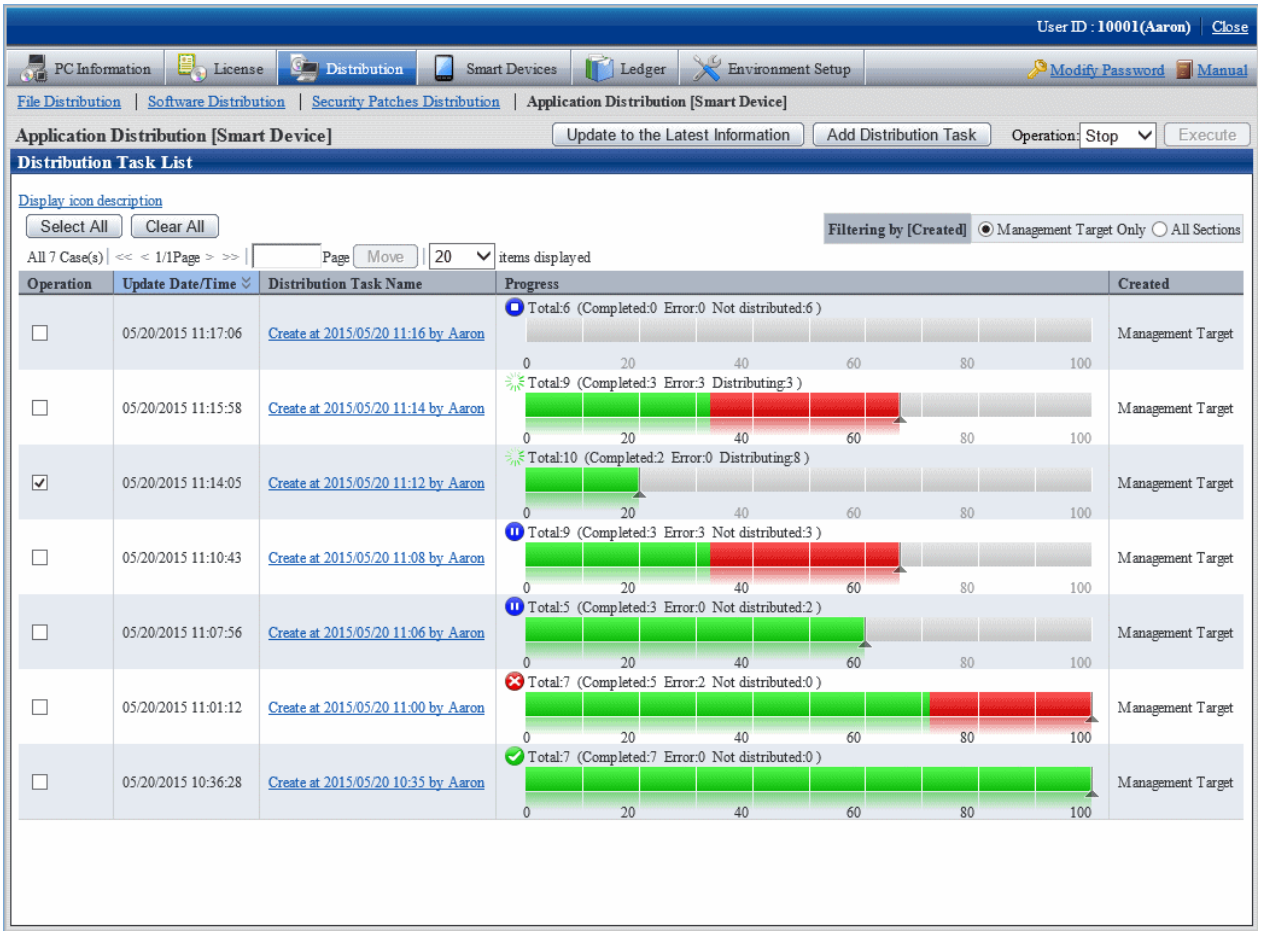
Android does not allow you to stop distribution to the following smart devices:

- A smart device that is turned off

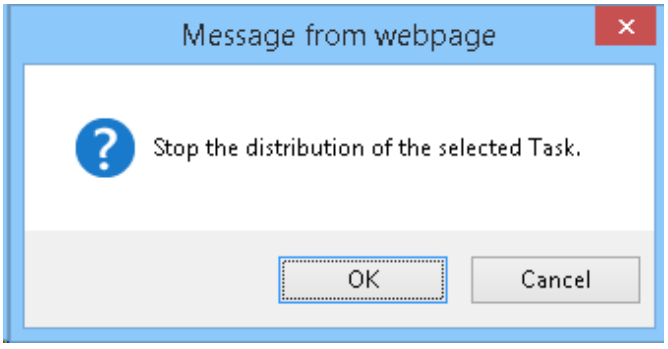
- A smart device that is not connected to a network

No result is reported even if you stop distribution to these smart devices, so the window continues to indicate that the stop process is in progress. If no distribution result is reported within seven days, distribution will be regarded as having ended abnormally.

Select the distribution task whose distribution you want to stop, select **Stop** in the **Operation** box, and click **Execute**.



The following message box will be displayed:

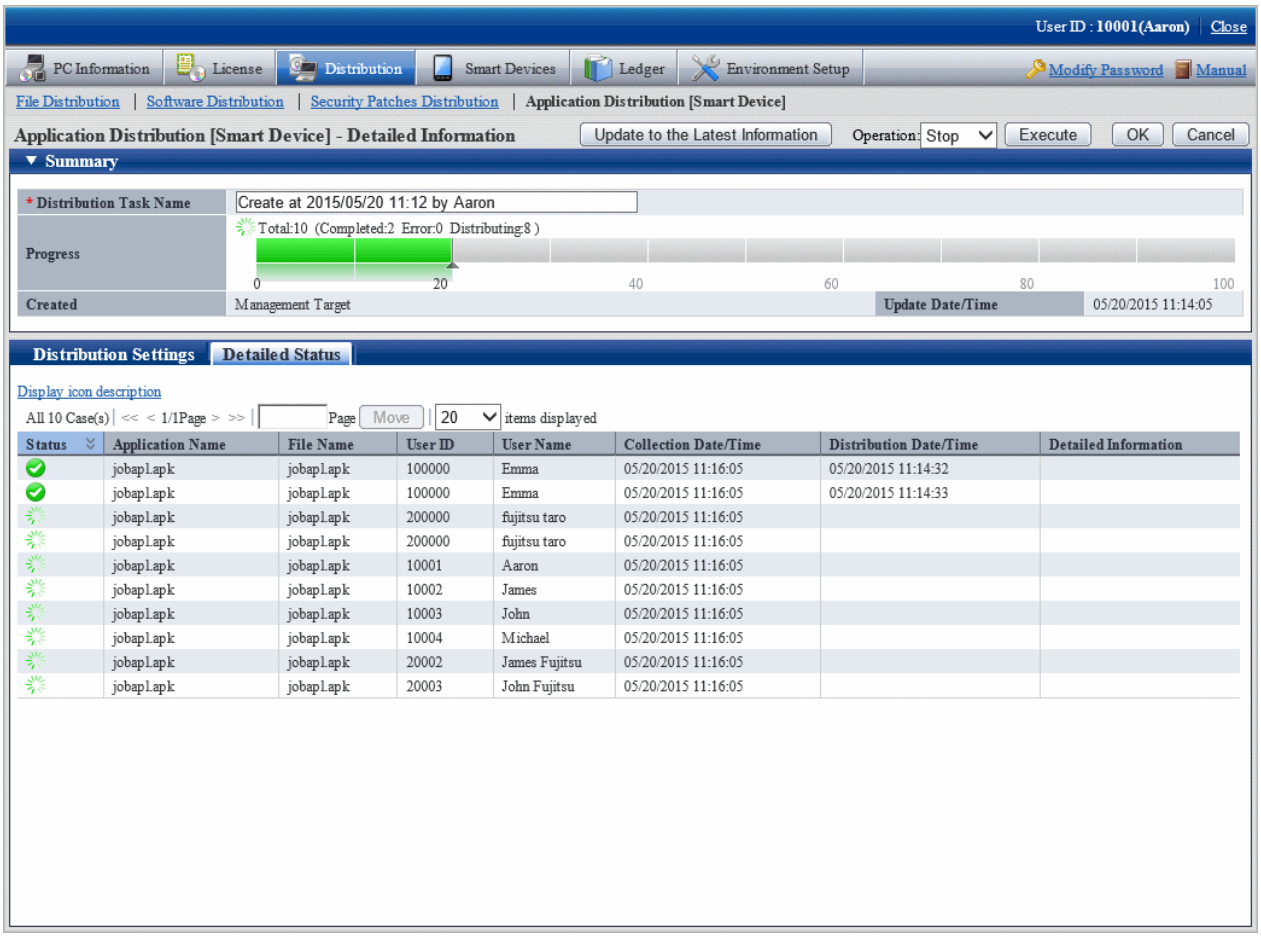


Click **OK** to stop distribution of the application.

If you click **Cancel**, distribution of the application does not stop.

If you select multiple distribution tasks including one that cannot be stopped, this process will stop only the distribution tasks that can be stopped.

The operation for stopping distribution is also available from the **Application Distribution [Smart Device] - Detailed Information** window. To stop distribution, select **Stop** in the **Operation** box, and click **Execute**.



10.3.3 Performing Distribution Again

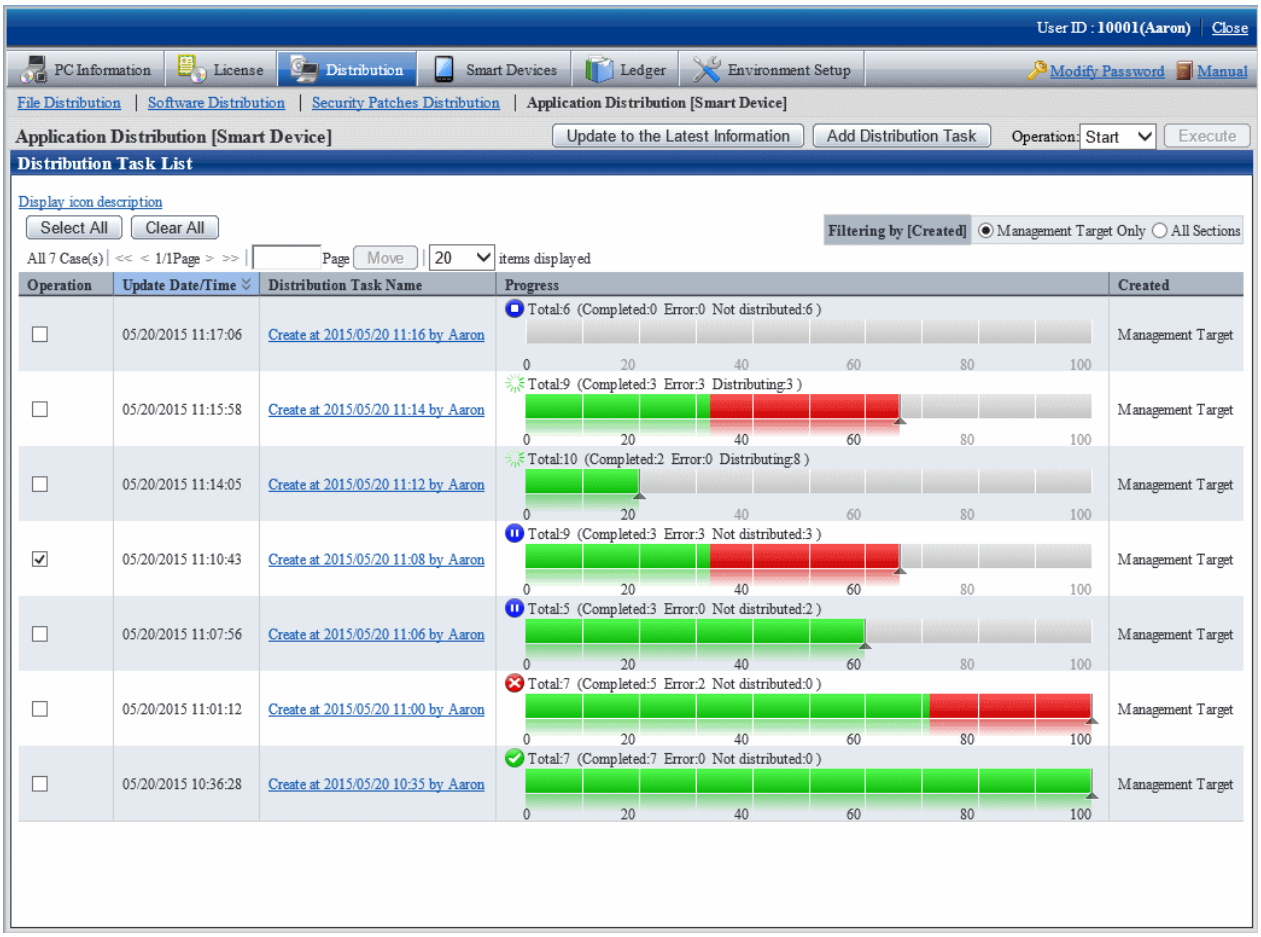
You can redistribute an application for the following:

- Smart device for which distribution was stopped (smart device for which distribution is not completed)

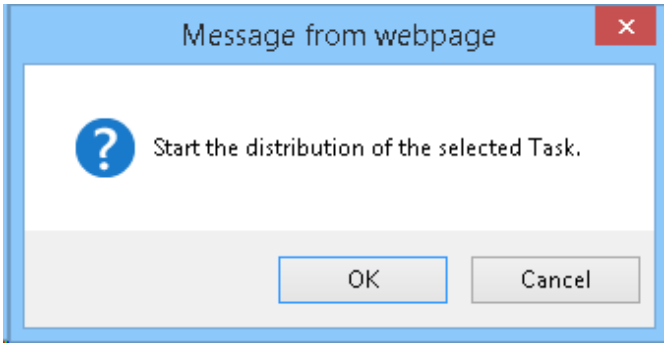
However, if distribution has failed, the state will continue to indicate that distribution failed until you remove the cause of the failure.

Refer to "When all distribution is completed but some distribution fails", check the cause, take action, and perform distribution again.

Select the distribution task you want to redistribute, select **Start** in the **Operation** box, and click **Execute**.



The following message box will be displayed:

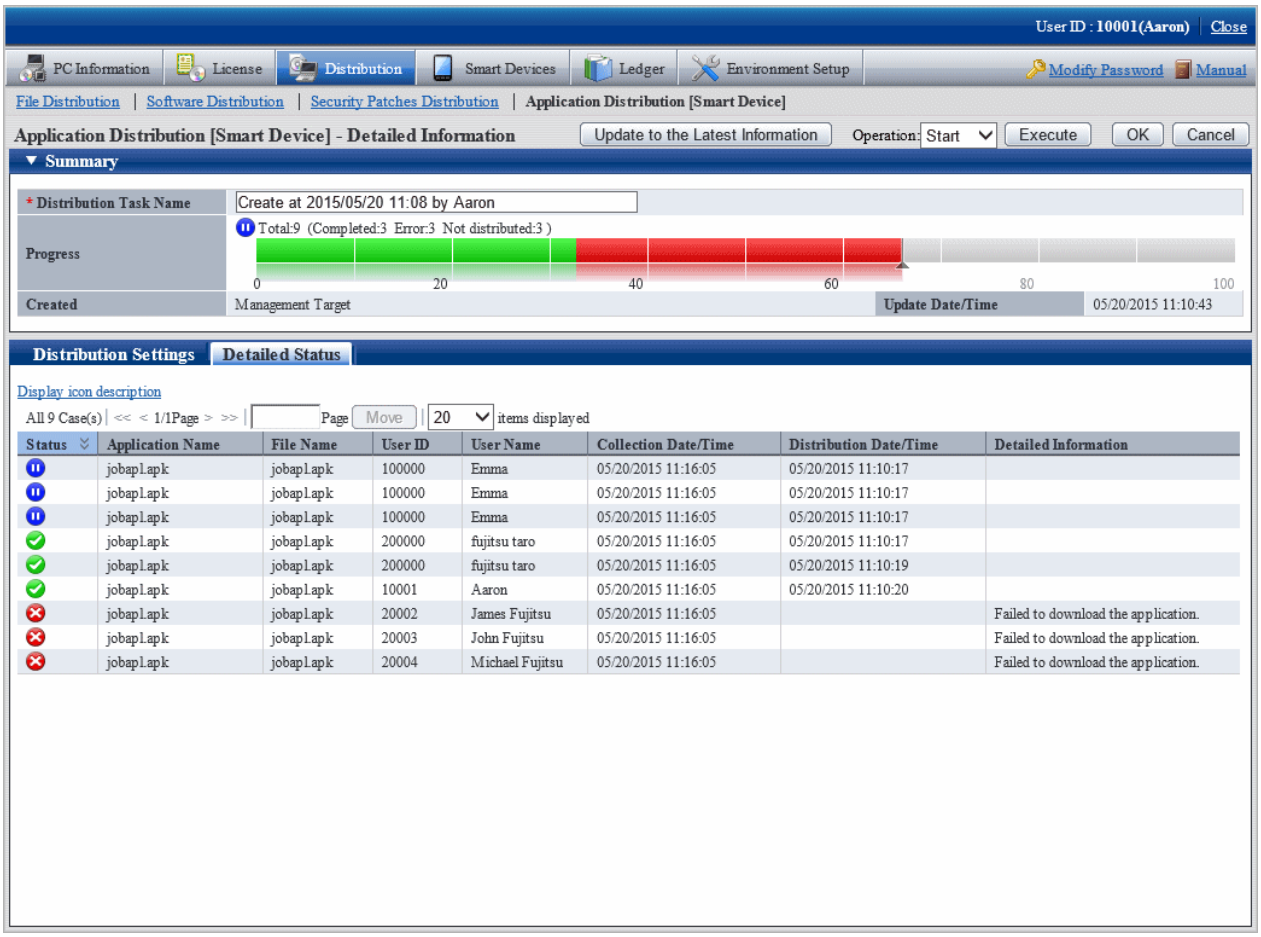


Click **OK** to start distribution of the application.

If you click **Cancel**, distribution of the application does not start.

If you select multiple distribution tasks including one that cannot be started, this process will start only the distribution tasks that can be started.

The operation for starting distribution is also available from the details window. To start distribution, select **Start** in the **Operation** box, and click **Execute**.

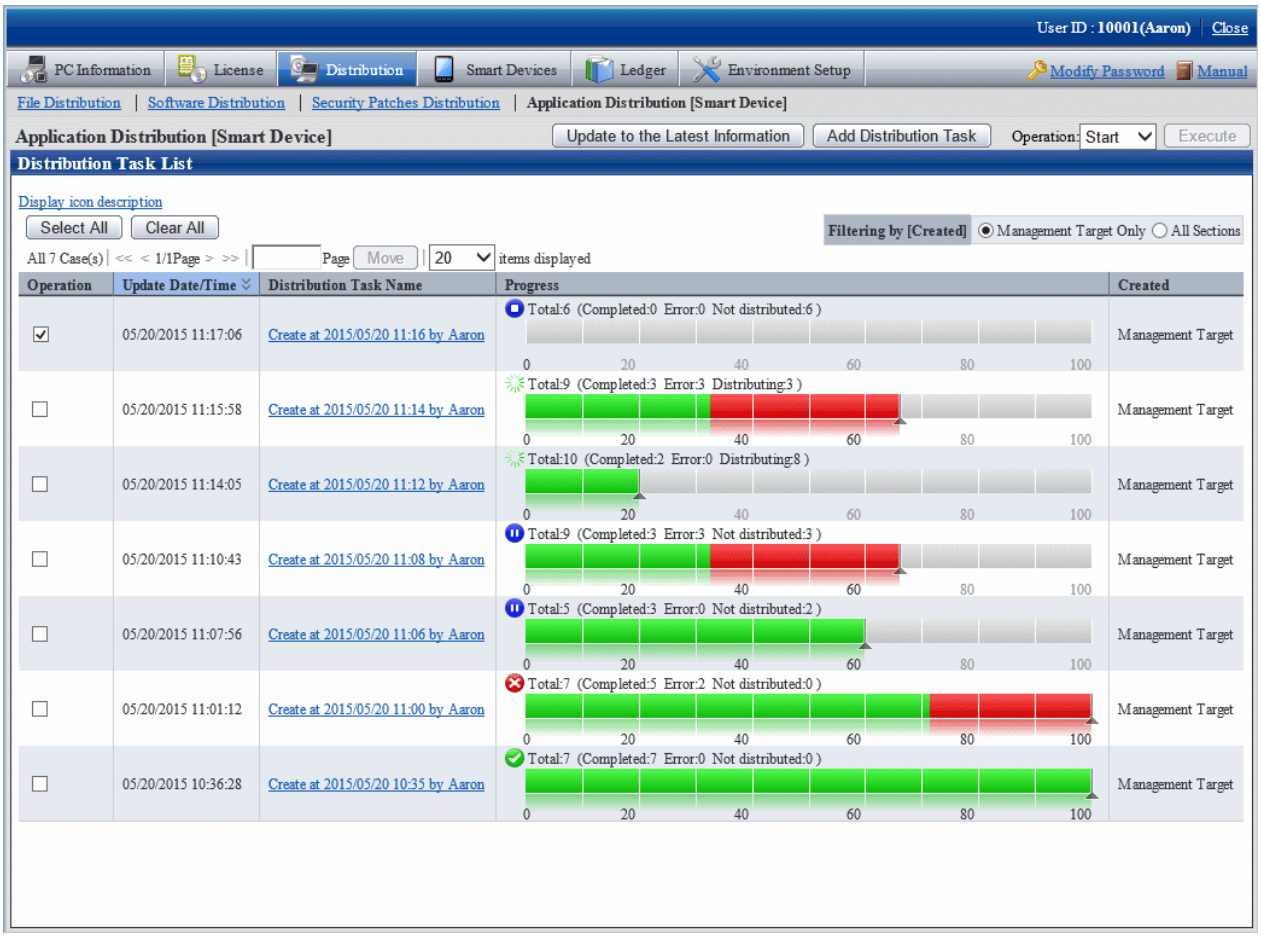


10.3.4 Distributing Ready Distribution Tasks

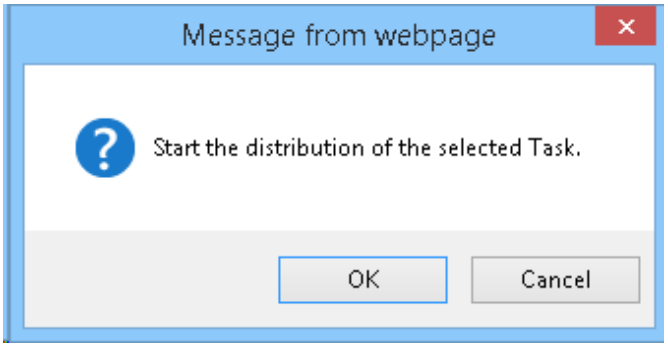
If you register an application to be distributed or a smart device targeted for distribution and you clear **Start the distribution immediately after adding** as a distribution task, the state will indicate that preparation for distribution is completed but distribution will not be performed.

To distribute a distribution task for which distribution preparation is completed, select the distribution task you want to distribute, select **Start** in the **Operation** box, and click **Execute**.

Even if you specify **Start Date** for the distribution task, distribution will start immediately after you perform this operation.



The following message box will be displayed:



Click **OK** to start distribution of the application.

If you click **Cancel**, distribution of the application does not start.

10.3.5 Checking the Content of Registered Distribution Tasks

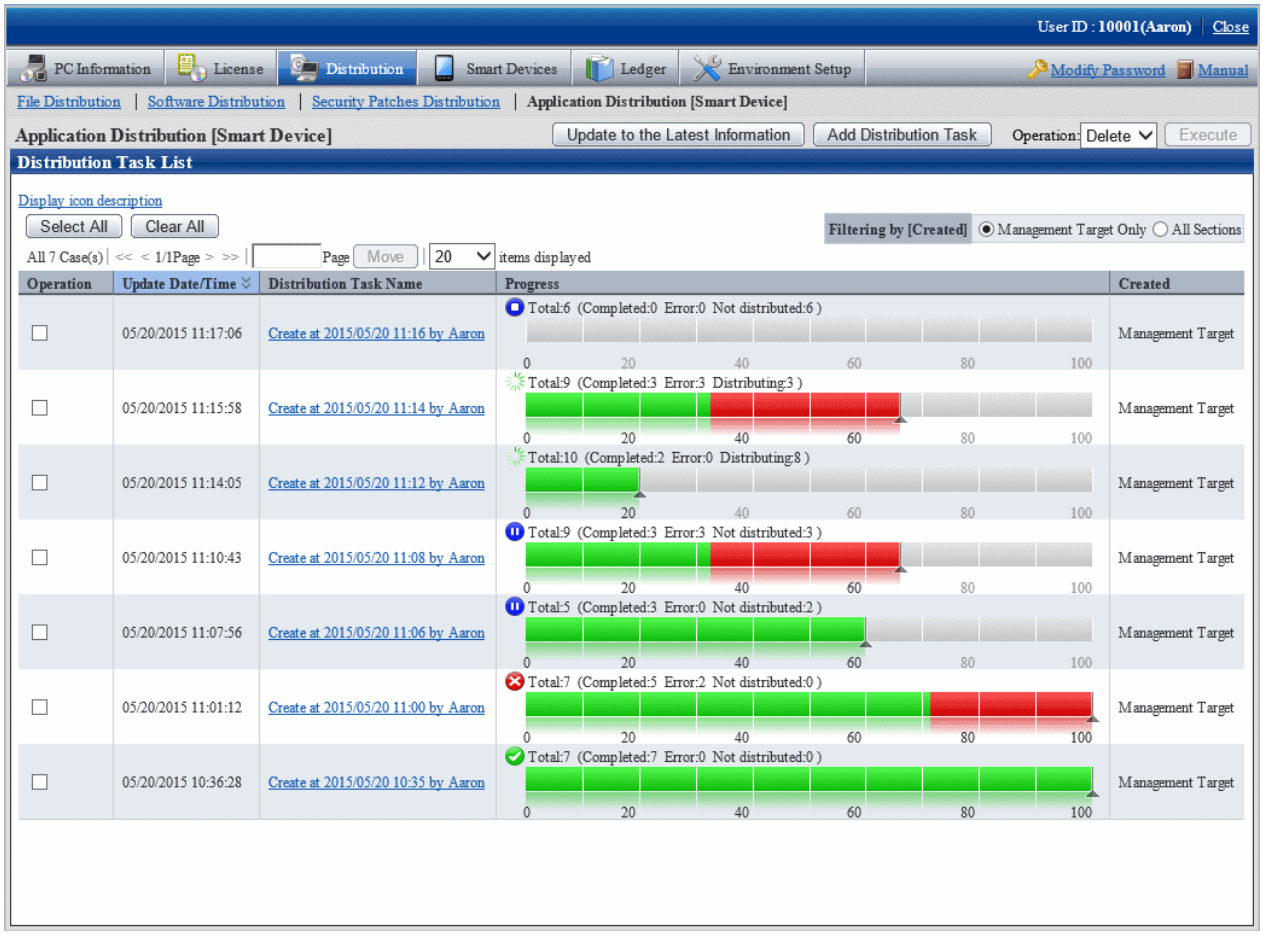
You can check the content of a distribution task registered in the distribution settings.

The procedure is as follows:

1. Log in to the main menu.

2. Click **Asset Management** > **Distribution** > **Application Distribution [Smart Device]**.

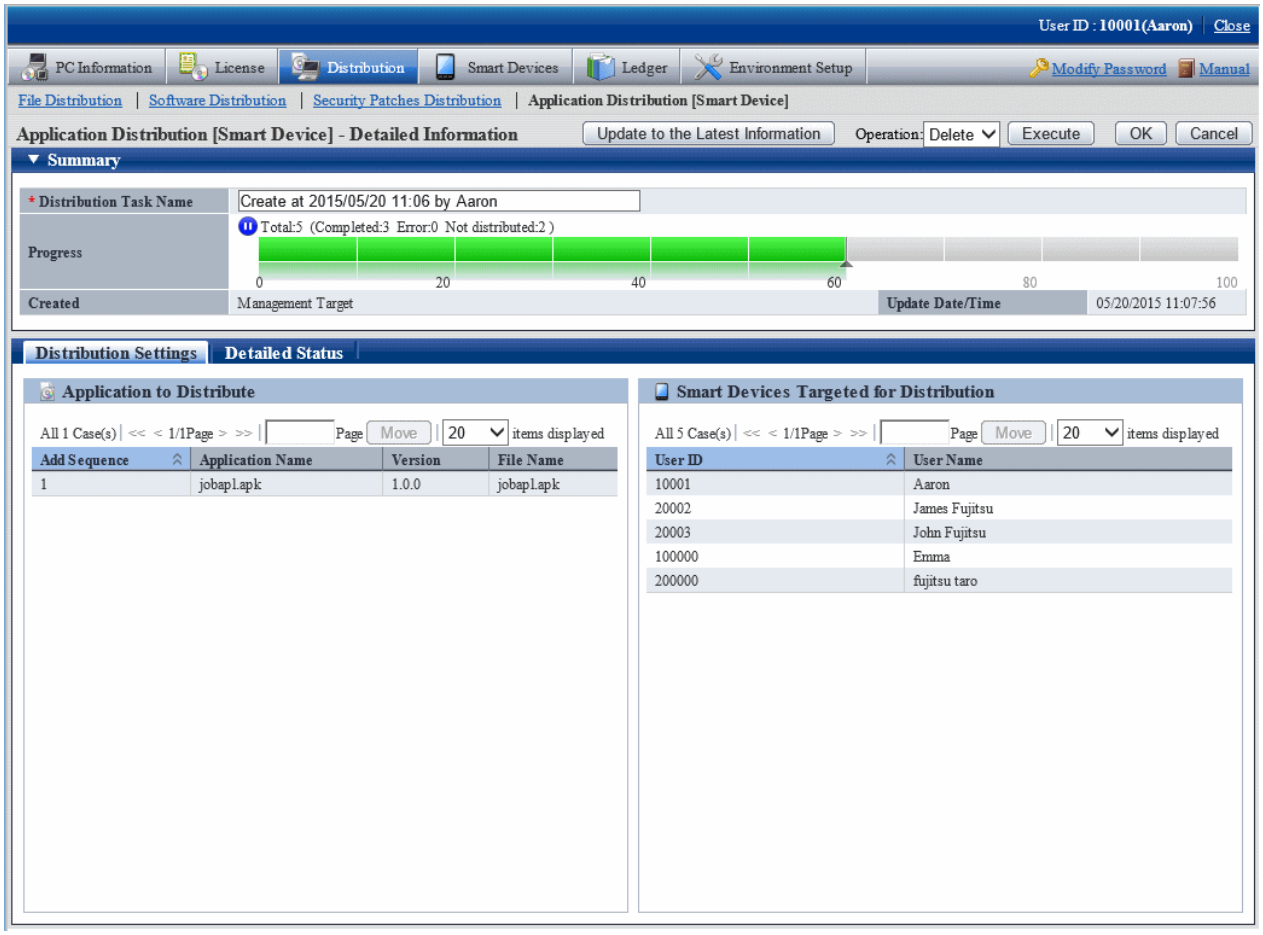
   The initial window of **Application Distribution [Smart Device]** is displayed.



3. Click the distribution task name you want to check.

4. Select the **Distribution Settings** tab in the lower half of the **Application Distribution [Smart Device]** window.

   You can check the application to be distributed and the smart device targeted for distribution.



10.3.6 Changing the Content of Registered Distribution Tasks

You can change the following content of a distribution task registered in the distribution settings:

- Applications to be distributed
- Smart devices targeted for distribution
- Distribution start date

However, you can change the content only for distribution tasks for which distribution preparation is completed.

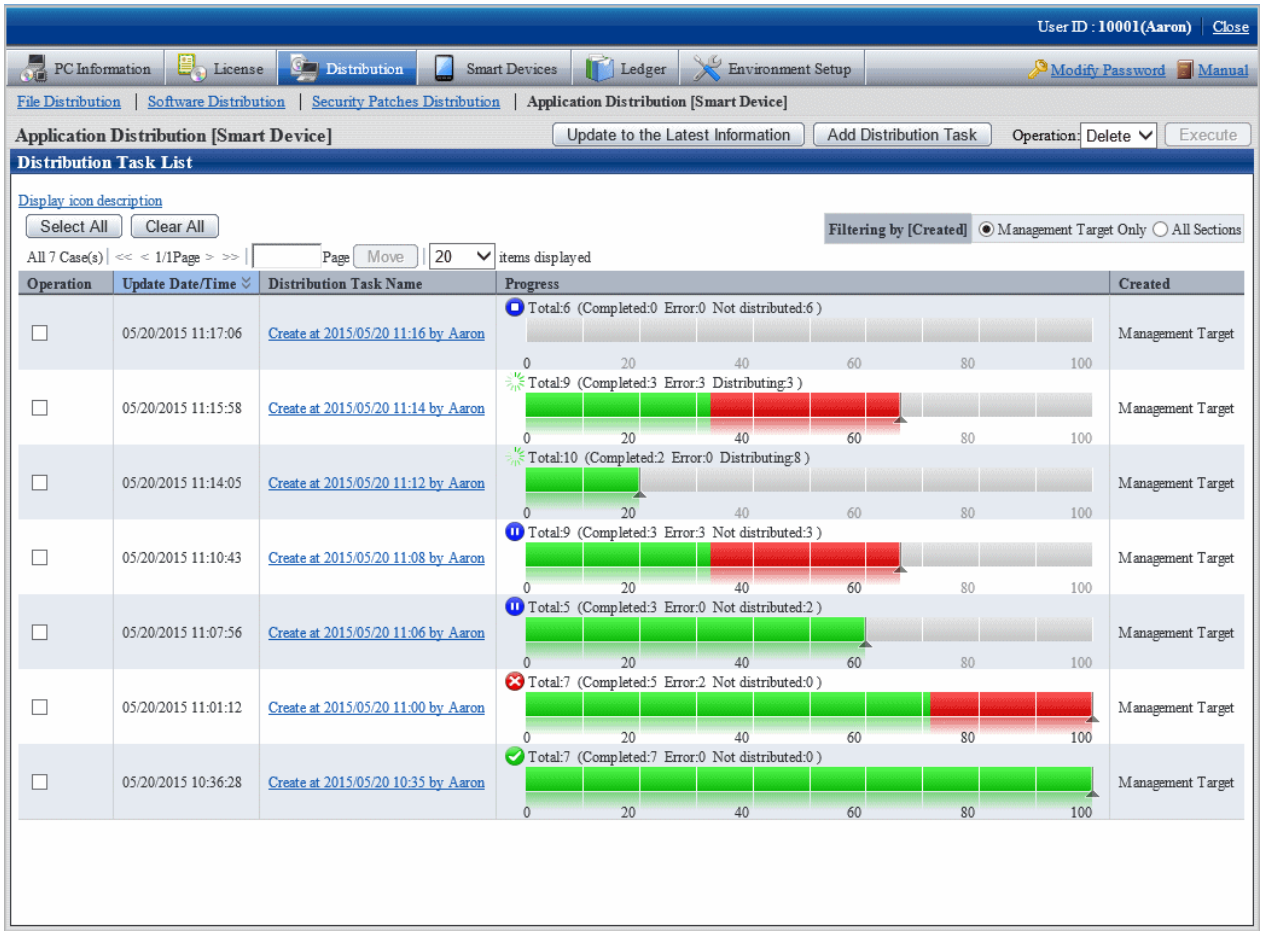
You cannot change registered content after distribution has been started.

The procedure is as follows:

1. Log in to the main menu.

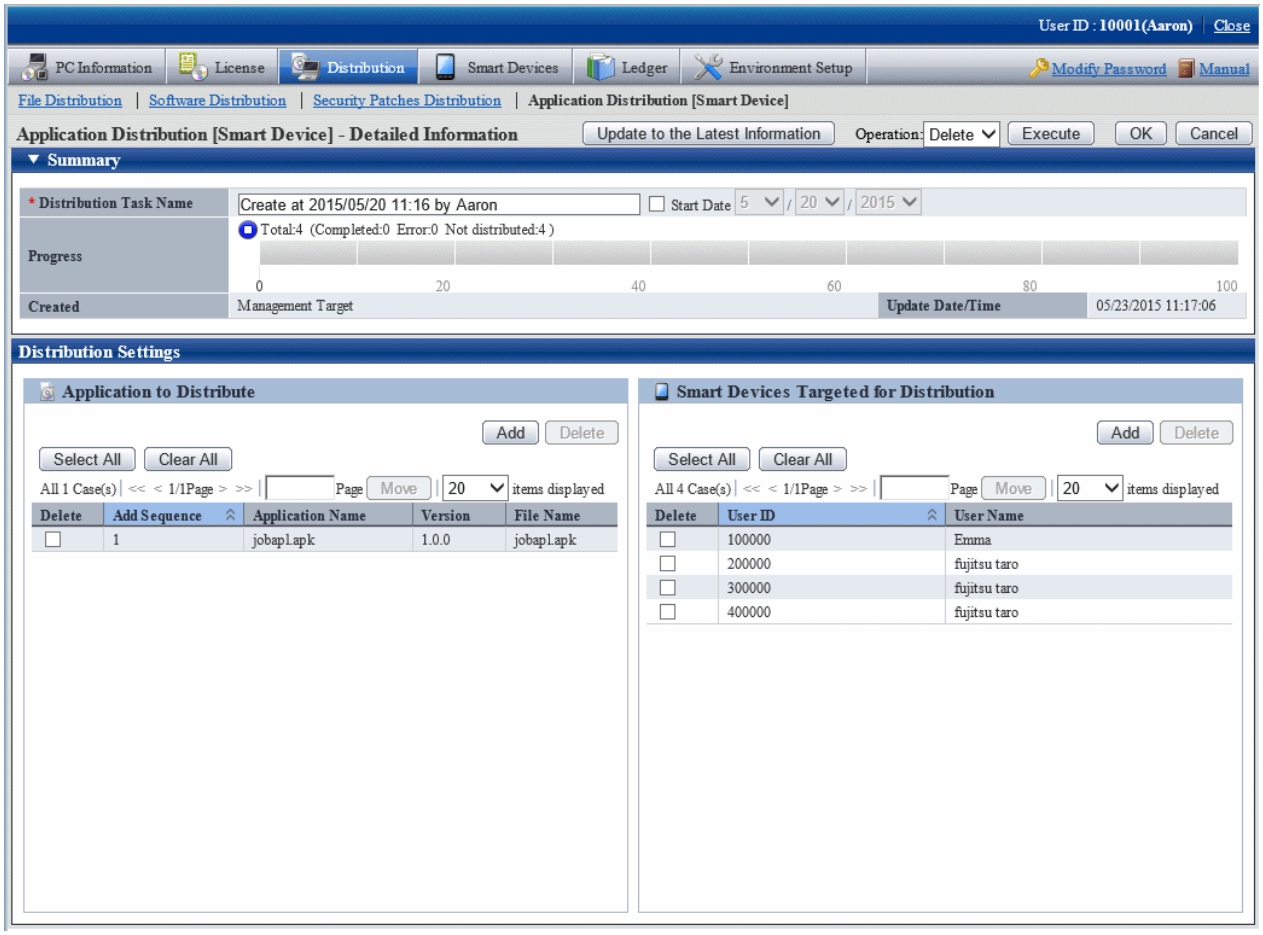
2. Click **Asset Management** > **Distribution** > **Application Distribution [Smart Device]**.

   The initial window of **Application Distribution [Smart Device]** is displayed. Click the distribution task name.



3. Select the **Distribution Settings** tab in the lower half of the Application Distribution [Smart Device] - Detailed Information window.

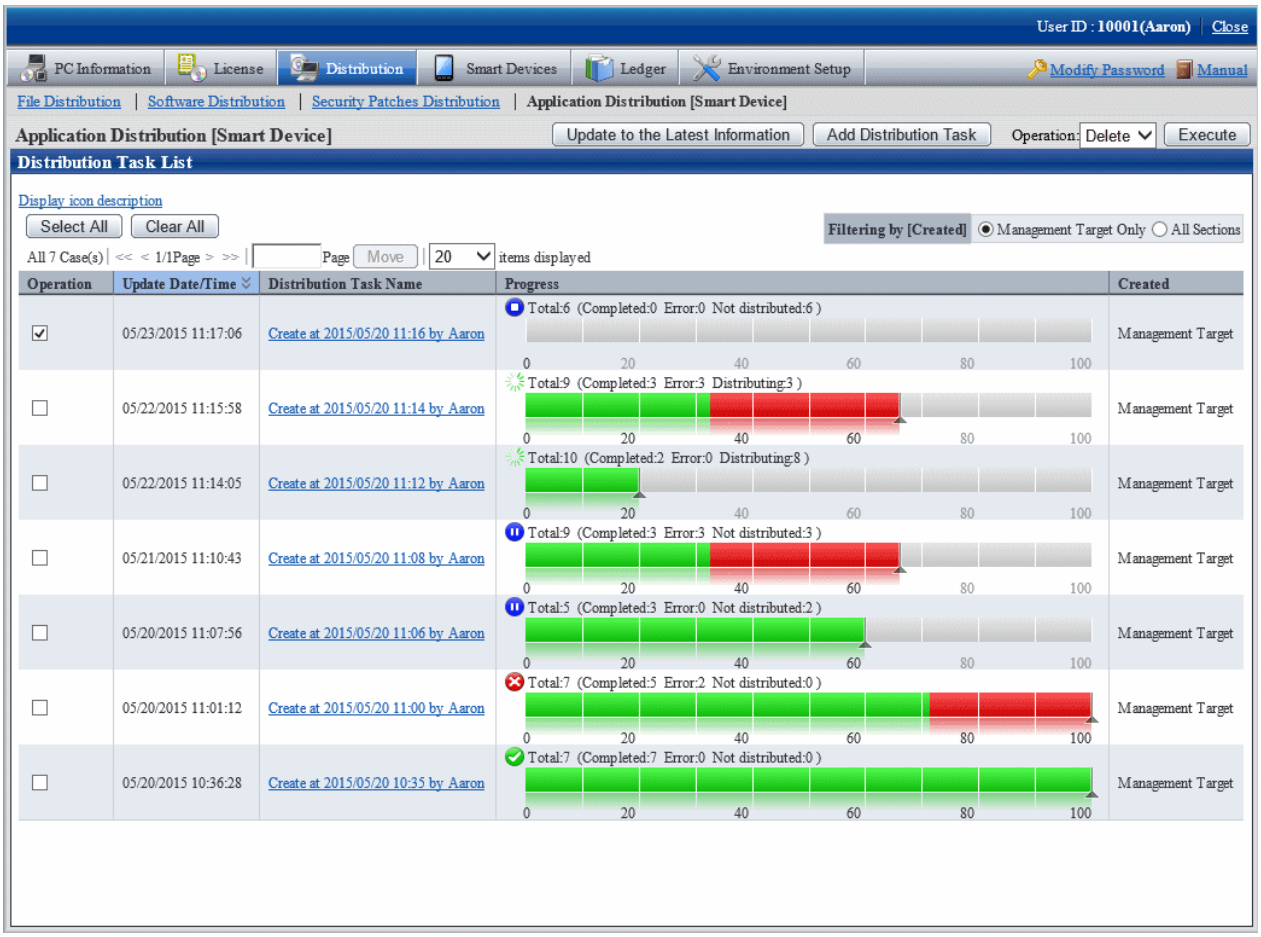
   You can change the applications to be distributed, the smart devices targeted for distribution, and the distribution start date.



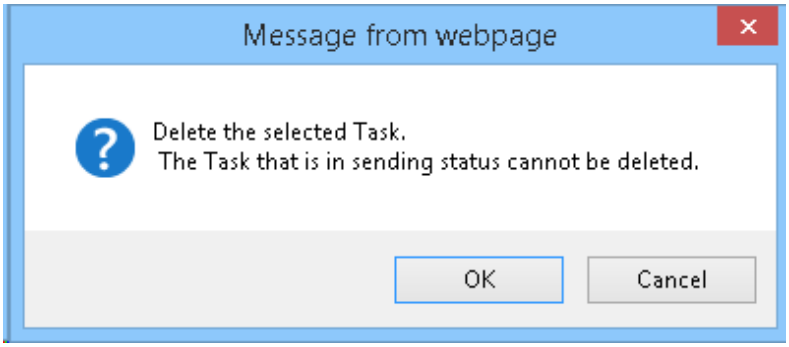
10.3.7 Deleting Unnecessary Distribution Tasks

Distribution tasks cannot be deleted automatically.

To delete unnecessary distribution tasks such as those that were completed or accidentally registered, select the distribution task in the initial window of **Application Distribution [Smart Device]**, select **Delete**, and click **Execute**.



The following message box will be displayed:



Click **OK** to delete the distribution task.

If you click **Cancel**, the distribution task is not deleted.

If you select multiple distribution tasks including one that cannot be deleted, this process will delete only the distribution tasks that can be deleted.

You cannot delete a distribution task that is being distributed. Stop the distribution before deleting the distribution task.

Chapter 11 Assets Management by Ledger

This chapter describes how to manage asset through ledger.

11.1 Management Ledger Settings

This section describes how to set management ledger.

Perform the following settings before using management ledger.

- "11.1.1 Set Contract Expiration Notification"
- "11.1.2 Set Registration for Device Information"
- "11.1.3 Set Security Auditing"
- "11.1.4 Set History Management"
- "11.1.5 Set Asset Classification Name"
- "11.1.6 Set Window Item Name"
- "11.1.7 Set Other Product Information Reflection"

11.1.1 Set Contract Expiration Notification

As the contract information of device (PC and device) managed in Systemwalker Desktop Patrol, for device with **Lease**, **Rent** or **Maintenance** set in **Contract Class**, they can be performed contract expiration notification in the following cases.

- When device approaching the set **Contract End Date**(prior notice of contract period) exist
- When device exceeding the set **Contract End Date**(prior notice of contract period) exist

The notification can be emailed to the address specified in the **Event Settings** window. Refer to "2.5 Set Alarm Notification" for details on the **Event Settings** window.

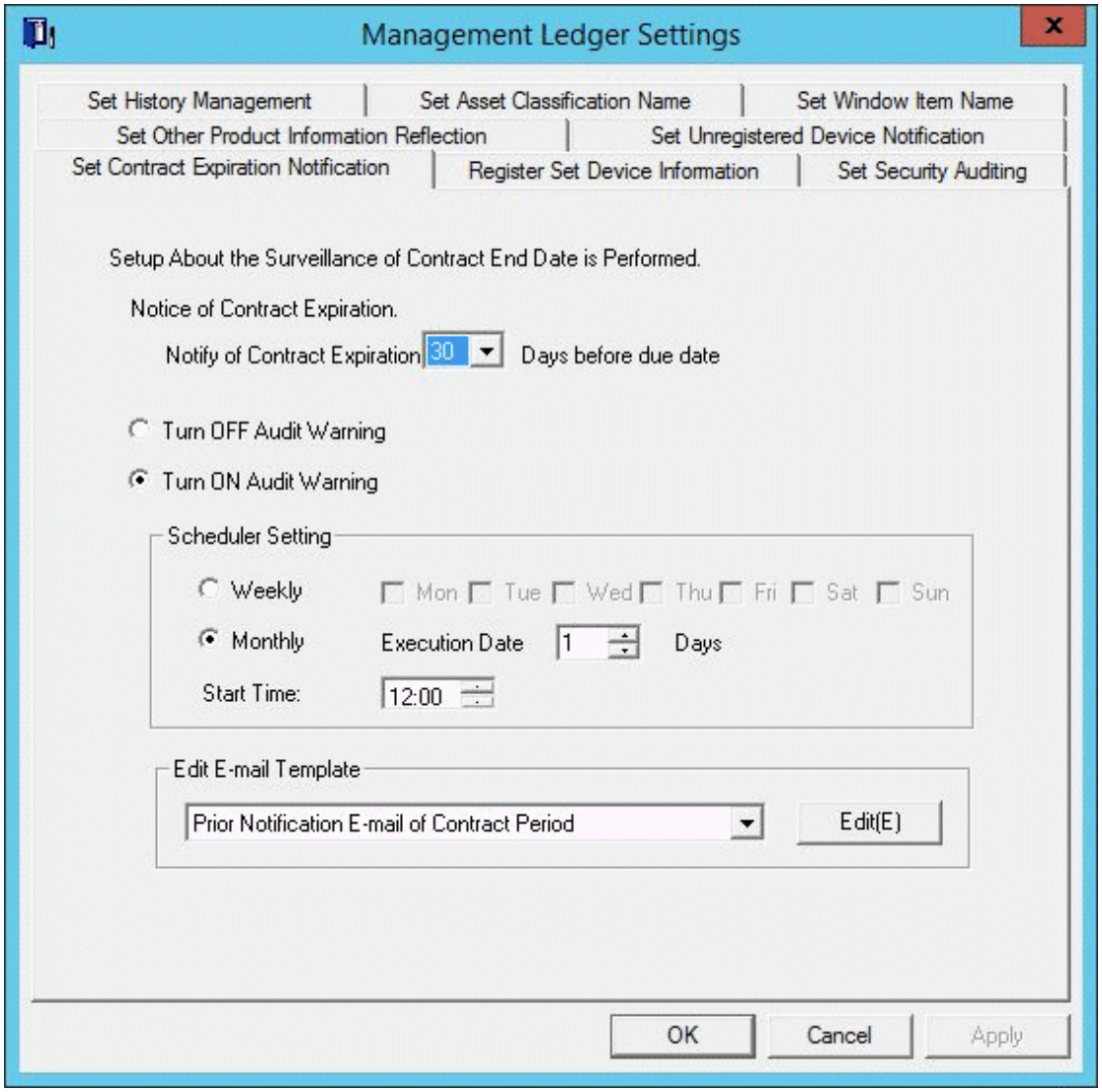
The procedure for setting the contract expiration notification is as follows.

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed

2. Select the **Set Contract Expiration Notification** tab.

   The following window will be displayed



3. Set the conditions and content for contract expiration notification.

   Set the following information and click the **OK** button.

   The information is set.

Item	Descriptions
Notice of Contract Expiration	Number of days before **Contract End Date** when a notice of contract expiration will be sent. The following values can be specified: **30**, **60**, **90**, and **180**. The initial value is **30**.
Turn OFF Audit Warning	Selected when not performing contract expiration notification.
Turn ON Audit Warning (Initial Value)	Selected when performing contract expiration notification. However, it cannot be selected when the setting in the **Settings of E-mail Environment** tab has not been completed. After selecting and clicking the **OK** button, the following tasks for contract expiration notification will be registered in the task function of Windows.

Item	Descriptions
	- Name: SWDTPAS_AlarmW.job - Operating authority: system account For the operation of contract expiration notification, refer to the later "Operation of contract expiration notification".
Scheduler Setting	Set after selecting **Turn ON Audit Warning**. As the date for performing warning auditing, select **Weekly** or **Monthly**. The initial value is **Monthly**. After selecting **Weekly**, the week checkbox can be checked. **Execution Date** can be specified if **Monthly** is selected. Besides, as **Execution Date**, when a date which does not exist in the set month has been specified, warning auditing cannot be performed in this month. Thus, when executing at the end of the month, study the use of executing at 00:00 on the first day of each month. If **Monthly** is selected, the initial value is **1st Day**, and the start time is the current time. Or set **Start Time** of starting warning auditing.
Edit E-mail Template	When editing the notification content of initial settings, select the following items and click the **Edit** button. - **Prior Notification E-mail of Contract Period** - **Contract Expiration Warning E-mail** For details of editing E-mail template, refer to the later "Edit e-mail template".

Operation of contract expiration notification

Contract expiration notification is operated according to the following information.

- Contract End Date

  It is the contract end date set in the contract information.

- Startup Date

  This is the date on which CS was started and notice of contract expiration was sent in accordance with the scheduled conditions.

- Prior Notice Date

  It is the information of **Notice of Contract Expiration** set according to the procedure above.

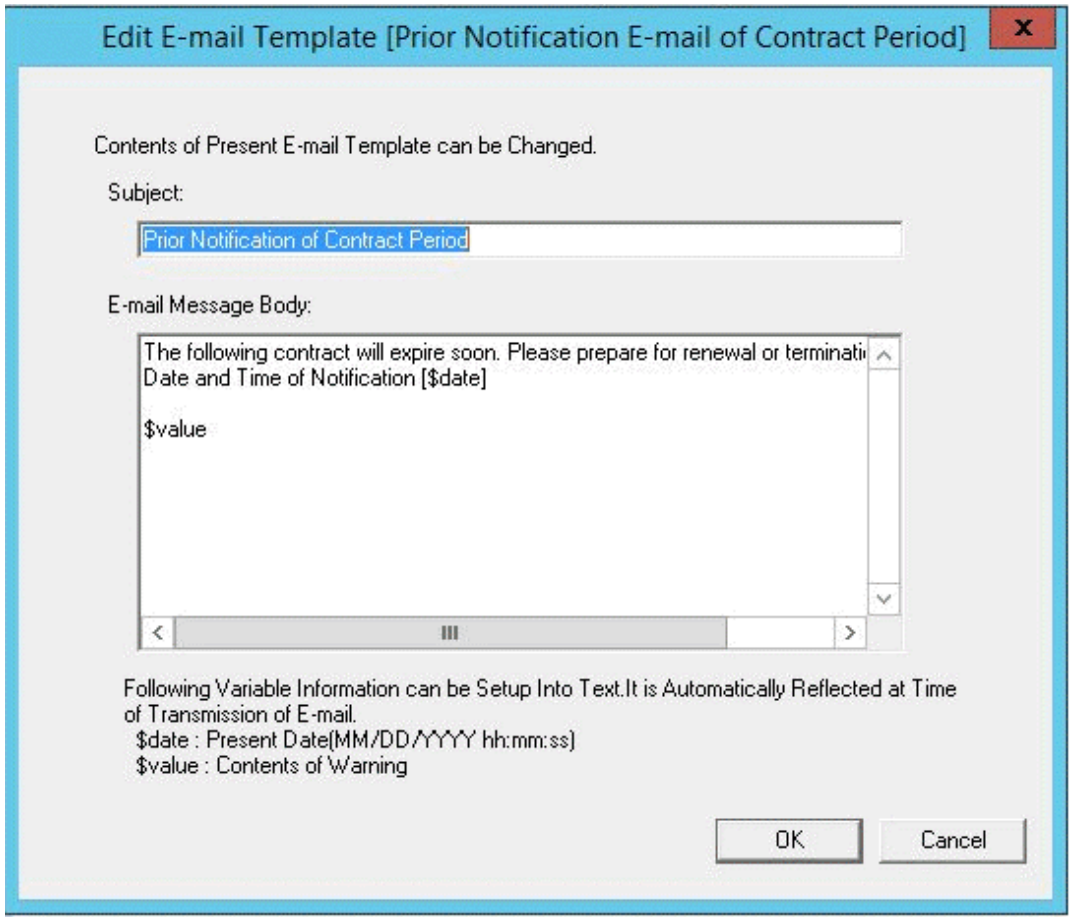
The operation according to the information above is as follows:

Conditions for Operation	Content of Operation
Contract End Date > **Startup Date** + **Prior Notice Date**	Contract expiration notification is not performed.
Contract End Date = **Startup Date** + **Prior Notice Date**	Notify **Prior Notice E-mail of Contract Period**.
Startup Date < **Contract End Date** < **Startup Date** + **Prior Notice Date**	Different due to the notification status of **Prior Notice E-mail of Contract Period**. - If not notified Notify **Prior Notice E-mail of Contract Period**. - If notified Contract expiration notification is not performed.

Conditions for Operation	Content of Operation
Contract End Date = **Startup Date**	Notify **Contract Expiration Warning E-mail**. Not notify **Prior Notice E-mail of Contract Period**.
Contract End Date > **Startup Date**	Different due to the notification status of **Notification E-mail of Contract Expiration Warning**. - If not notified Notify **Contract Expiration Warning E-mail**. - If notified Contract expiration notification is not performed.

Edit e-mail template

By selecting E-mail template in the window where the **Set Contract Expiration Notification** tab of the **Environment Setup** window has been selected and clicking the **Edit** button, the following window can be displayed and E-mail template can be edited.



Item	Descriptions
Subject	Set E-mail subject of contract expiration notification. Specify up to 128 fullwidth or 256 halfwidth alphanumeric characters and symbols. If more than 128 fullwidth or 256 halfwidth characters are specified, errors will occur when sending.
E-mail Message Body	Set E-mail message body of contract expiration notification. Specify up to 1024 fullwidth or 2048 halfwidth alphanumeric characters and symbols.

Item	Descriptions
	The part exceeding 1024 fullwidth or 2048 halfwidth characters will be deleted.

When editing E-mail template, set the information above and click the **OK** button.

Besides, the initial value will be set as the following information.

- Prior notice E-mail of contract period

  [Subject]
  Prior Notice of Contract Period

  [E-mail Message Body]
  The following contract has approached contract expiration date. Please prepare the formality for continuing or terminating the contract.
  Date and time for notification: [$date]

  $value

- Contract expiration warning E-mail

  [Subject]
  Contract Expiration Warning

  [E-mail Message Body]
  The following contract has expired. Please prepare the formality for continuing or terminating the contract.
  Date and time for warning: [$date]

  $value

Set variable information in "$date" and "$value" above.

Set the date and time for notification or warning in "$date".

As contract information, set **Contract Class**, **Contract No.**, **Contract End Date** and **Number of Contract Device** in "$value".

11.1.2 Set Registration for Device Information

In Systemwalker Desktop Patrol, set the device (PC and device) and manage asset number.

When registering the device information, asset number must be entered, but it can be omitted and set automatically through the later procedure.

The procedure for setting the method for registering asset number is as follows.

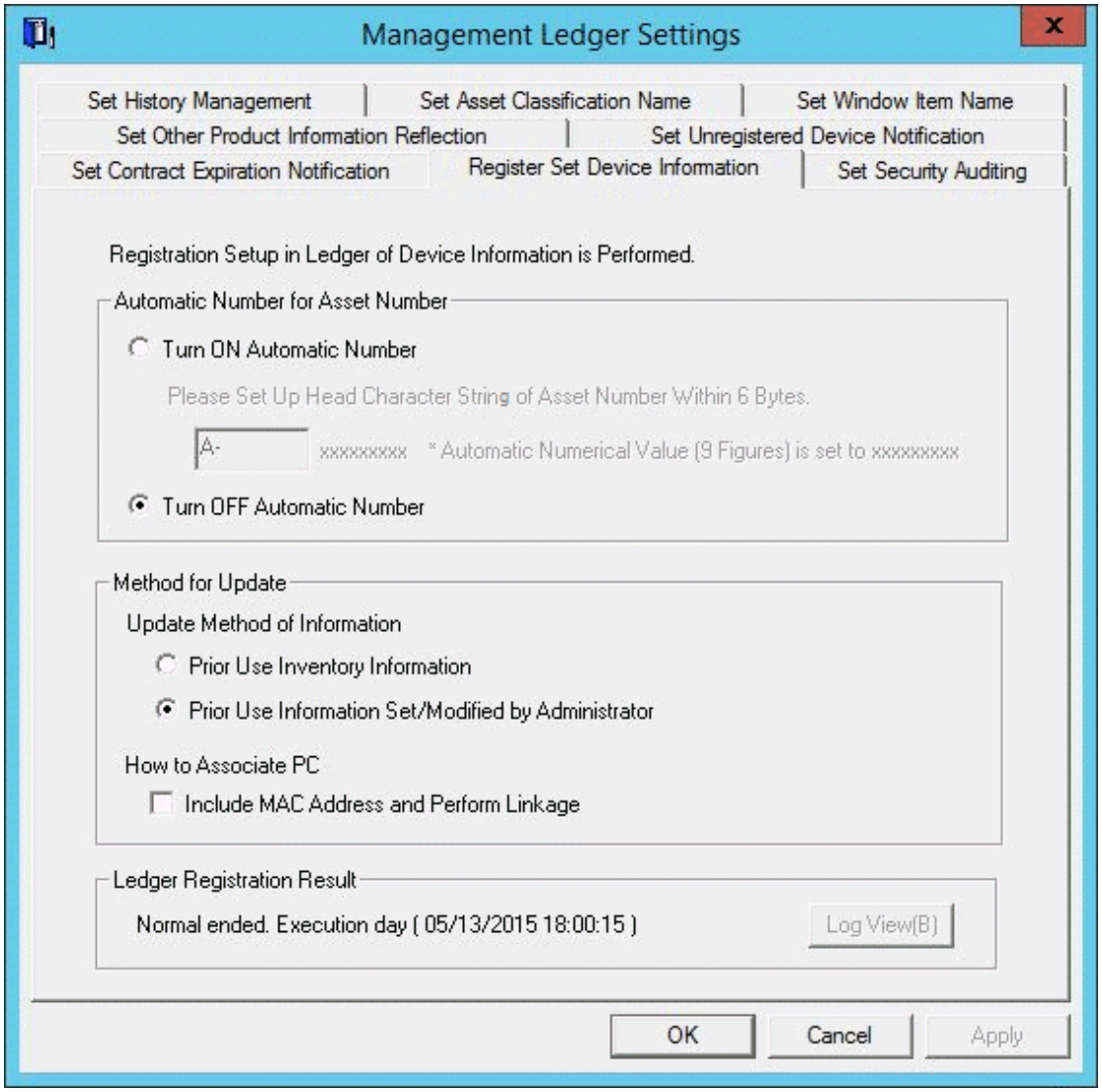
Perform the setting by the system administrator. The section administrator need not set.

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed

2. Select the **Register Set Device Information** tab.

   The following window will be displayed



3. Set the method for registering asset ledger oriented to device information.

   Set the following information and click the **OK** button.

Item		Descriptions
Automatic Number for Asset Number	**Turn ON Automatic Number**	Selected when automatically setting asset number in case the device information has been registered. Set the beginning characters of automatically collected asset number. The following characters within 6 characters can be set as the beginning characters. Single-byte letters: "A"~"Z" (capitals only) Single-byte numbers: "0"~"9" Single-byte symbols: "-", ".", "" (space), "$", "/", "+", "%"
	Turn OFF Automatic Number (Initial Value)	Selected when not automatically setting asset number in case the device information has been registered.

Item		Descriptions
Method for Update	**Prior Use Inventory Information**	Selected when prior using Inventory information collected in Systemwalker Desktop Patrol and all is reflected.
	Prior Use Information Set/ Modified by Administrator (Initial Value)	Selected when prior using the administrator setting or modified information. The following information set or modified by the administrator cannot be overwritten by using Inventory information collected in Systemwalker Desktop Patrol. - **User ID** - **Class** - **Type** - **Manufacturer Name** - **Model Name** - **Serial Number** - **IP Address 1** - **MAC Address 1** - **IP Address 2** - **MAC Address 2** - **Setup Place**
	Include MAC Address and Perform Linkage	When linking Inventory information with asset ledger, it will be linked as the same device in case MAC address matches. This applies only to devices that have not yet been linked to inventory information. Linking is not performed for devices that have been registered automatically based on inventory information or have already been linked to inventory information.

The information is set.

11.1.3 Set Security Auditing

This section describes how to set security auditing.

The procedure for setting security auditing is as follows:

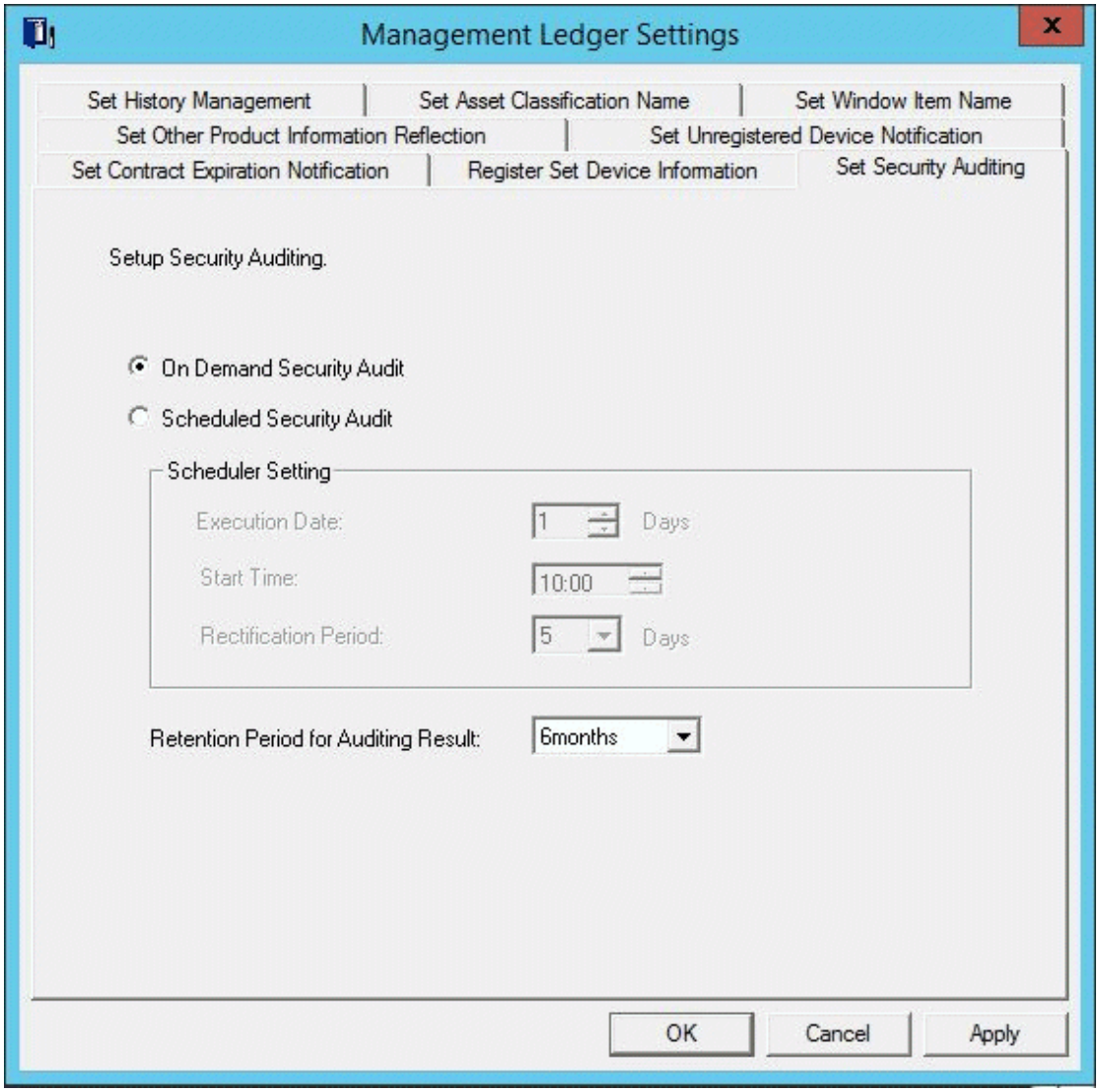
Perform this setting by the system administrator. The section administrator need not set.

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**..

   The **Management Ledger Settings** window will be displayed

2. Select the **Set Security Auditing** tab.

   The following window will be displayed



3. Set security auditing schedule and auditing result saving period.

   Set the following information and click the **OK** button.

   The information is set.

Item		Descriptions
On Demand Security Audit		Selected when not starting security auditing by schedule.
Scheduled Security Audit (Initial Value)		Selected when starting security auditing by schedule.
Scheduler Setting	**Execution Date**	Set the date for performing security auditing. Single-byte numbers only can be set.
	Start Time	Set time for performing security auditing.
	Rectification Period	Set number of days of rectification period. Single-byte numbers from 0 to 6 can be set. When 0 is specified, the rectification period does not exist, and the security auditing is performed only on the date set by schedule.

Item		Descriptions
		Set rectification period as one excluding the startup date (number of days). For example, when specifying as starting on the first day of each month and setting rectification period as 5 days, it will be started during the first day to the sixth day of each month. Besides, the execution date and rectification period should be specified in the same month.
Retention Period for Auditing Result		Select the auditing result saving period from the following options. - **3 months** - **6 months** - **1 year** The initial value is 6 months. Set the auditing result saving period as one excluding this month. For example, if the retention period is set as 3 months, and it is July 15th currently, the auditing result of April, May and June will be reserved. The auditing result exceeding the retention period will be deleted automatically.

11.1.4 Set History Management

This section describes how to set history management.

The procedure for setting security auditing is as follows:

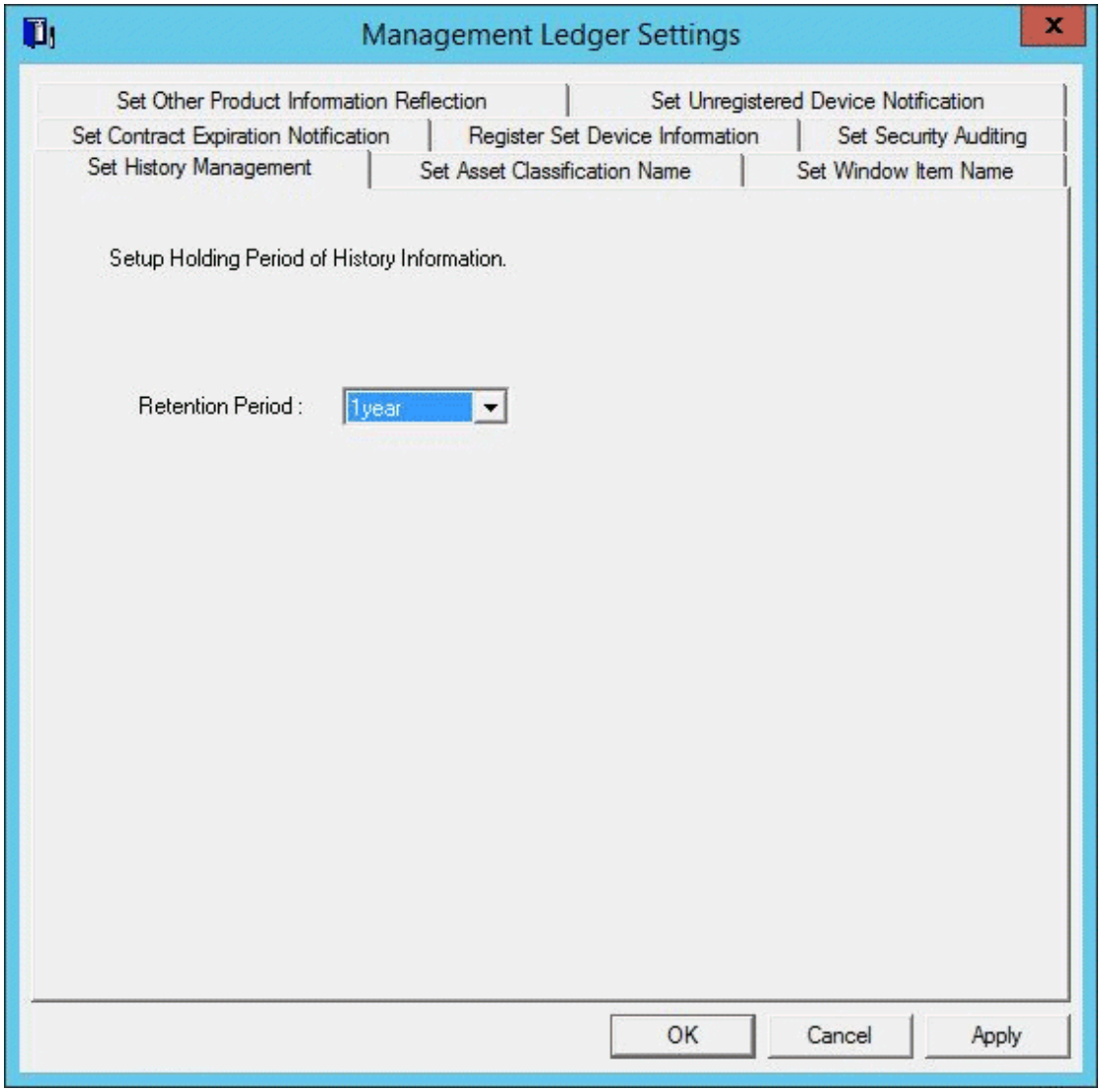
Perform this setting by the system administrator. The section department need not set.

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed

2. Select the **Set History Management** tab.

   The following window will be displayed



3. Set the retention period for history.

   Set the following information and click the **OK** or **Apply** button.

   The information is set.

Item	Descriptions
Retention Period	Select the retention period for history management information from the following options. - **6 months** - **1 year** - **2 years** - **3 years** - **4 years** - **5 years** The initial value is 1 year.

11.1.5 Set Asset Classification Name

This section describes how to set **Asset Classification Name** displayed in the window in use.

The set **Asset Classification Name** will be reflected to all management windows. Besides, as the setting of **Asset Classification Name**, the following operations will be performed.

Setting Operation	Setting Result
Add	As the value of **Asset Classification Name** when registering and modifying the device information, the added value will be selectable.
Update	The value of **Asset Classification Name** set in the registered device will become the revised value.
Delete	The value of **Asset Classification Name** set in the registered device will be blank (not set yet).

Procedures

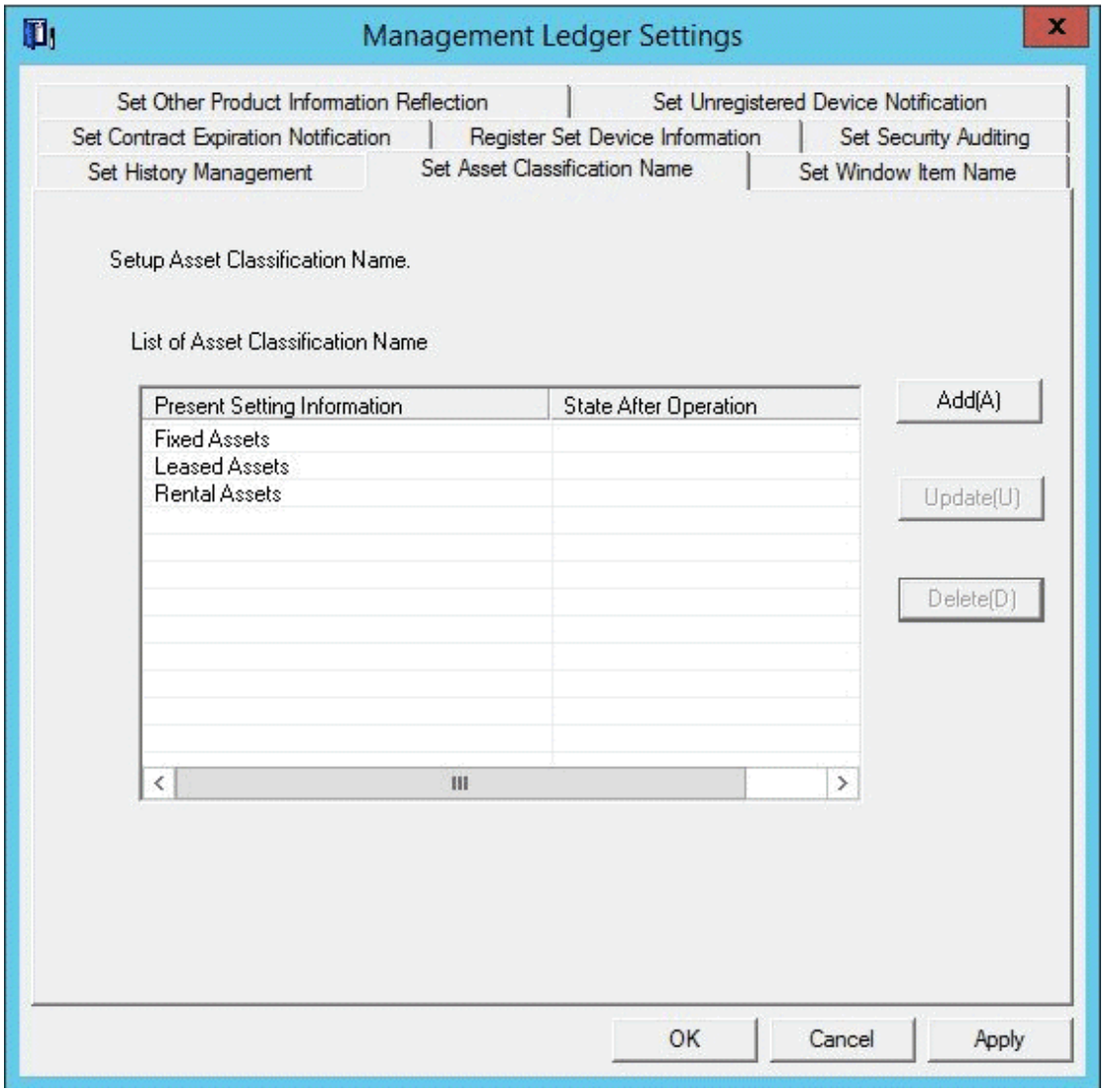
The procedure for setting **Asset Classification Name** is as follows:

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed

2. Select the **Set Asset Classification Name** tab.

   The following window will be displayed



3. Set **Asset Classification Name**.

   Operate according to the following situations.

   - "Add"

     Performed when adding a new **Asset Classification Name**.

   - "Update"

     Performed when revising **Asset Classification Name**.

     But **Fixed Assets**, **Leased Assets** and **Rental Assets** cannot be revised.

   - "Delete"

     Performed when deleting **Asset Classification Name**.

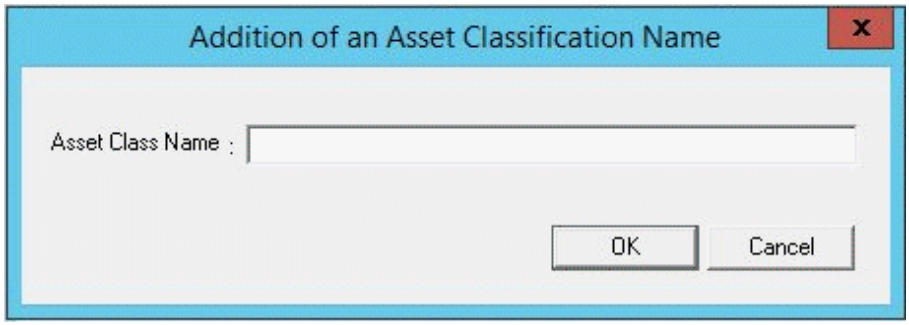
     But **Fixed Assets**, **Leased Assets** and **Rental Assets** cannot be deleted.

Add

1. Add a new **Asset Classification Name**.

   Click the **Add** button.

   The following window will be displayed



2. Set the name of the added **Asset Class Name**.

   Set the following information and click the **OK** button.

   Asset Classification is added.

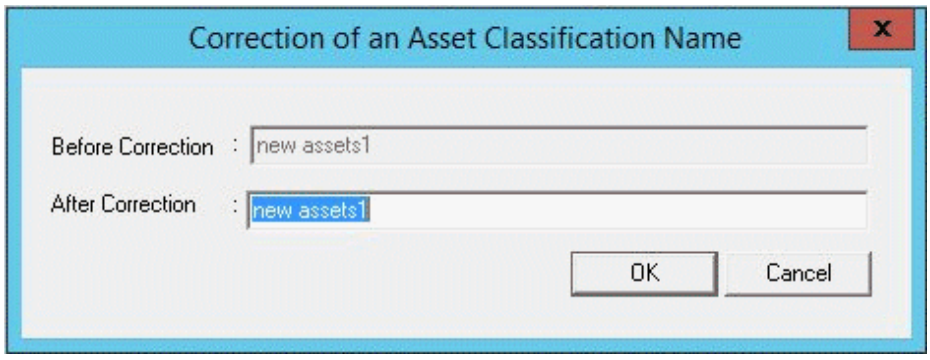
Item	Descriptions
Asset Class Name	Set the new added **Asset Class Name**. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols.

Update

1. Update **Asset Classification Name**.

   Select the **Asset Classification Name** to be revised, and click the **Update** button.

   The following window will be displayed



2. Set the name of the revised **Asset Class Name**.

   Set the following information and click the **OK** button.

   Asset Class Name is updated.

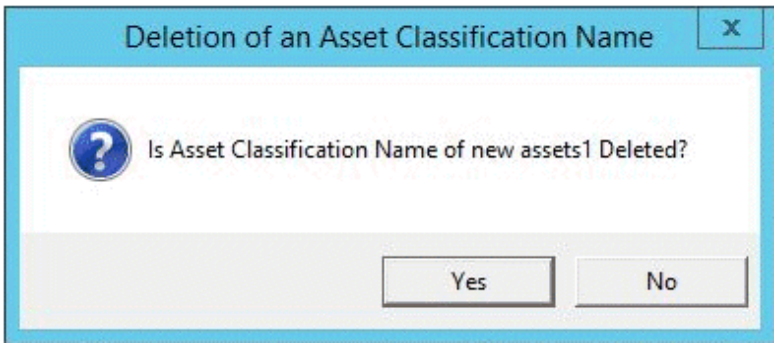
Item	Descriptions
After Correction	Set the revised **Asset Class Name**. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols.

Delete

1. Delete **Asset Class Name**.

   Select **Asset Class Name** to be deleted and click the **Delete** button.

   The following window will be displayed



2. Delete **Asset Class Name**.

   Click the **OK** button.

   Asset Class Name is deleted.

11.1.6 Set Window Item Name

This section describes how to set the name of items displayed in the window in use.

The set item name will be reflected to all management windows.

The "System Account" authority is required for using this function.

Procedures

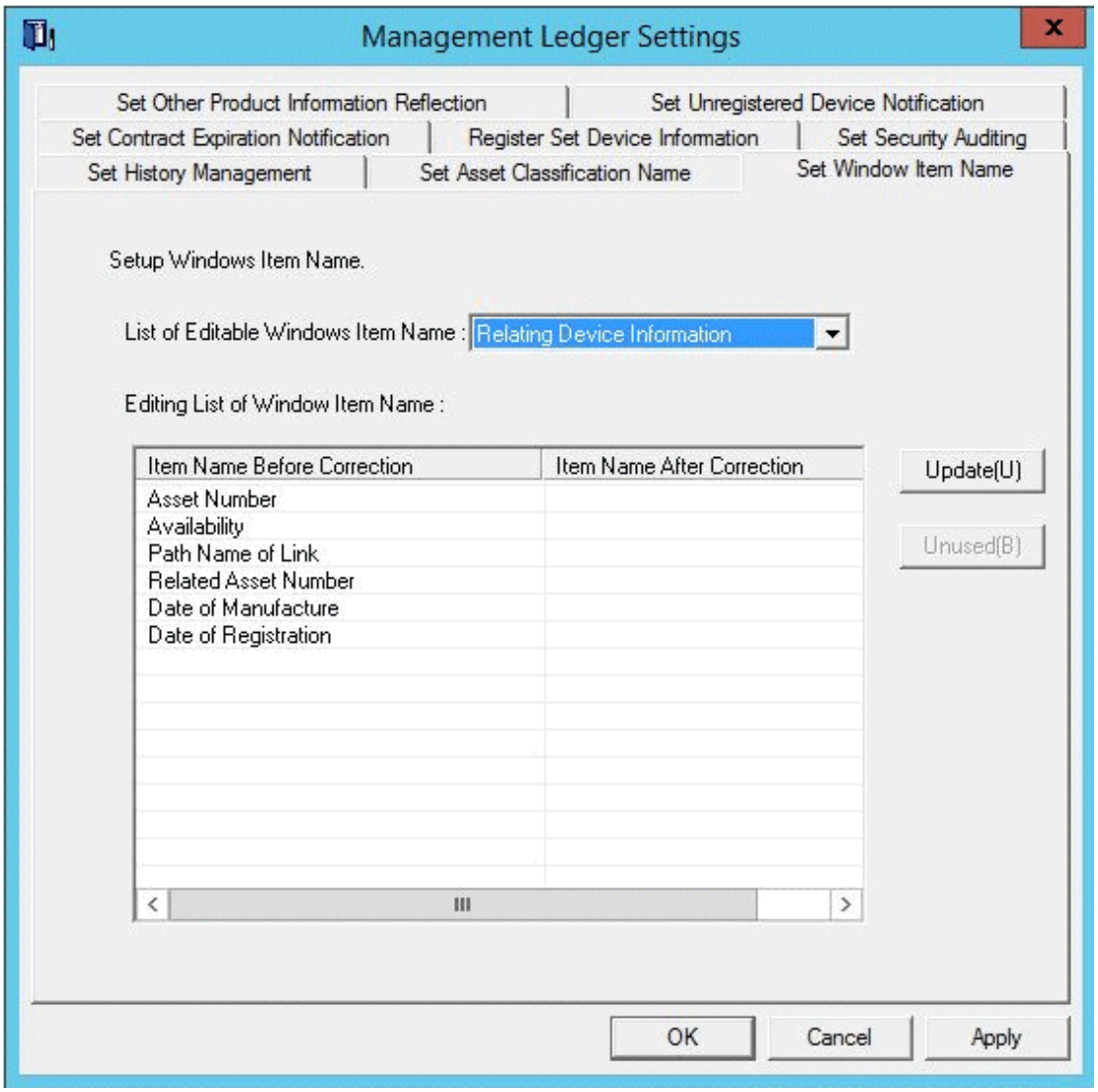
The procedure for setting window item name is as follows:

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed

2. Select the **Set Window Item Name** tab.

   The following window will be displayed



3. Set window item name.

Item	Descriptions
List of Editable Windows Item Name	Select the classification of the set window item name from the following options. - **Relating Device Information** Display the item name related to device information. - **Relating Inherent Information** Display the item name of **Relating Inherent Information** of device information. - **Relating Contract Information** Display the item name related to contract information.
Editing List of Window Item Name	Revise after selecting the set item name. Specify up to 20 fullwidth or 40 halfwidth alphanumeric characters and symbols.

After clicking the **OK** button, the set information will be reflected.

11.1.7 Set Other Product Information Reflection

When importing the CSV file of Inventory information output through other products to asset ledger, it should be set.

For setting procedure, refer to "14.3 Import to Asset Ledger".

11.1.8 Set Unregistered Device Notification

This section explains how to set notification of unregistered devices.

A notification will be emailed to the address specified in the **Event Settings** window when a device not registered in the ledger or connected to without permission is detected. Refer to "2.5 Set Alarm Notification" for details on the **Event Settings** window.

Refer to "Install ADT" in the *Systemwalker Desktop Patrol Installation Guide* for details on the settings for detecting devices not registered in the ledger and devices connected to without permission.

Procedure

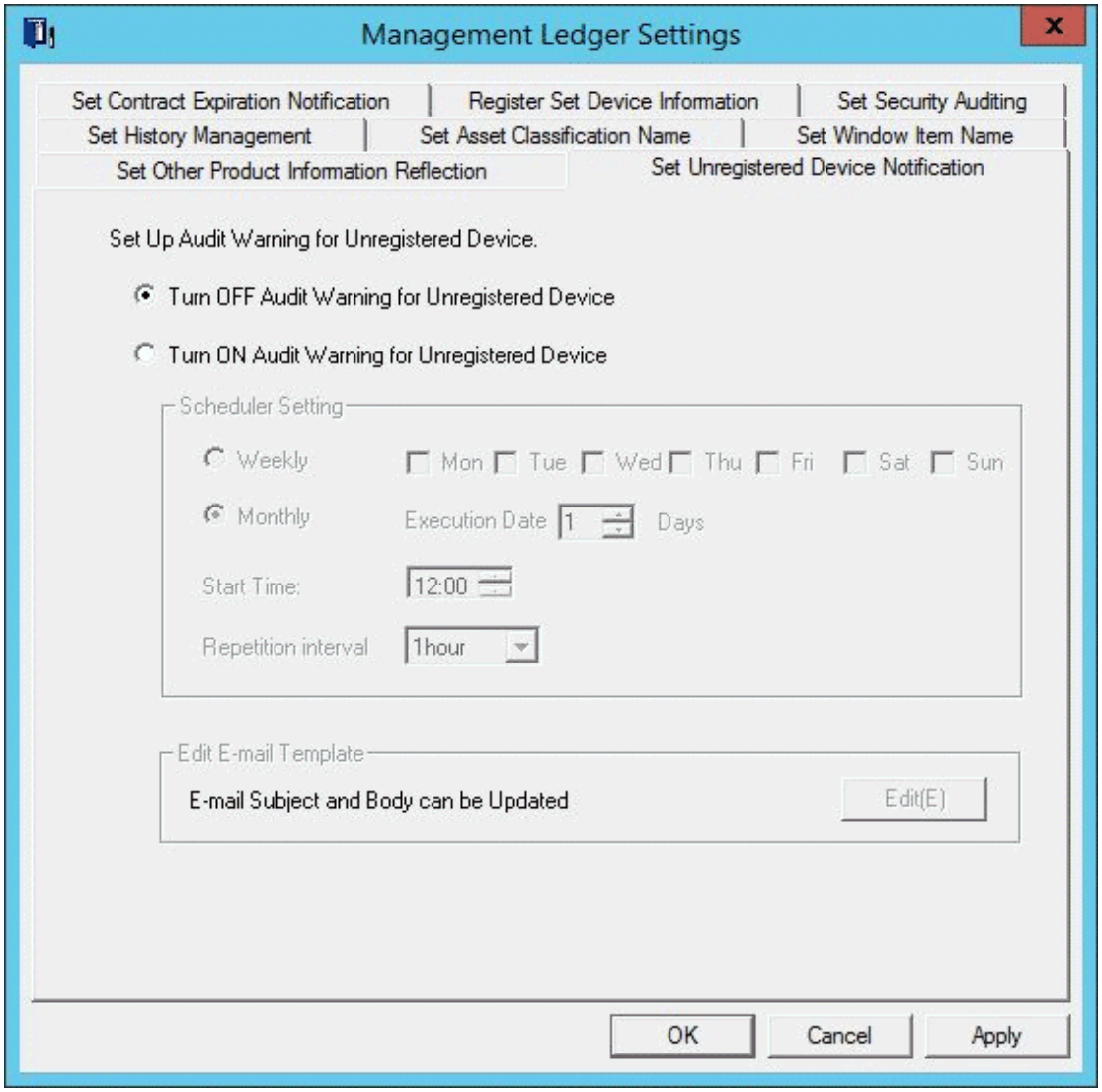
Follow the steps below to configure unregistered device notification:

1. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Management Ledger Settings** window will be displayed.

2. Click the **Set Unregistered Device Notification** tab.

   The following window will be displayed:



3. Specify how to send unregistered device notifications.

   Set the following information and click **OK**.

Item	Description
Turn OFF Audit Warning for Unregistered Device	Select this option to disable audit warning of unregistered devices.
Turn ON Audit Warning for Unregistered Device	Select this option to enable audit warning of unregistered devices. If this option is selected, when **OK** is clicked, the following Windows task for audit warning of unregistered devices will be registered: - Name: SWDTPAS_Unreg.job - Operating authority: System account
Scheduler Setting	These items must be specified if **Turn ON Audit Warning for Unregistered Device** is selected. Select **Weekly** or **Monthly** as the period for performing audit warning. The initial value is **Monthly**.

Item	Description
	Selecting **Weekly** enables the check boxes for the days of the week. Selecting **Monthly** enables **Execution Date**. Note that if the day specified in **Execution Date** does not exist for a certain month, audit warning will not be performed for that month. For this reason, to enable audit warning at the end of the month, consider setting the execution operation at 00:00 on the first day of each month instead. If **Monthly** is selected, the initial value is 1, and the start time will be the current time. Specify the **Start Time** at which audit warning is to start. If **Repeat Interval** is selected, specify the time interval at which audit warning is to be performed. The following values can be specified (if **None** is specified, audit warning will be performed only once): **None**, 30 Minutes, One Hour, 2 Hours, and 6 Hours.
Edit E-mail Template	Clicking **Edit** allows the user to change the email subject and body. Refer to "Edit e-mail template" for details.

11.2 Register Asset Information to Ledger

This section describes how to register or modify the asset information (device information and contract information) managed in the management ledger.

11.2.1 Procedures for Registering/Modifying Asset Information

This section describes the method and procedure for registering or modifying the asset information (device information and contract information) managed in the management ledger.

Method for registration/modification

When registering or modifying the asset information (device information and contract information managed in the management ledger, the methods are as follows.

Point

IPv6 address information

PC information that contains IPv6 address information can also be registered in the management ledger and changed.

- Register/Modify Inventory Information

  It is the method for registering or modifying collectively Inventory information collected in Systemwalker Desktop Patrol as the asset information (device information and contract information).

  This is called "automatic synchronization" and is registered as the following Windows task, configured to run daily every three hours, starting at 00:00:

  - Name: SWDTPAS_AutoS.job
  - Operating authority: System account

  Besides, "User Management Information", "Section Management Information" and "Building Management Information" of Systemwalker Desktop Patrol will be registered/modified along with Inventory information.

  This method also targets smart devices whose inventory information was collected on the Smart Device Relay Server.

- The smart devices targeted for registration and modification of inventory information are those running Android or iOS. The management items in the management ledger are different from those for Windows PCs, as follows:

  - **Class**: Smart device (fixed)
  - **Type**: Client (fixed)
  - **User ID**: User ID set using smart device CT (Android only), or user ID linked with the smart device by the administrator. If the user ID is omitted and no link has been established, MobileUser will be used.
  - **Device Name (PC Name)**: Smart device (fixed)
  - **User Name**: User name. If the user ID is omitted and no link has been established, the inventory information account (example: account01@gmail.com) will be used.

  After importing the management items to the management ledger, the device is marked as **Not Configured** in the left pane of the **Ledger** tab. If the system administrator or section administrator changes the user ID of the device via **Device Management** > **Modify**, the device will be treated as a section device.

- Register/Modify Ledger

  It is the method for registering or modifying collectively the information managed as ledger as the asset information (device information and contract information).

  The object devices are device s such as PCs, printers, HUB, desks and chairs which cannot collect Inventory information through Systemwalker Desktop Patrol.

  Besides, Inventory information which can be collected through Systemwalker Desktop Patrol can also be registered. Because it will be used along with the registration method through Inventory information at this time, double registration occurs, pay attention.

- Register/Modify by Automatically Detecting Device Information

  It is the method for notifying the automatically detected device information and registering device which have not been registered to the asset ledger in the notified device information.

  Regular detection can be set by schedule and the unregistered device information can be registered as management target to asset ledger in the **Unregistered Management** window.

  The object device is PCs, UNIX machine, printers, Fax and Router.

  The methods for automatically detecting the unregistered device are as follows.

  - Network Segment-based Check
  - Batch Network Check

  For details, refer to "11.2.3 Registration/Modification by Automatically Detecting Device Information".

- Register/Modify through the Window

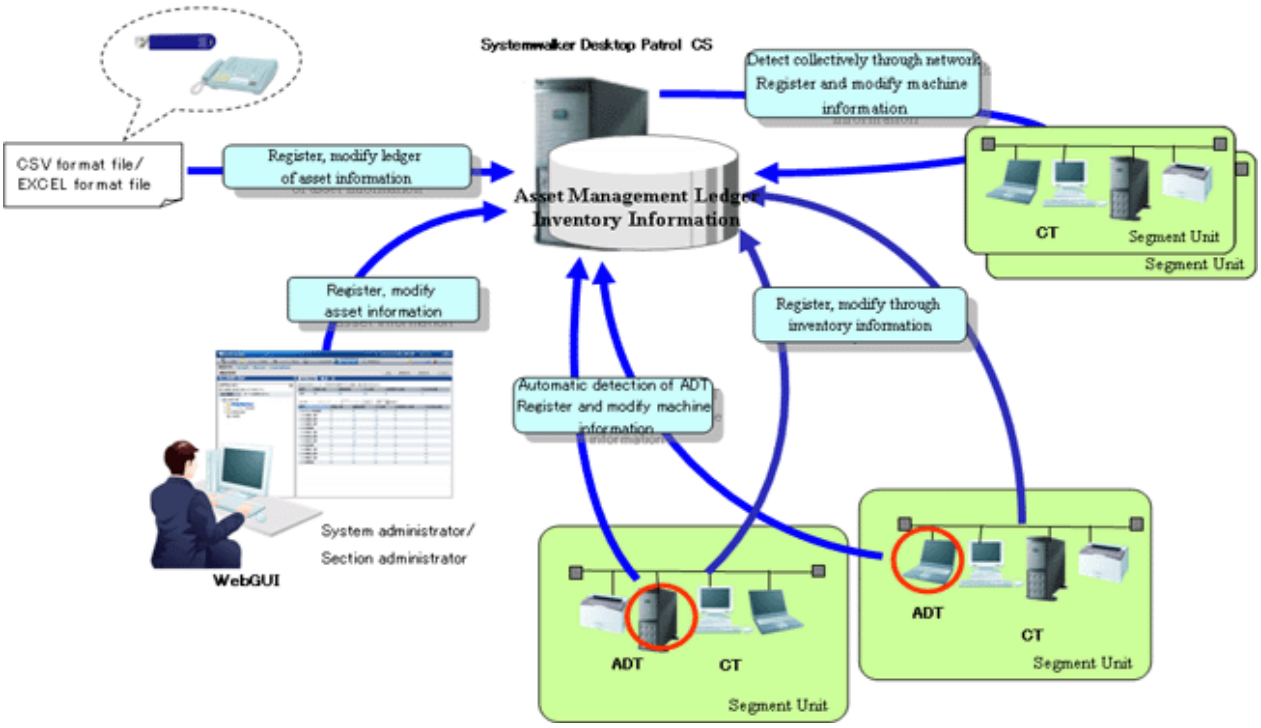
  It is the method for registering or modifying the asset information (device information and contract information) one by one through the window.

  It is mainly the method when collective registration or modification is not needed, for example, when in use.

  Besides, this chapter centers on collective registration or modification, so registration or modification through the window will not be described. For details, refer to "11.3.2 Register/Modify Device Information" or "11.4.2 Register/Modify Contract Information".

Sketch map for device information registration/modification

The following is the sketch map for registering or modifying the asset information (device information and contract information).



As is displayed in the figure above, for PCs which can collect Inventory information through Systemwalker Desktop Patrol, the asset information (device information and contract information) is registered/modified by registering/modifying Inventory information.

Besides, by ADT set in the unit of network segment or batch network check, device connecting network can be detected automatically and the detected information can be registered to the source manually.

For device s (for example, USB memory and telephone, etc.) which cannot be collected through automatic detection according to Inventory information of Systemwalker Desktop Patrol and ADT, create the ledger and register or modify the asset information (device information and contract information).

Procedures for registration/modification

The procedure for registering or modifying the asset information (device information and contract information) is described according to the network connection device and device.

Procedures for registering/modifying asset information of network connection machine

These are the procedure for registering/modifying device other than PC collecting Inventory information through Systemwalker Desktop Patrol and PC connecting network (UNIX machine, printers, Fax and Router).

1. Determine manual setting or automatic setting for the asset number

In management ledger, set the device and manage the asset number. The asset number is the number required when identifying and making an inventory of device information.

The asset number can be set manually or automatically.

Set manually in case of setting the asset number by combining the current management system in the company. For how to set, refer to "11.1.2 Set Registration for Device Information".

2. Register/Modify unregistered machine

Register or modify the unregistered device information collected through device information automatic detection as the asset information (device information) managed in the management ledger.

For how to register/modify, refer to "11.2.3 Registration/Modification by Automatically Detecting Device Information".

3. Create contract information file

Create the contract information file for managing the machine.

When the contract information need not be registered or modified in case the device is fixed asset, access the next procedure.

Create a new contract information file. You can create a completely new file by yourself, or you can use an Excel template for registration during the "11.2.2 Register/Modify Ledger" process.

When the contract information has been in use and registered, the contract file can also be created by outputting the registered information. For how to create, refer to "11.4.4 Save Contract Information as Ledger".

4. Create device information file

Create the device information file for managing the machine.

Set the device information related to PC in the device information file.

Create the device information file through the template in the process of new creating or "11.2.2 Register/Modify Ledger". For the file format when new creating, refer to *Systemwalker Desktop Patrol Reference Manual*.

When the asset number has been set manually in "1. Determine manual setting or automatic setting for the asset number", the asset number will be set.

When linking the contract information and device information set in "3. Create contract information file", set [Contract No.] set in the contract information file as [Contract No.] or [Maintenance Code] of the device information file.

5. Register/Modify the ledger

Register or modify the created contract information file and device information file.

For how to register/modify, refer to "11.2.2 Register/Modify Ledger".

Procedures for registering/modifying asset information of device

These are the procedure for registering/modifying device s such as PCs, printers, HUB, desks and chairs which cannot collect Inventory information through Systemwalker Desktop Patrol.

1. Determine manual setting or automatic setting for the asset number

In management ledger, set the device and manage the asset number. The asset number is the number required when identifying and making an inventory of device information.

The asset number can be set manually or automatically.

Set manually in case of setting the asset number by combining the current management system in the company. For how to set, refer to "11.1.2 Set Registration for Device Information".

2. Create contract information file

Create the contract information file for managing the machine.

When the contract information need not be registered or modified in case the device is fixed asset, access the next procedure.

Set information related to device contract in the contract information file.

Create a new contract information file. You can create a completely new file by yourself, or you can use an Excel template for registration during the "11.2.2 Register/Modify Ledger" process.

When the contract information has been in use and registered, the contract file can also be created by outputting the registered information. For how to create, refer to "11.2.3 Registration/Modification by Automatically Detecting Device Information".

3. Create device information file

Create the device information file for managing the machine.

Set device information related to the device in the device information file.

When the asset number has been set manually in "1. Determine manual setting or automatic setting for the asset number", set the asset number.

When linking the contract information set in "2. Create contract information file" and the registered/modified device information, set [Contract No.] set in the contract information file as [Contract No.] or [Maintenance Code] of the device information file.

Create the device information file through the template in the process of new creating or "11.2.2 Register/Modify Ledger". For the file format when new creating, refer to *Systemwalker Desktop Patrol Reference Manual*.

When the device information has been in use and registered, the device information file can also be created by outputting the registered information. For how to create, refer to "11.4.4 Save Contract Information as Ledger".

4. Register/Modify the ledger

Register or modify the created contract information file and device information file.

When the asset number has been set automatically in "1. Determine manual setting or automatic setting for the asset number", the asset number will be set automatically.

For how to register/modify, refer to "11.2.2 Register/Modify Ledger".

11.2.2 Register/Modify Ledger

This section describes how to register or modify information managed as ledger as the asset information (device information and contract information) managed in the management ledger.

Besides, when the asset information (device information and contract information) has been in use and registered, the file for registration can be created by outputting the registered information. By editing and registering the output file, the information can be updated collectively.

Note

User Memo is not displayed in the initial settings

For **User Memo** that can be registered or modified as the device information according to the following procedure, if **User Memo Related** has not been set in the window item name setting, even if being registered or modified, it will not be displayed in the window.

For window item name setting, refer to "11.1.6 Set Window Item Name".

Notes during modification

When modifying the asset information (device information and contract information), pay attention to the following issues.

Device information

- Modify the device information with **Asset Number** set

  Modify the device information with consistent **Asset Number**.

  When the modified device information exists as PC Inventory information, **Device Name** and **User ID** cannot be modified. Input the same content as the registered information. Items other than **Asset Number**. **User ID** and **Device Name** can be modified.

  If a smart device has inventory information, **Device Name** and **User ID** can be changed.

- Modify the device information with **Asset Number** unset

  Modify the device information with **Device Name** matching **User ID**.

  At this time, **Asset Number** should be set. If it has not been set manually, enable automatic collection setting.

  If **Device Name** and **User ID** do not match for a device for which **Smart device** has been set for **Class**, also change information for the device for which **MAC Address** and **Class** match. If **MAC Address** is duplicated on the same device, the device with the newer registration date time or detection date time will be the target.

- Modify **Class**

  In the device where **Class** has been set as **PC**, it cannot be modified as the classification of non **PC**.

  The same applies to devices for which **Smart device** is set for **Class**.

Contract information

Modify the contract information with **Contract No.** matching **Contract Class**.

But before **Contract No.** is prohibited, **Contract Class** can be modified from **Lease** as **Rent**, or from **Rent** as **Lease**.

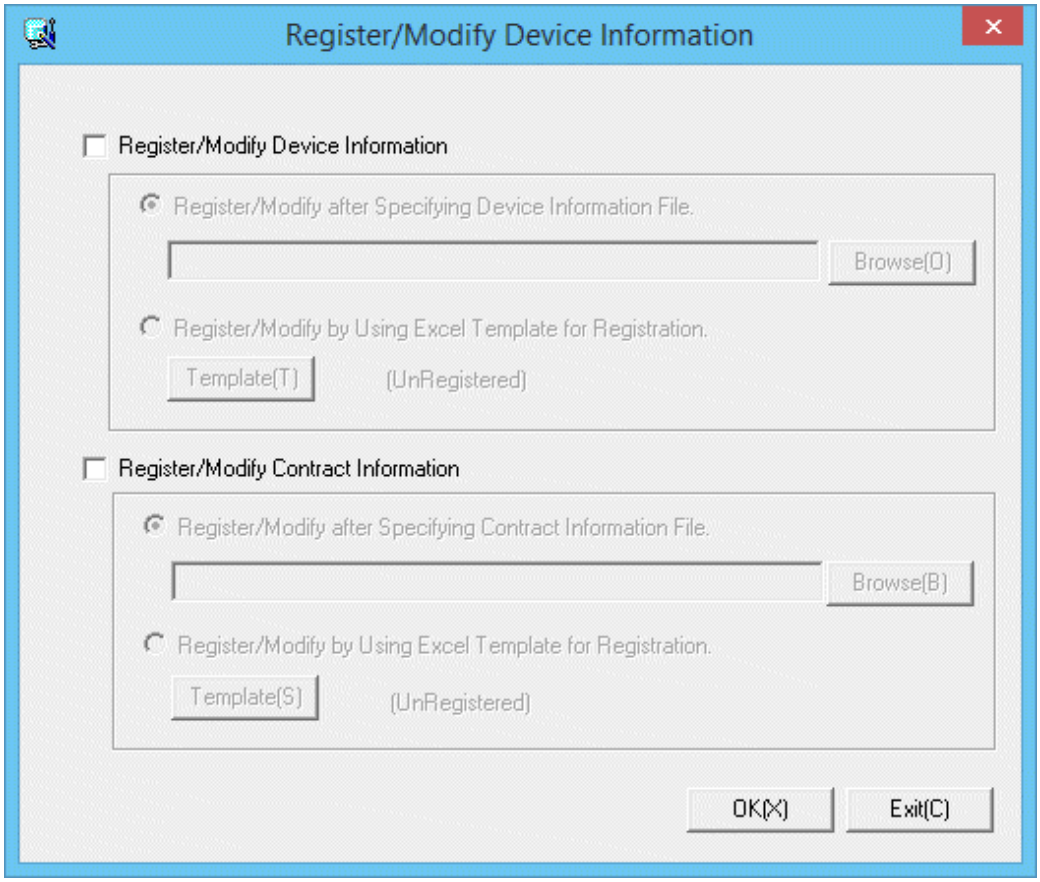
Procedures

The procedure for registering/modifying the ledger is as follows:

1. Logon to AC menu.

2. Select **Register/Modify Device Inf**.

   The following window will be displayed



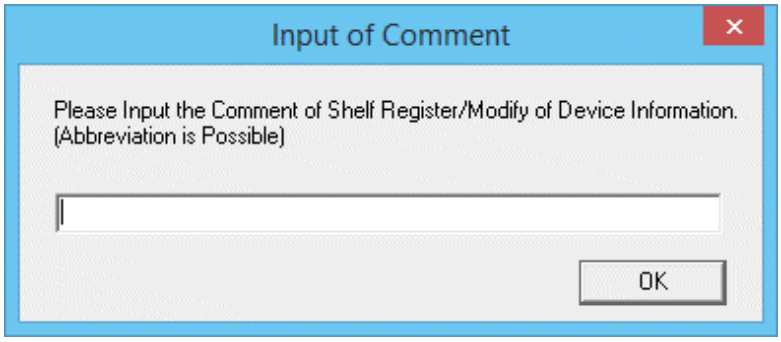
3. Register/Modify the asset information (device information and contract information).

   Set the following information and click the **OK** button.

Item		Descriptions
Register/Modify Device Information		Selected when registering or modifying device information. After being selected, **Register/Modify after Specifying Device Information File** and **Register/Modify by Using Excel Template for Registration** can be selected.
	Register/Modify after Specifying Device Information File	Set the specified device information file through the **Browse** button. Specify a valid Windows file name using up to 128 fullwidth or 256 halfwidth characters. For device information file, refer to *Systemwalker Desktop Patrol Reference Manual*.
	Register/Modify by Using Excel Template for Registration	Click the **Template** button and set device information in Excel. For items set in the device information file, refer to *Systemwalker Desktop Patrol Reference Manual*.
Register/Modify Contract Information		Selected when registering or modifying contract information.

Item		Descriptions
		After being selected, **Register/Modify after Specifying Contract Information File** and **Register/Modify by Using Excel Template for Registration** can be selected.
	Register/Modify after Specifying Contract Information File	Set the specified contract information file through the **Browse** button. Specify a valid Windows file name using up to 128 fullwidth or 256 halfwidth characters. For contract information file, refer to *Systemwalker Desktop Patrol Reference Manual*.
	Register/Modify by Using Excel Template for Registration	Click the **Template** button and set contract information in Excel. For items set in the contract information file, refer to *Systemwalker Desktop Patrol Reference Manual*.

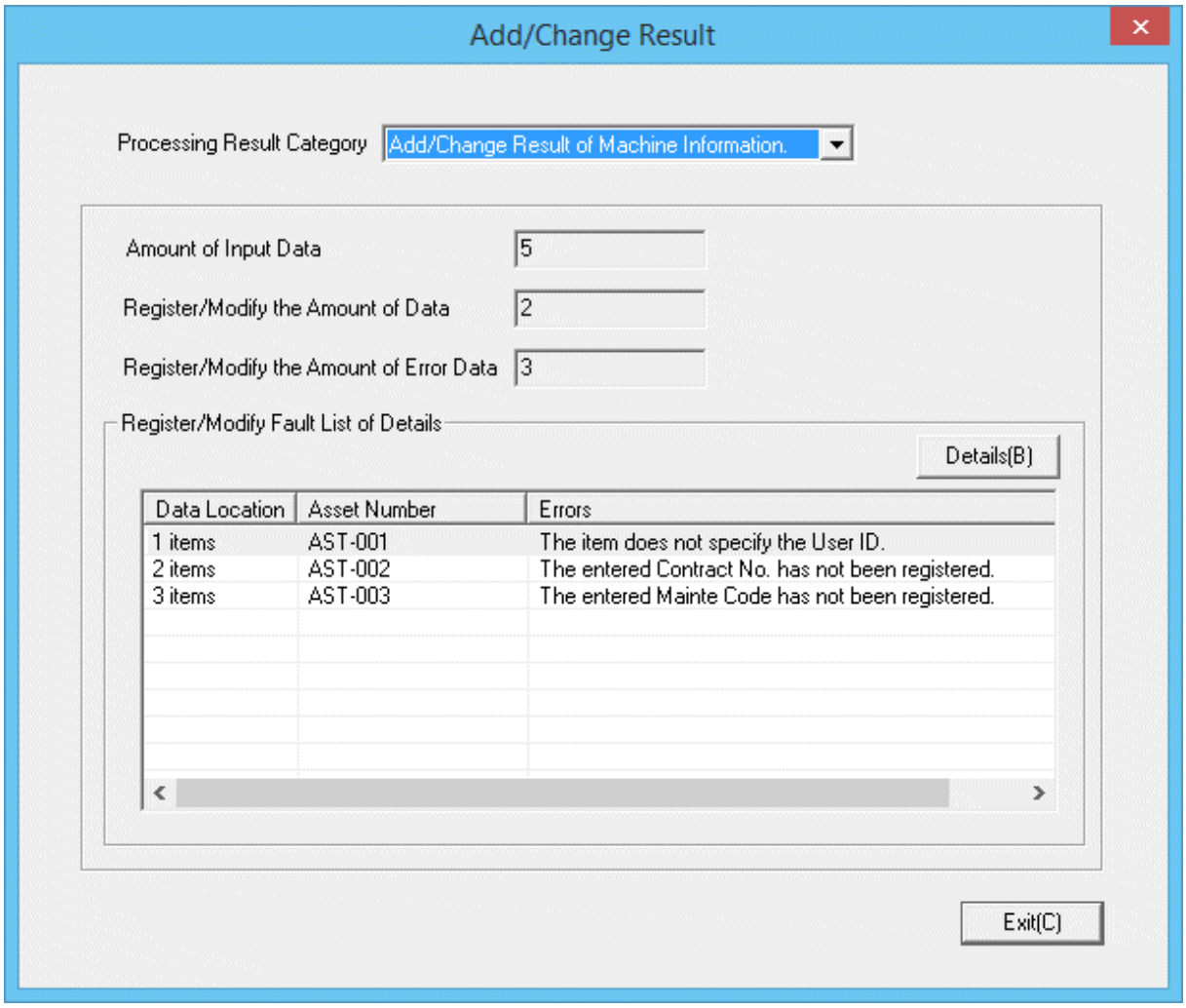
The following window will be displayed
Displayed only when selecting **Register/Modify Device Information**.



4. Input the comment and click the **OK** button.

Item	Descriptions
Input of Comment	Input the comment for the content with device information collectively registered/modified. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. Besides, the annotation input here is valid when updating the new added device or the following device information. - **Asset Number** - **Related Asset Number** - **User ID** - **Setup Place** - **Availability** - **User Memo** - **Contract No.** - **Maintenance Code**

The following window will be displayed



5. Confirm the registration/modification result.

   Confirm the following information.

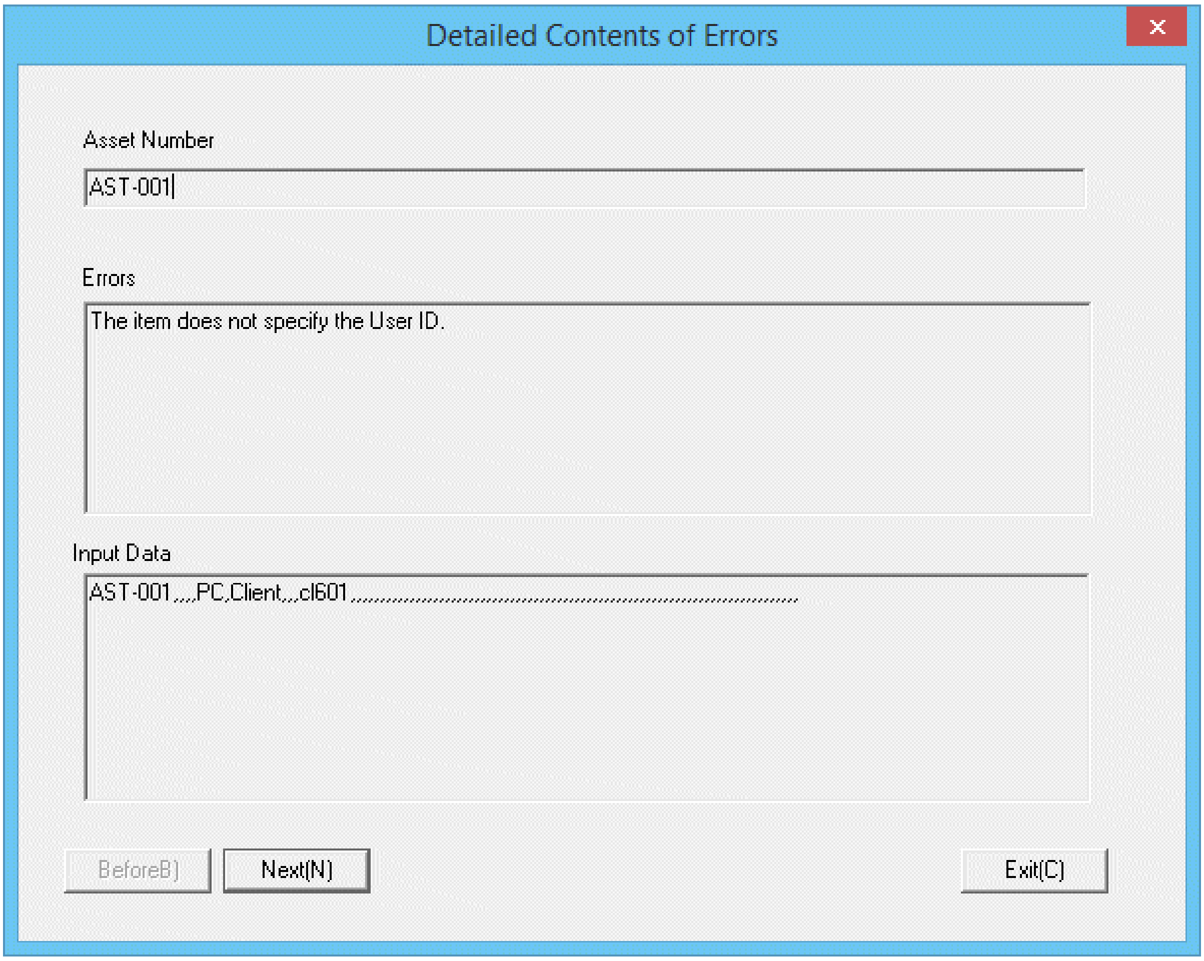
Item	Descriptions
Processing Result Category	Select the category for registration/modification result to be confirmed. - **Add/Change Result of Machine Information** The registration/modification result of device information can be confirmed. - **Add/Change Result of Contract Information** The registration/modification result of contract information can be confirmed.
Amount of Input Data	Amount of the input data can be confirmed.
Register/Modify the Amount of Data	Amount of data to be registered/modified can be confirmed.
Register/Modify the Amount of Error Data	Amount of data which cannot be registered/modified can be confirmed.

Item	Descriptions
Register/Modify Fault List of Details	Information of data which cannot be registered/modified can be confirmed. - **Data Location** Display the number of lines of data which cannot be registered/modified. - **Asset Number** or **Contract No.** **Asset Number** which cannot be registered or modified in case the device information is displayed. **Contract No.** which cannot be registered or modified in case the contract information is displayed. - **Errors** Display the cause that it cannot be registered or modified.

6. When information which cannot be registered/modified, confirm the details.

   Select the information from **Register/Modify Fault List of Details** and click the **Details** button.

   The following window will be displayed



7. Confirm registration/modification result with error.

   The following information is confirmed.

Item	Descriptions
Asset Number or **Contract No.**	**Asset Number** which cannot be registered or modified in case the device information is displayed.

Item	Descriptions
	Contract No. which cannot be registered or modified in case the contract information is displayed.
Errors	Display the cause that it cannot be registered or modified.
Input Data	Display the information of data which cannot be registered/modified.

11.2.3 Registration/Modification by Automatically Detecting Device Information

This section describes how to detect automatically and register the information of device connected the network as the device information managed in the management ledger.

The methods for detecting automatically the unregistered device are as follows.

- Batch Network Check

  It is the method for detecting automatically and collectively the unregistered device out of the network segment through CS Server.

- Network Segment-based Check

  It is the method for detecting the unregistered machined by using ADT after installing ADT in each network segment. This can be done by obtaining detailed device information for checking devices not registered in a ledger, or by obtaining device information (simple and prompt collection) for checking devices connected to without permission.

The function differences between batch network check and network segment-based check are as follows:

Device Information	Batch network check	Network Segment-Based Check
Acquired out of the network segment	Can	Cannot
Device to be detected	Device meeting all the following conditions - Power on - Connected the network - Return ICMP response	Device meeting all the following conditions - Power on - Connected the network
Acquired information	Device category (Note 1) OS category IP address (Note 2) MAC address Host name Manufacturer name Date and time for detection Annotation *For device not supporting SNMP, only IP address, host name and date and time for detection are acquired.	Device category (Note 1) OS category IP address (Note 3) (Note 4) MAC address (Note 4) Computer name/host name Manufacturer name Date and time for detection (Note 4) Annotation *For devices not supporting SNMP, only the IP address, MAC address, host name/ computer name, and detection datetime are obtained.
Install ADT	Not necessary. But compared with network segment-based check, the number of detectable device is less.	ADT should be installed in each network segment. But compared with batch network check, the number of detectable device is more.

Note 1: For device category, "PC" will also be collected as "Other Device". Confirm the actual status of the device through IP address/ host name and register to the ledger according to the category of confirmed device as other device.

Note 2: Only IPv4 information is collected, in IPv4 and IPv4/IPv6 dual stack environments. In dual stack environments, information is collected only from IPv4 segments, and only if CS supports IPv4. IPv6 information is not collected.

Note 3: Only IPv4 information is collected, in IPv4 and IPv4/IPv6 dual stack environments. IPv6 information is not collected.

Note 4: To collect devices connected to without permission, only the IP address, MAC address, and detection datetime are collected.

Use conditions

The selection for either batch network check or network segment-based check is different due to the considerations for use.

Use condition 1

Firstly, it is the method for detecting the unregistered device through batch network check.

When confirming the collected device information matches roughly the detected number of device and category, continue using batch network check.

However, the batch network check might not be able to detect PC with OS of Windows Vista or later strengthening the security. When the detected Number of PC(s) is smaller than the assumed number, PC which cannot be detected through batch network check might exist.

At this time, install ADT in each network segment, switch to network segment-based check and detect the unregistered device.

Use condition 2

It is the method used in "Whether to take PC as detection object" respectively.

Since the OS of Windows Vista or later strengthened the security, responses will not be made to ICMP and SNMP in the initial setting. Thus, batch network check might not be able to detect more PCs, network segment-based check and batch network check should be used respectively through "Whether to take PC as detection object" in automatic detection.

Detection Object	Detection Method
Detect PC only	Network segment-based check
Detect the network device other than PC	Batch Network Check
Detect all network device	Network segment-based check

For example, to investigate whether PC where CT has not been installed exists, because it had better to detect "PC Only", detect through "Network Segment-based Check". Since PC can be collected through CT, if device other than PC are to be detected, take "Network Device Other than PC" as detection object, and detect through "Batch network check".

Use condition 3

This method detects whether a connection device that has been managed in a management ledger is later connected to without permission.

If a device connected to a network could have been connected to without permission after the following types of operation have been run, use the network segment-based check:

- A batch network check is run to detect unregistered devices (use condition 1).
- Usage is determined based on "whether to take PC as detection object" (use condition 2).
- Devices to be managed are registered in the management ledger in advance.

There are two types of network segment-based check, as explained below. Refer to "Install ADT" in the *Systemwalker Desktop Patrol Installation Guide* for details on how to configure detailed settings.

- Collecting devices connected to without permission: Use this method to detect devices connected to without permission within a relatively short period, such as one hour.

- Collecting devices not registered in the ledger: Use this method to detect devices within a relatively long interval, such as one week.

By setting unregistered device notification, notifications can be emailed. Refer to "11.1.8 Set Unregistered Device Notification" for details.

Using stage for automatic detection

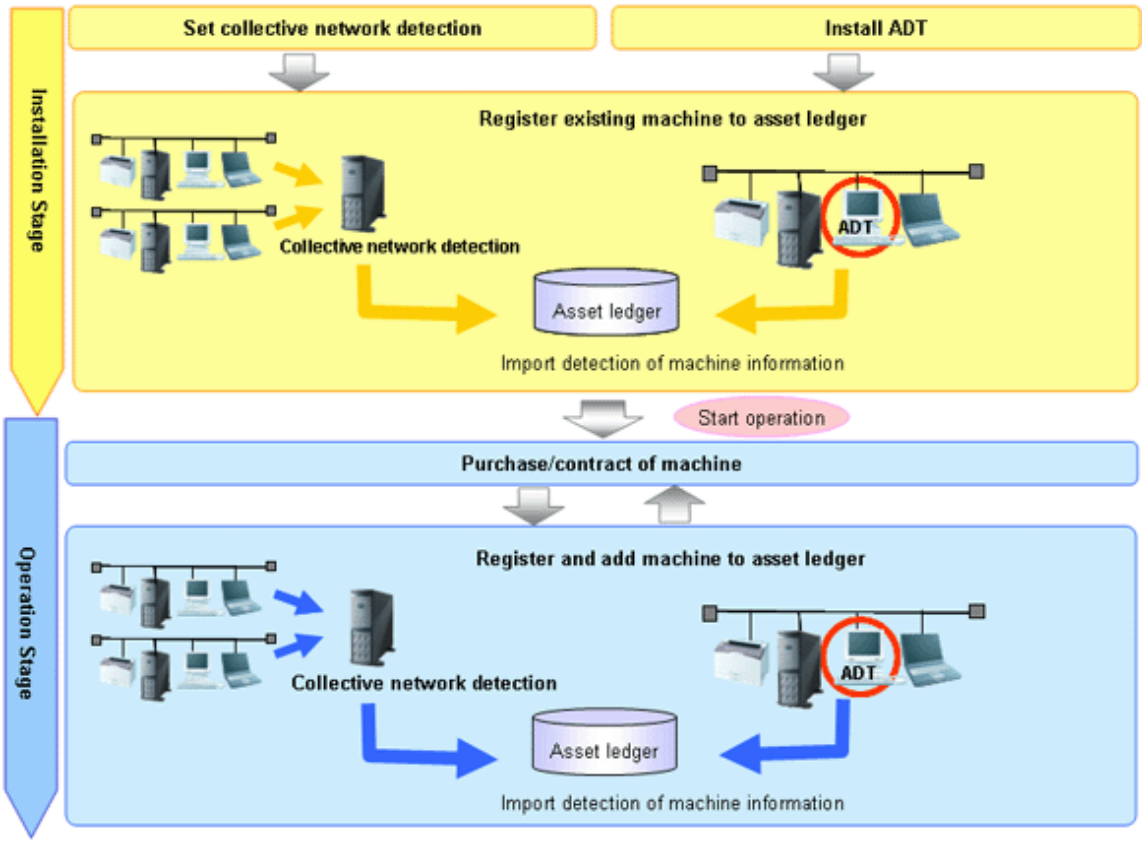
The registration/modification function according to automatic detection can be used in 2 larger stages.

- Installation stage

  The installation stage refers to the stage before using after setting batch network check by schedule or installing ADT and registering the current device information to the asset ledger.

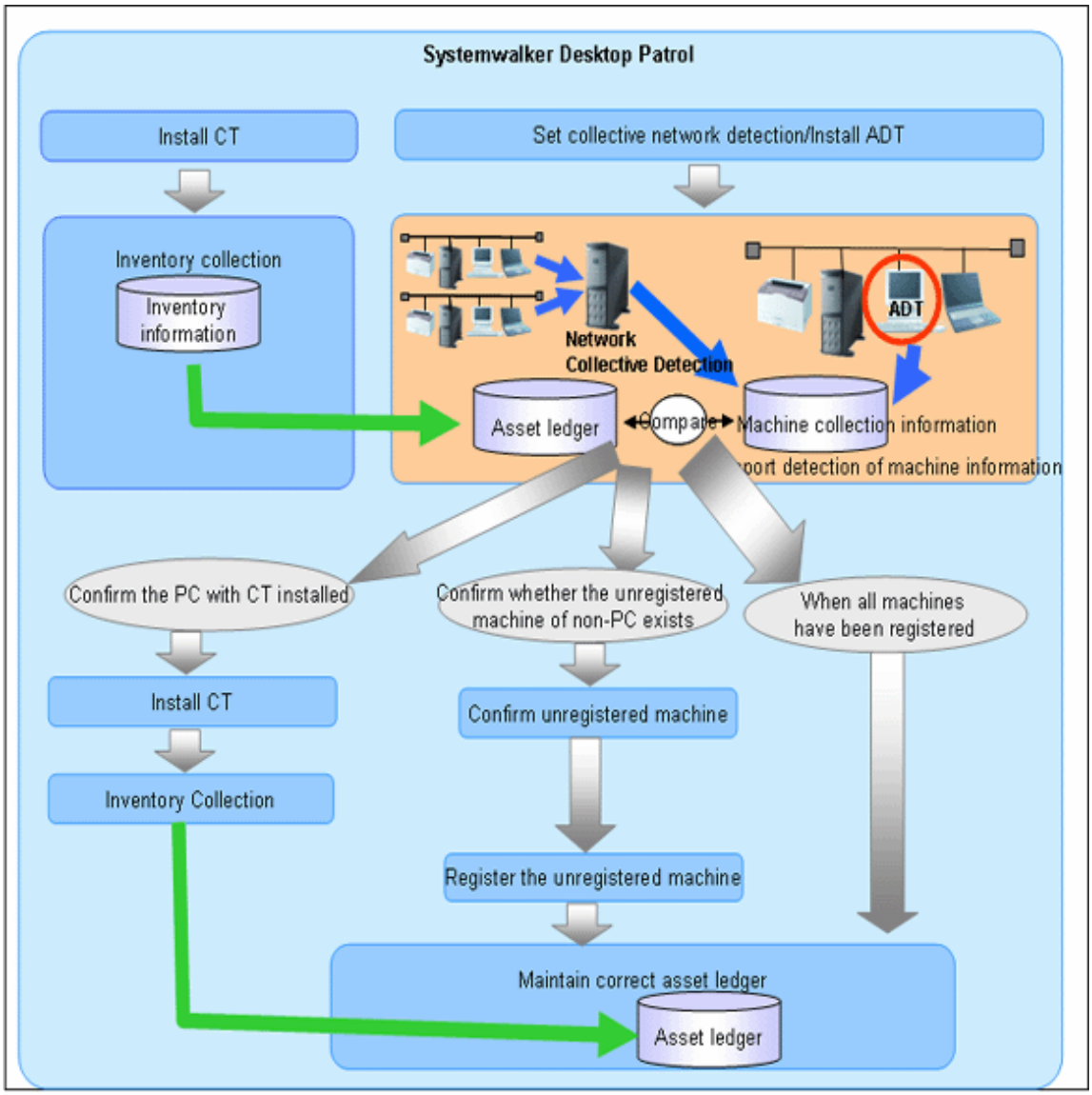
- Using stage

  The using stage refers to the stage of adding device information to the asset ledger, confirming legality maintenance of the asset ledger and making an inventory after adding device through device purchasing and lease contract.



Operation procedure in the installation stage

It describes the procedure for the automatic detection and registration of device information in the installation stage.



It is mainly to create asset ledger by using Inventory information collected through Systemwalker Desktop Patrol for PC. For device which have not been connected the network PC (UNIX device, printers, Fax, Router, etc.), the asset ledger will be created by using the automatic detection function of device information.

Besides, for device which cannot be detected automatically such as USB memory, refer to "11.2.2 Register/Modify Ledger" to register to the asset ledger.

The procedure in the installation stage is as follows:

[Batch network check]

The unregistered device are detected automatically and collectively through CS.

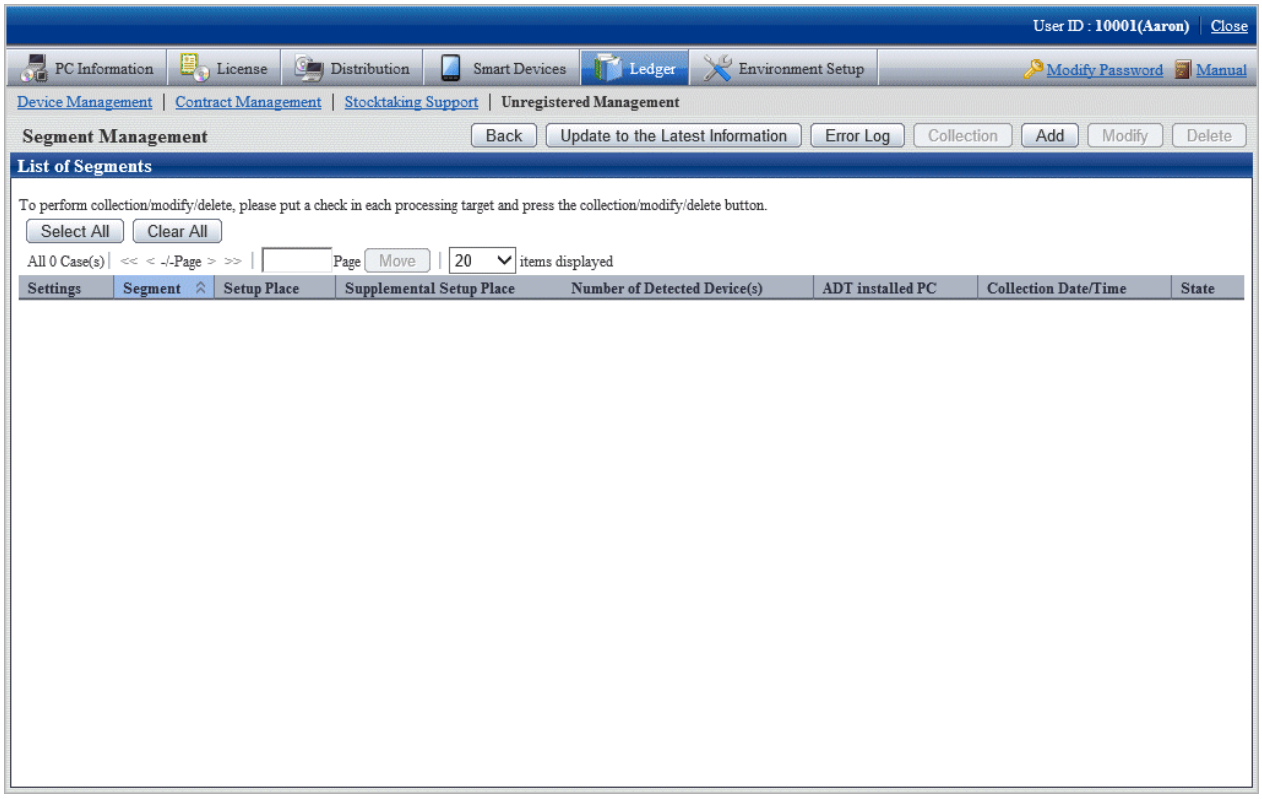
This method takes the network segment registered in **Segment Management** as detection object, and device information out of the network segment can be detected. However, for network segments which have been performed network segment-based check through ADT, they will be excluded from the object.

When errors occurred in the detection, the errors will be output to the **Unregistered Management** > **Collection Status** > **Error Log** window or the event log.

This function is installed when installing CS, so it is unnecessary to install it again, but it should be set as follows after installing CS.

Procedures

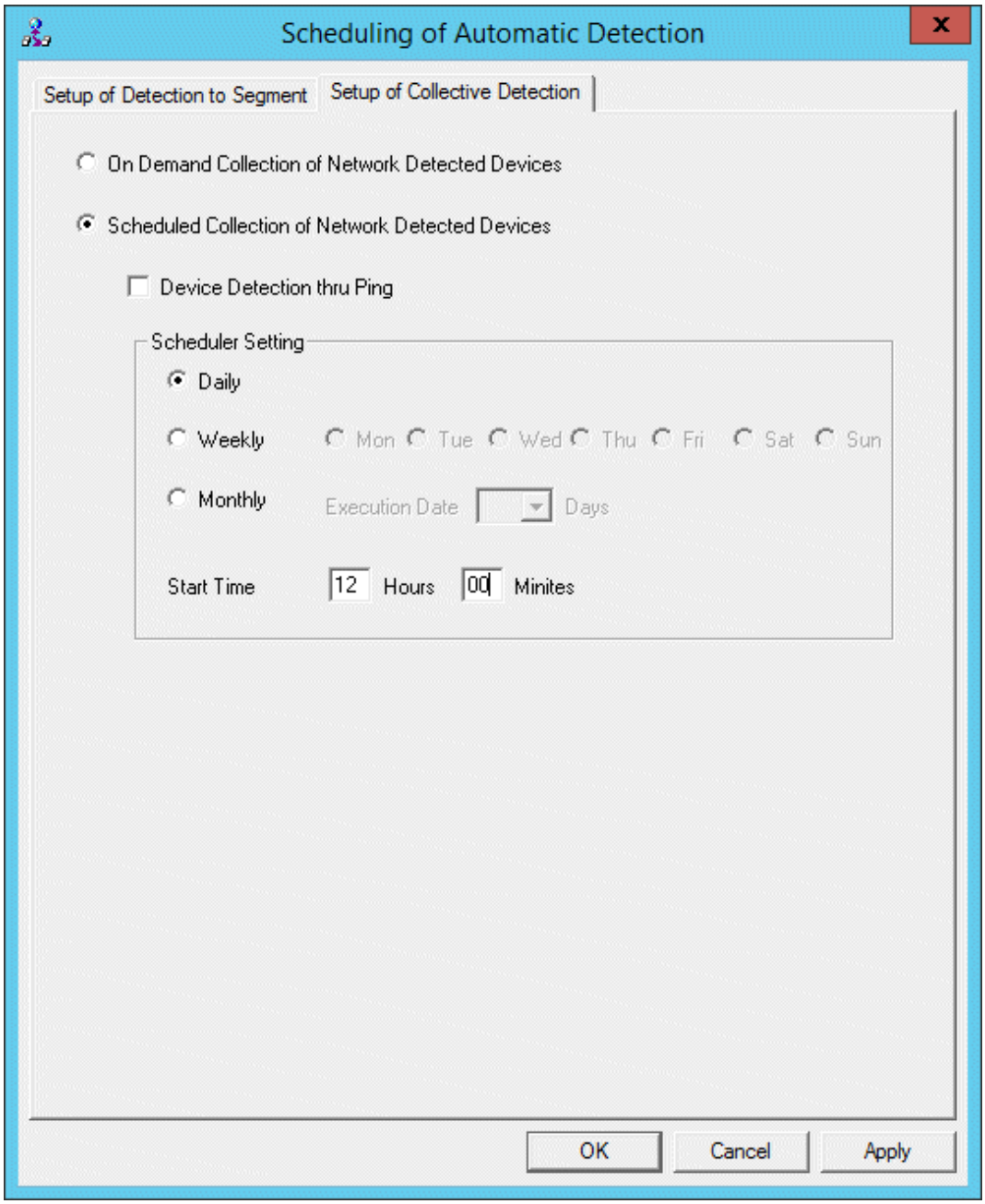
1. Set the range and object of automatic detection.
   Open the **Assets Management** > **Ledger** > **Unregistered Management** > **Segment Management** window in the main menu.



2. Segment information to be detected automatically is defined beforehand by a batch network check. The segments targeted for automatic detection are the ones defined here and the ones for which ADT will not perform a network segment-based check. For details, refer to "Linked network segment and setting location".

3. Set automatic detection schedule.
   On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Scheduling of Automatic Detection**, or **Apps** > **Systemwalker Desktop Patrol** > **Scheduling of Automatic Detection**.

4. Select **Scheduled Collection of Network Detected Devices** in the **Setup of Collective Detection** tab in the **Scheduling of Automatic Detection** window, and set the schedule in each item of **Scheduler Setting**.



Item	Descriptions
On Demand Collection of Network Detected Devices	Selected when not starting batch network check by schedule.
Scheduled Collection of Network Detected Devices	Selected when starting batch network check by schedule.
Device Detection thru Ping	Selected when device responding to Ping only will also be detected as the unregistered device. After being selected, device which cannot get MAC address (*1) will also be output to the **List of Unregistered Device** window.

Item		Descriptions
		*1: Devices that respond to ICMP but not to SNMP (that is, devices that do not support SNMP or with SNMP security protection)
Scheduler Setting	**Daily**	Selected when notifying the device information daily.
	Weekly	Selected when detecting the device information weekly. The values that can be specified (via the option buttons) are: Monday to Sunday.
	Monthly	Selected when detecting the device information monthly. Select the date for execution in **Execution Date**. Besides, as **Execution Date**, when the date not existing in the set month has been specified, automatic detection cannot be performed in this month. Thus, when executing at the end of the month, consider executing at 00:00 on the first day of each month. When selecting **Monthly**, the initial value is **1st Day**, and the start time is the current time.
	Start Time	Set the time for starting collective detection of device information.

5. Click the **Apply** button.

[Network Segment-based Check]

1. Install ADT.

   For how to create "ADT Module", refer to *Systemwalker Desktop Patrol Installation Guide*.

2. Distribute/set ADT to each network segment of the client.

   For how to distribute/set ADT, and select PC for installing ADT, refer to *Systemwalker Desktop Patrol Installation Guide*.

3. Install CS in each PC.

4. Collect Inventory information through CS.

   Thus, PC information is registered to the asset ledger.

5. By using the automatic detection function of the device information, confirm the unregistered device according to information collected by device imported through ADT.

   For how to import the device information, refer to "11.2.3.1 Import Detected Device Information". Besides, for how to confirm the unregistered device, refer to "11.2.3.2 Display/Register Unregistered Device". If a segment for which a detected device exists was not defined in advance, the segment is automatically defined. In this case, set the setting location of the segment. Refer to "Linked network segment and setting location" for details on how to set the setting location of a segment.

6. If the unregistered device exist, confirm whether CT has been installed in the correspondent PC.

   - When CT has been installed:

     Since Inventory collection might fail, confirm the environment setup of CT.

   - When CT has not been installed:

     If CT has not been installed, perform Inventory collection after installing CT.

     Besides, if CT has not been installed, register PC information to the asset information manually according to Procedure 7.

   After the operation above, perform Procedure 4. and Procedure 5. again.

7. By using the automatic detection function of the device information, register the unregistered device other than PC (UNIX device, printers, Fax, Router, etc.) and device where CT has not been installed to the asset ledger collectively. Besides, after

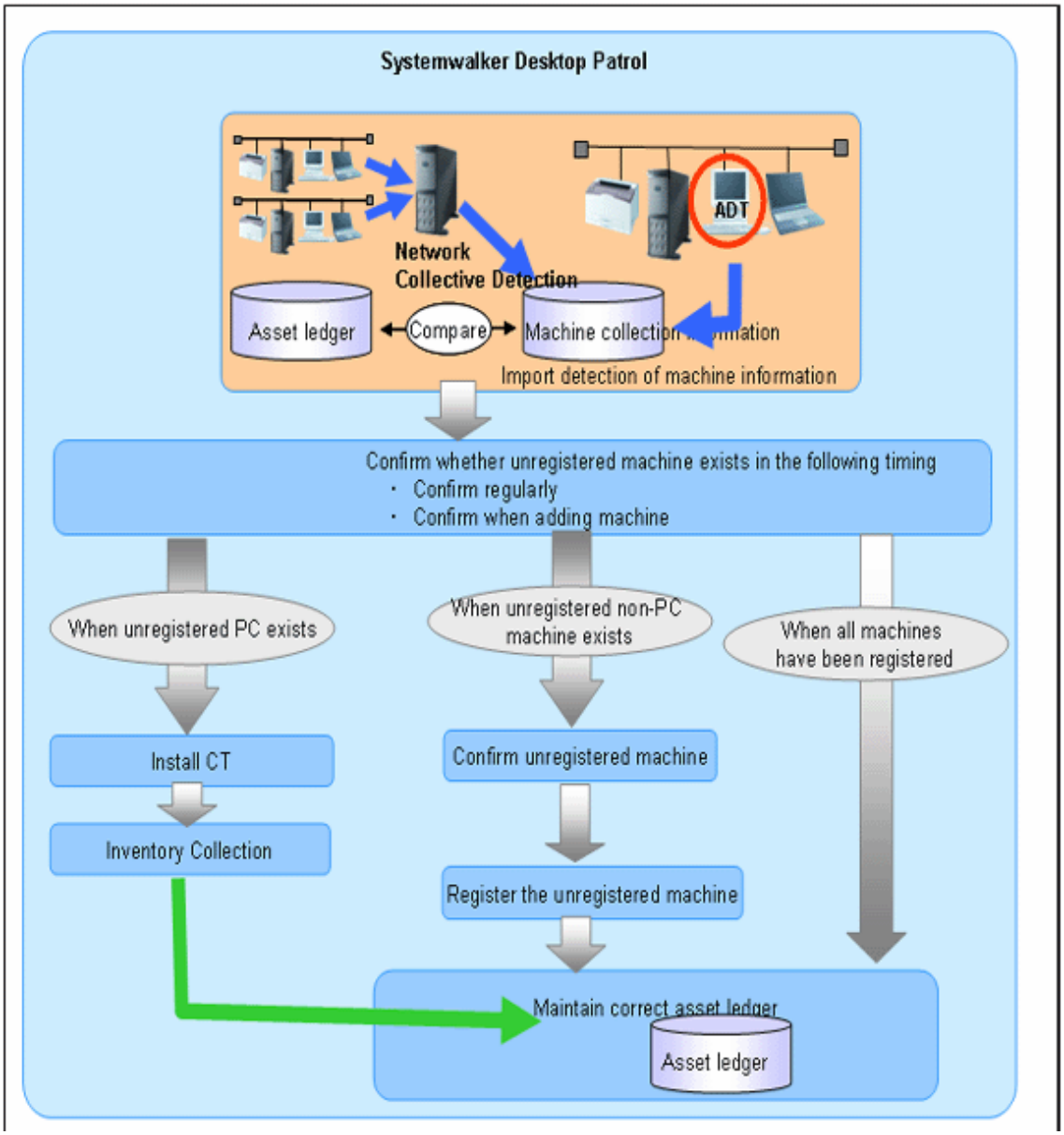
assets management has been performed before installing Systemwalker Desktop Patrol, the current asset information can be reflected and registered when registering collectively to the asset ledger in this operation.

For how to register the unregistered device, refer to "11.2.3.2 Display/Register Unregistered Device".

Through the operations above, even if for PC and device other than PC, they can be registered to the management ledger without missing one, and the asset ledger can be created and maintained correctly.

Operation procedure in the using stage

It describes the procedure for automatic detection and registration of the device information in the using stage.



In the using stage of Systemwalker Desktop Patrol, use the automatic detection function of the device information aiming at maintaining the asset ledger correctly.

The basic procedure is by using this function, register the device which have not been registered to the asset ledger detected through the automatic detection function of the device information to the asset ledger again, and maintain as the correct asset ledger.

Same as the installation stage, for PC, create the asset ledger by using Inventory information collected through Systemwalker Desktop Patrol. For device which have not been connected the network PC (UNIX device, printers, Fax, Router, etc.), the asset ledger will be created by using the automatic detection function of the device information.

The following describes how to maintain the asset ledger when using Systemwalker Desktop Patrol through the automatic detection function of the device information.

[Method for Maintaining Asset Ledger]

1. Confirm regularly whether the unregistered device exist in the **Unregistered Machine** window of the device information automatic detection function.

   In general use, combining the set schedule, weekly or monthly confirmation is enough.

2. If unregistered device exist, confirm the location according to the displayed information.

   Through the information collected as the unregistered device and detailed machine, confirm the detailed information of location, user and machine.

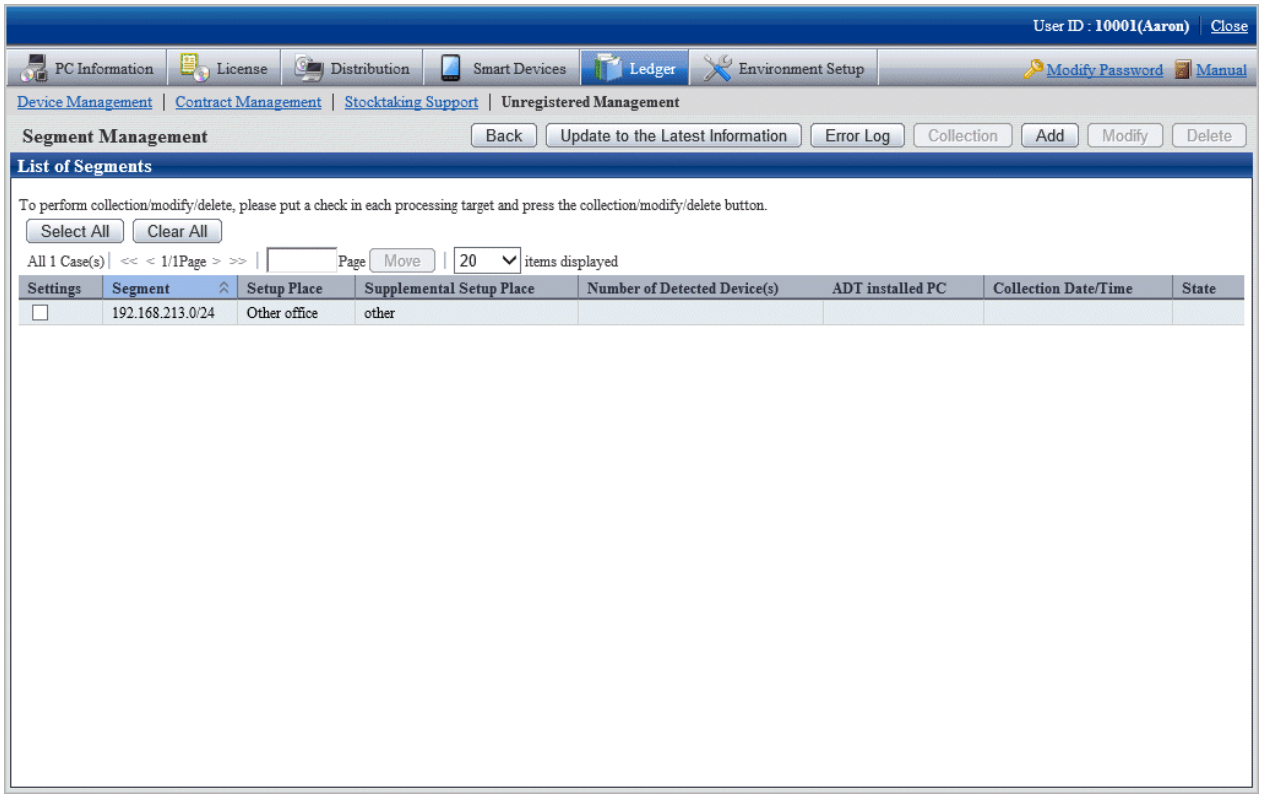
3. Register the unregistered machined to the asset ledger.

   Register the device confirmed in Procedure 2. to the asset ledger.

   When the device is PC, it will be registered automatically through CT information and Inventory collection. When the device is not PC, it will be registered to the asset ledger by using the automatic detection function of the device information.

Using method

1. Set device information collection by schedule.
2. Open the **Assets Management** > **Ledger** > **Unregistered Management** > **Segment Management** window in the main menu.



Items displayed in the Segment Management window

Item	Descriptions
Segment	Display IP address of the network segment in the following format. XXX.XXX.XXX/YY or XXX.XXX.XXX.XXX/YY XXX: Range of network segment IP address YY: Bit value of subnet mask

Item	Descriptions	
	Example: in case of 20-bit subnet mask XXX.XXX.XXX/20 in case of 24-bit subnet mask XXX.XXX.XXX.XXX/24 *If 0 is added to be followed by the value, the 0 will be removed. Example: entered value 192.000.002 configuration value 192.0.2	
Setup Place	Display the setting location defined in the network segment.	
Supplemental Setup Place	Display the supplement for the setting location defined in the network segment.	
Number of Detected Device(s)	Display the number of automatically detected machined.	
ADT installed PC	Display the computer name, IP address and MAC address of PC automatically detected through ADT detection machine. When detecting by using "Batch network check Function", display as "(Collective Detection)".	
Collection Date/ Time	The date and time for notifying automatically the device information. Display in the format of mm/dd/yyyy hh:MM:ss.	
State	**Collecting**	Execute **Request for Collection**, the latest message is shown as in collection.
	(Blank)	Indicate the status other than in collection.

3. Confirm the unregistered device by referring to "11.2.3.2 Display/Register Unregistered Device" and manage the device by referring to "11.3 Device Management".

11.2.3.1 Import Detected Device Information

This section describes how to detect automatically and register the device information.

When connecting CS via network

The device information can be detected through batch network check or network segment-based check.

With either method, it will be notified to Systemwalker Desktop Patrol CS automatically according to the schedule set during installation. Thus, other special settings are not necessary other than "Automatic Detection Schedule Setting" during installation.

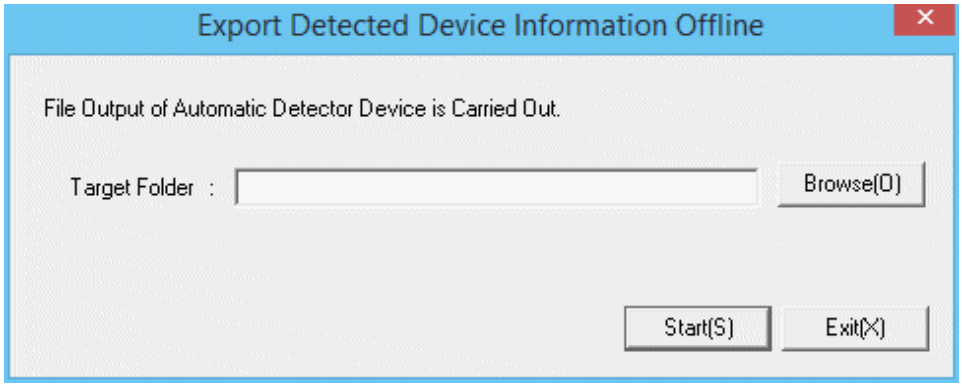
When connecting CS not via network

When the object network segment has not been connected CS via network, the device information of off-line detection should be notified. By using the off-line export function on PC with ADT installed, the device information is output in CSV.

The procedure for notification is as follows:

1. On ADT, click **Start** > **All Programs** > **Systemwalker Desktop Patrol ADT** > **Export Detected Device Information**, or **Apps** > **Systemwalker Desktop Patrol ADT** > **Export Detected Device Information**.

   The following window is output.



2. Set the following information and click the **Start** button.

Item	Descriptions
Target Folder	Specify the folder for the output device information.

   The device information will be output to the output target folder in the following format.

   [Output Format] "ADT_yyyymmddhhMMssn.adt"

   yyyymmddhhMMss: execution date and time (year, month, day, hour, minute and second in the Christian era)

   n: the retry times in case the file name is repeated when exporting multiple ADT information

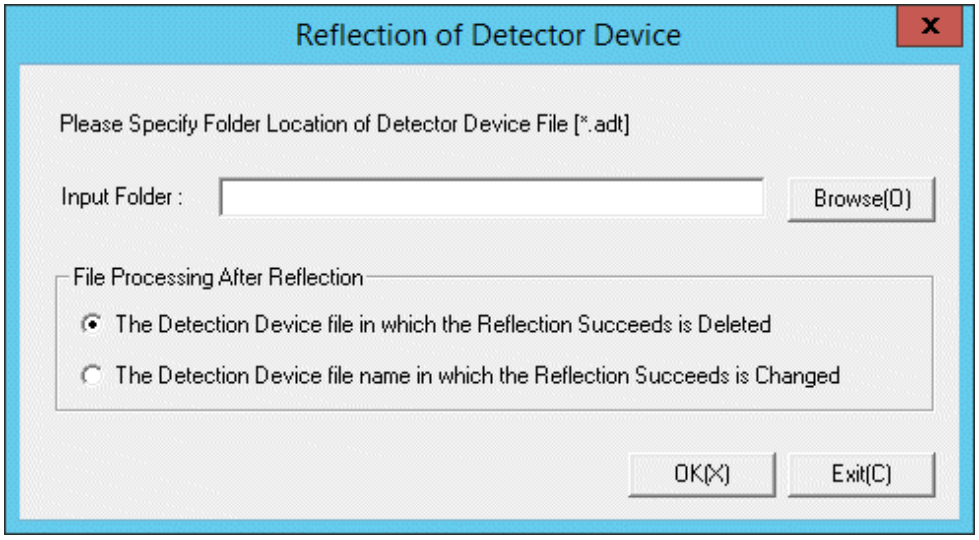
Do not modify the output file name

After the output file name is modified, **Reflect Detected Device** in CS performed in Procedure 4. might fail. So do not modify the output file name

3. Save the file output in "2." to an arbitrary folder on CS by using the removable media.

4. On CS, click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Reflection of Detector Device**, or **Apps** > **Systemwalker Desktop Patrol** > **Reflection of Detector Device**.

   The following window is output.



5. Set the following information and click the **OK** button.

Item	Descriptions
Input Folder	Specify the folder for saving the device information.
File Processing After Reflection	Select the file processing method after reflection. - **The Detection Device file in which the Reflection Succeeds is Deleted** (Initial Value) After reflection, the detected device file with reflection completed will be deleted. - **The Detection Device file name in which the Reflection Succeeds is Changed** After reflection, modify the name of the detected device file with reflection completed as "yyyymmddhhMMssn.old".

The device information is reflected.

Confirmation method when the device information cannot be collected

The notification date and time of the device information can be confirmed in the unit of network segment. In case this notification date and time is not updated within a certain period, it might not be able to collect the device information.

The method for confirmation when the device information cannot be collected is as follows:

ADT log confirmation

In case communication error occurred when notifying the errors when collecting the device information and the device information to CS through ADT, the error will be output to ADT log.

The procedure for confirming ADT log is as follows:

1. On ADT, click **Start** > **All Programs** > **Systemwalker Desktop Patrol ADT** > **Scheduling of Automatic Detection**, or **Apps** > **Systemwalker Desktop Patrol ADT** > **Scheduling of Automatic Detection**.
2. Click the **Log Viewing Display** button in the **Scheduling of Automatic Detection** window.

   The error log window will be displayed

   Confirm the content of error log, and handle it according to the errors.

CS log confirmation

In case errors occurred when saving the device information detected through batch network check/ADT (when reflecting to the database), logs will be collected on CS. For the confirmation of logs on CS, refer to "11.2.3.2 Display/Register Unregistered Device".

11.2.3.2 Display/Register Unregistered Device

By comparing the device collected information connected the network with the asset ledger, the information of the unregistered device which have not been registered to the asset ledger can be displayed in the window. Besides, for device displayed as unregistered device, they can be registered to the asset ledger.

The device collected information displayed here has nothing to do with the collection method of the device, it will be saved for 60 days from the date and time for automatic detection.

The device information in this period will accumulate the collected content of device information. However, when modifying the network segment for batch network check as network segment-based check in this period, the device information in the correspondent network segment will be replaced as the content of network segment-based check.

Startup method of the unregistered management window

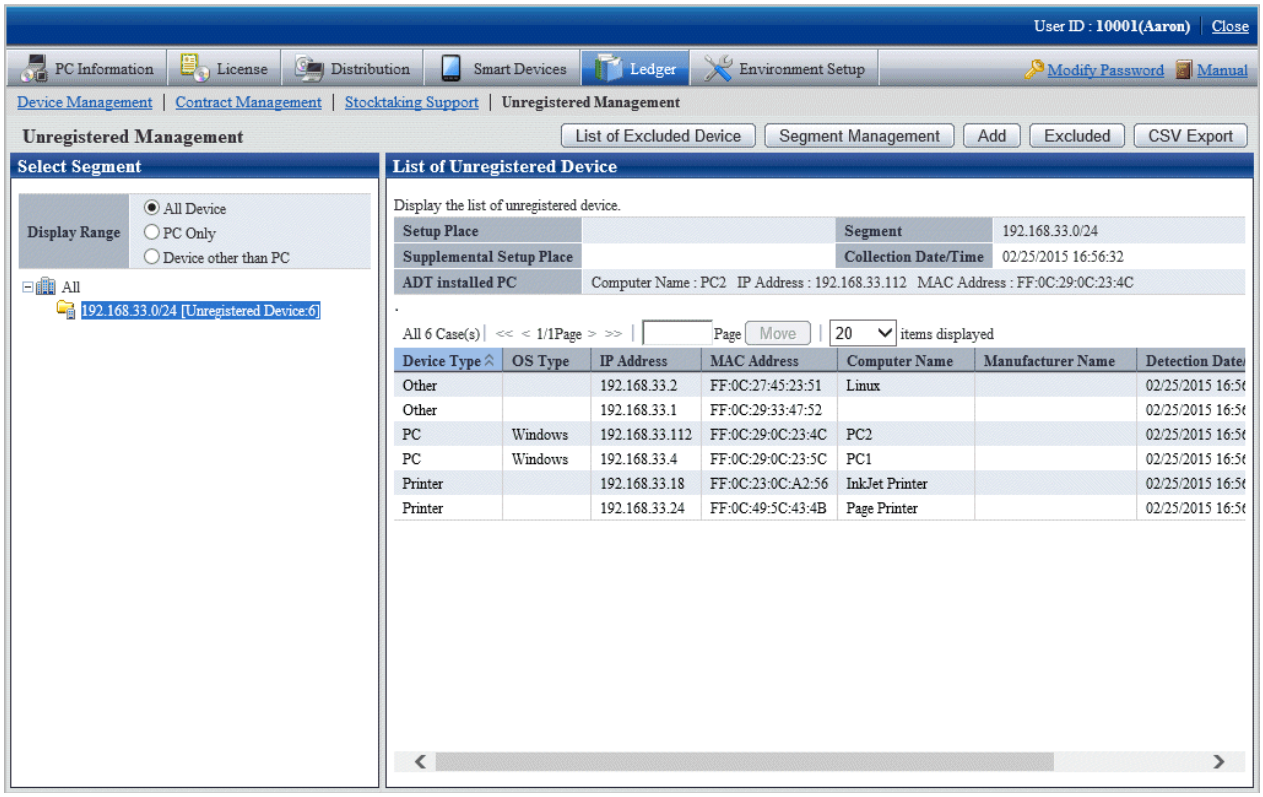
The method for starting the **Unregistered Management** window is as follows:

1. Log onto the main menu and click the **Ledger**.

   The **Ledger** window will be displayed

2. Click **Unregistered Management**.

   The following window will be displayed



When the displayed message is more in each list window displayed in the unregistered management window, the message can be moved to the specified page. Besides, the number of items displayed in one page can be set.

Linked network segment and setting location

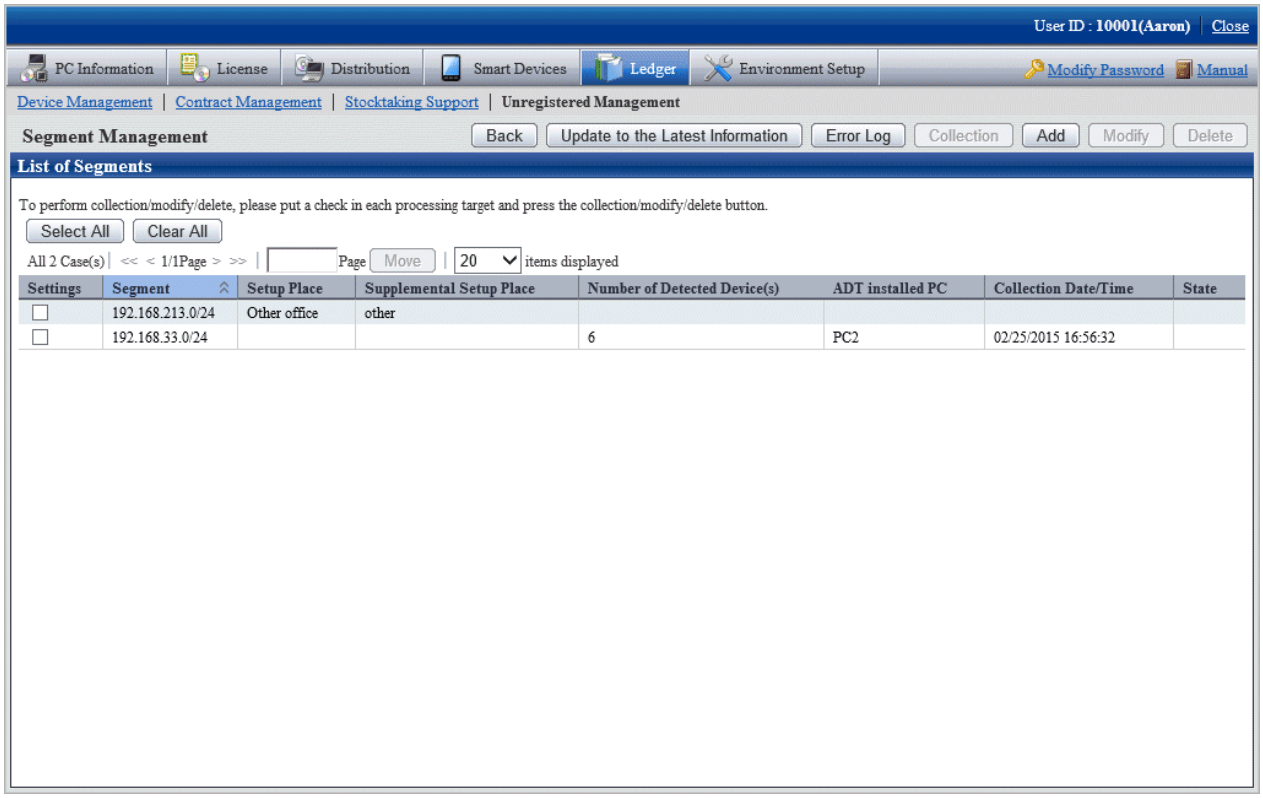
Before displaying the unregistered device/using the registration function, the segment management setting linked with the network segment and setting location name is required. The segment management setting is performed through **Segment Management** window.

If the collection of device information is requested via network segment-based check, the network segment and name of the setting location may not have been linked. In this case, this task must be performed.

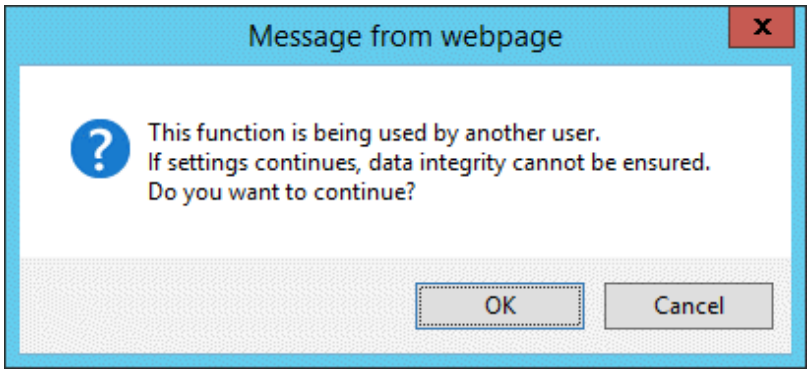
Besides, the building name in the building management information will be used in the setting location linked with the network segment, so perform the segment management setting after registering the building management information.

1. Click the **Segment Management** button in the **Unregistered Management** window.

   The following **Segment Management** window is displayed. Click the **Add, Modify,** or **Delete** button in the window to edit the network segment information.



   The following information will be displayed after clicking the **Segment Management** button. This message appears when other user is displaying the segment management window.



   [Item of Each Button]

Item	Descriptions
Back	Display **Unregistered Management** window.
Update to the Latest Information	Update the **Segment Management** window to the latest status. After specifying **Collection**, update the network segment whose **Status** is **Collecting** to the latest status for use. *When the status of **Collecting** continues, even if clicking the **Update to the Latest Information** button, the **Segment Management** window will always be **Collecting**, but it will not be updated, pay attention to this.

Item	Descriptions
Error Log	It is the collection status log notified by the message through batch network check/ADT. For log confirmation, refer to "Error Log".
Collection	For ADT of the network segment after selecting **Location**, request to collect the latest information. After making request, the **Request for Collection** window can be switched to, confirm whether the request succeeded or not. *For network segment whose **Status** is **Collecting**, request for collection will not be sent after clicking **Request for Collection**, pay attention to this.
Add	Add new definitions for the network segment and setup place. For adding procedure, refer to "Register".
Modify	Modify the definition of the registered network segment and setup place after selecting **Set**. If multiple network segments have been selected, the **Modify** button will be grayed out and cannot be clicked. For modification procedure, refer to "Modify".
Delete	Delete the definition of the registered network segment and setup place after selecting **Set**. For deletion procedure, refer to "Delete".

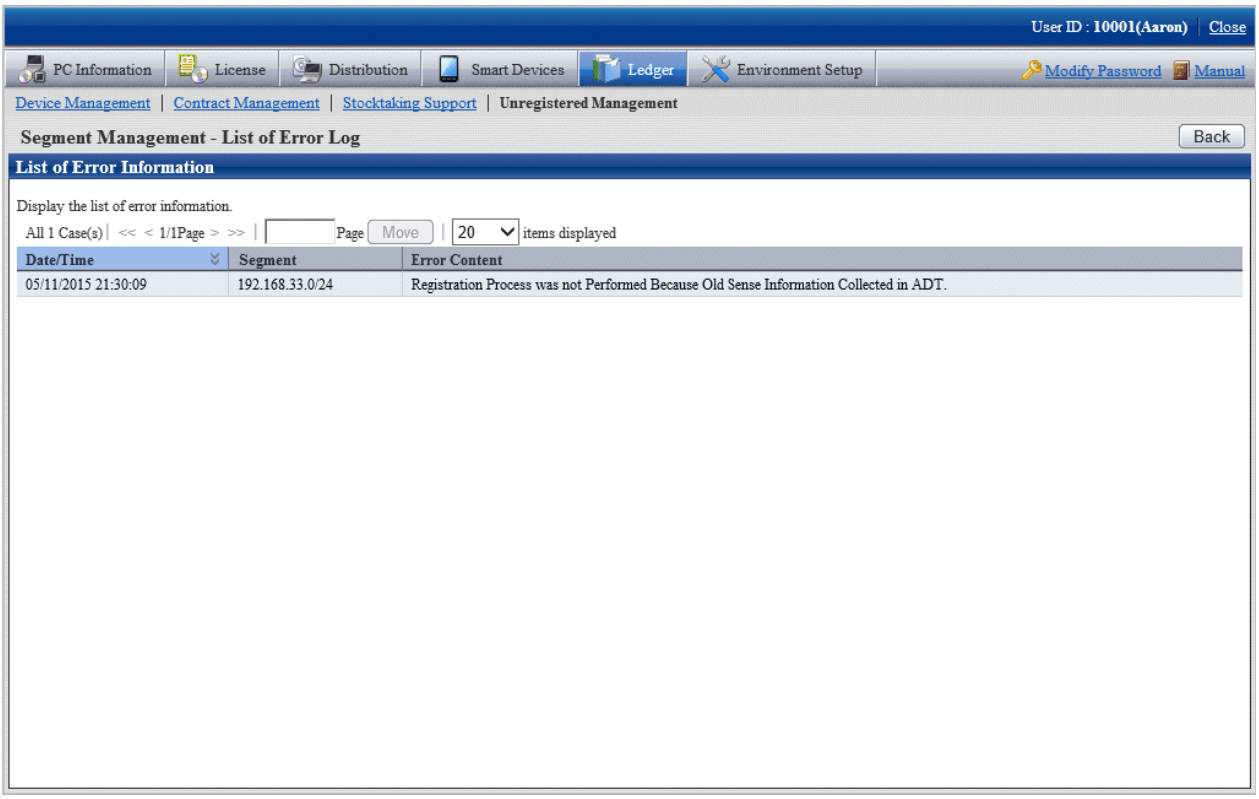
[Items Displayed in the Segment Management window]

Item	Descriptions
Segment	Display IP address of the network segment in the following format. XXX.XXX.XXX/YY or XXX.XXX.XXX.XXX/YY XXX: range of IP address of the network segment YY: Bit value of subnet mask Example: in case of 20-bit subnet mask XXX.XXX.XXX/20 in case of 24-bit subnet mask XXX.XXX.XXX.XXX/24 *If 0 is added to be followed by the value, the 0 will be removed. Example: entered value 192.000.002 configuration value 192.0.2
Setup Place	Display the setting location defined in the network segment.
Supplemental Setup Place	Display the supplement for the setting location defined in the network segment.
Number of Detected Device(s)	Display the number of device detected by batch network check/ADT.
ADT Install PC	Display the computer name, IP address and MAC address of PC automatically detected through ADT detection machine. When detecting by using "Batch network check Function", display as "(Collective Detection)".
Collection Date / Time	The date and time for notifying the device information through batch network check/ADT.

Item	Descriptions	
	Display in the format of mm/dd/yyyy hh:MM:ss.	
State	**Collecting**	Execute **Request for Collection** and the latest message is shown as in collection.
	(Blank)	Indicate the status other than in collection.

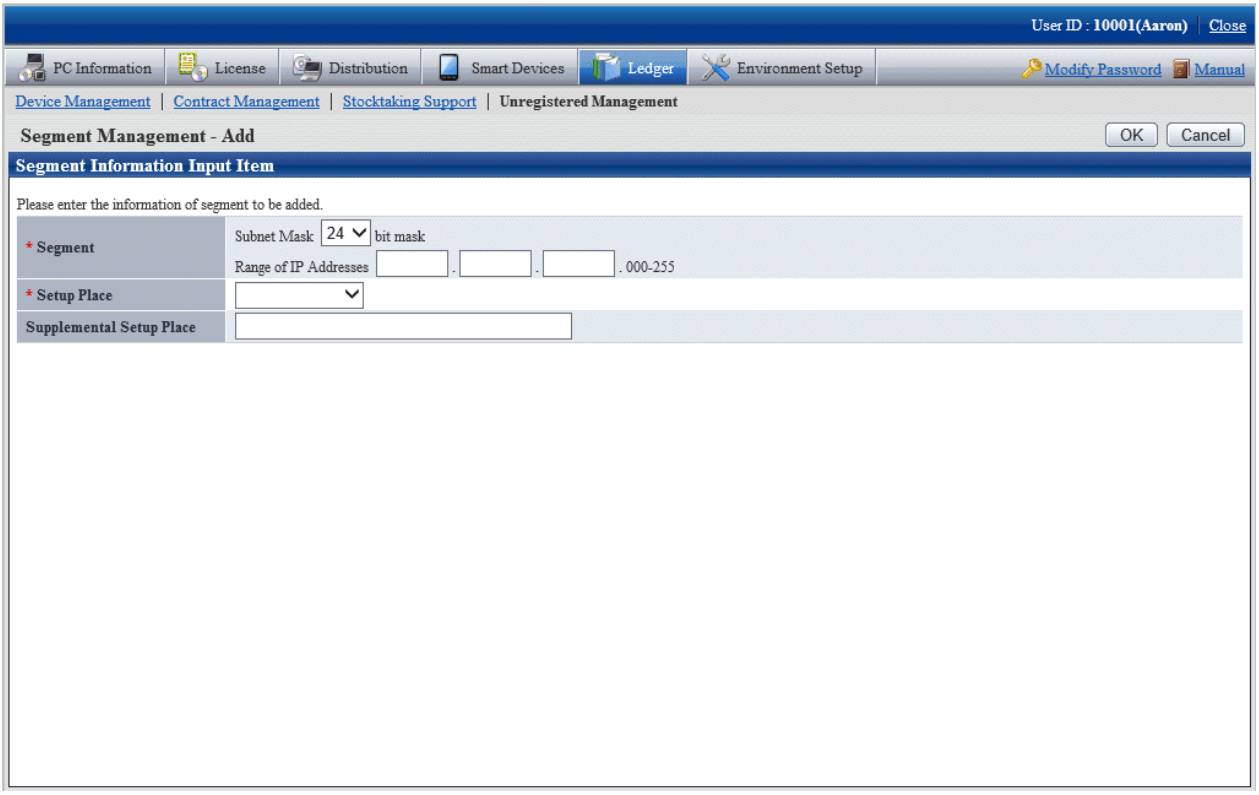
Error log

After clicking the **Error Log** button, the **Segment Management - List of Error Log** window will be displayed. The error log generated when receiving through batch network check/ADT will be output in the window, confirm the content.



Register

After clicking the **Add** button, the **Segment Management - Add** window will be displayed. Input the network segment information in the following window and click the **OK** button.

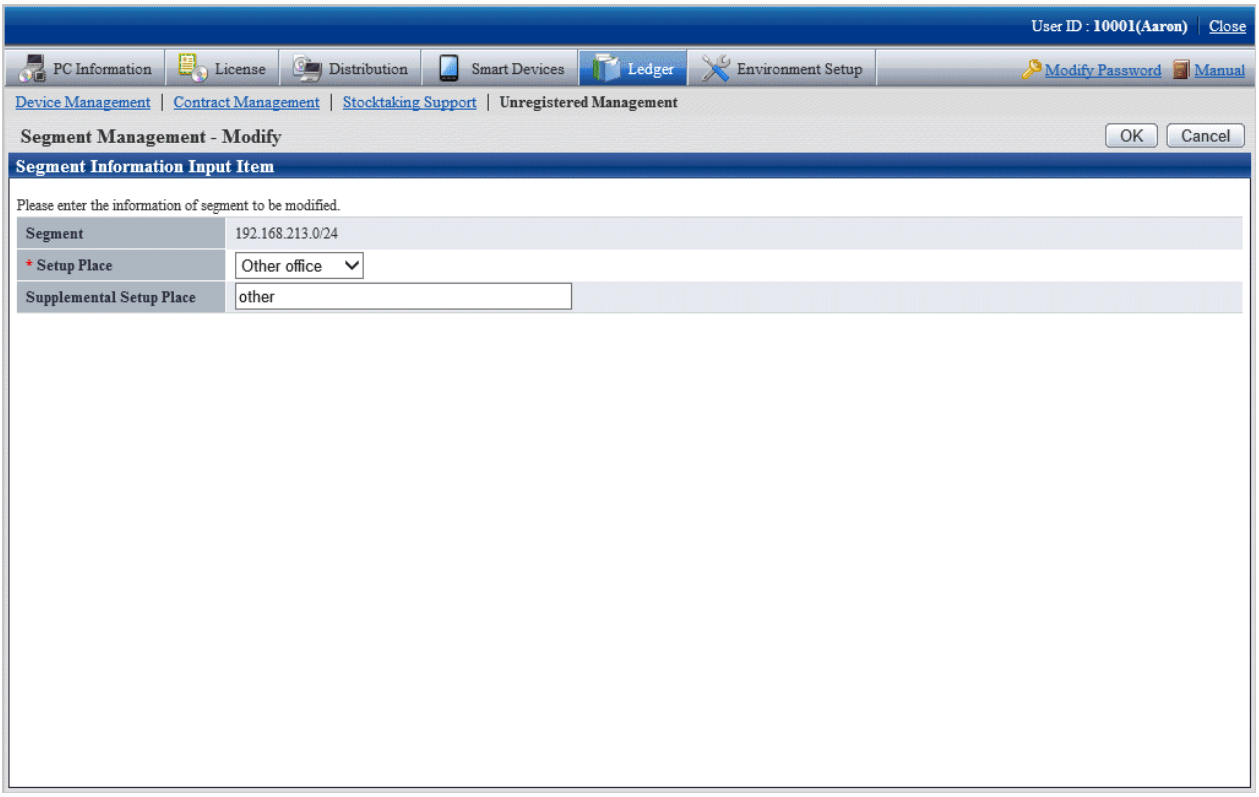


[Add Setting Items of Network Segment]

Item	Descriptions
Segment (Required)	Set the added registered network segment by using the following format. Subnet Mask: YY bit mask Range of IP Address: [XXX.XXX.Range.000-255] or [XXX.XXX.XXX.Range] XXX: single-byte numbers can be set within 0~255. YY: the mask value of subnet can be set within 16~28. The selection range is changed along with the mask value of subnet.
Setup Place (Required)	Select the setting location of the network segment. The building name of the building management information of Systemwalker Desktop Patrol can be selected.
Supplemental Setup Place (Required)	Set the supplement for the network segment setting location. When multiple network segments belong to the same setting location, the supplement information for identification is set in this item. Example) Setting location: Kanto Head Office Supplement: south on the 9th floor Specify up to 10 fullwidth or 20 halfwidth characters.

Modify

After clicking the **Modify** button, the **Segment Management - Modify** window will be displayed. Input the modified network segment information, and click the **OK** button.



[Segment Management-Modify Setting Items in the Window]

Item	Descriptions
Setup Place (Required)	Select the setting location of the network segment. The building name of the building management information of Systemwalker Desktop Patrol can be selected.
Supplemental Setup Place (Required)	Set the supplement for the network segment setting location. When multiple network segments belong to the same setting location, the supplement information for identification is set in this item. Example) Setting location: Kanto Head Office Supplement: south on the 9th floor Specify up to 10 fullwidth or 20 halfwidth characters.

Note

The segment management information should be reset when the organization is modified

When the building management information is modified due to the organization modified, etc., use "Segment Management Window" to reset the segment management information combining the latest organization information. Refer to "Segment Management Window" to confirm whether the setting location has changed to the unset or error setting location, and reset it after confirming the actual situation. (According to the modification of the building management information, situation where resetting is unnecessary exists.)

Delete

After clicking the **Delete** button, the network segment information selecting **Settings** will be deleted.

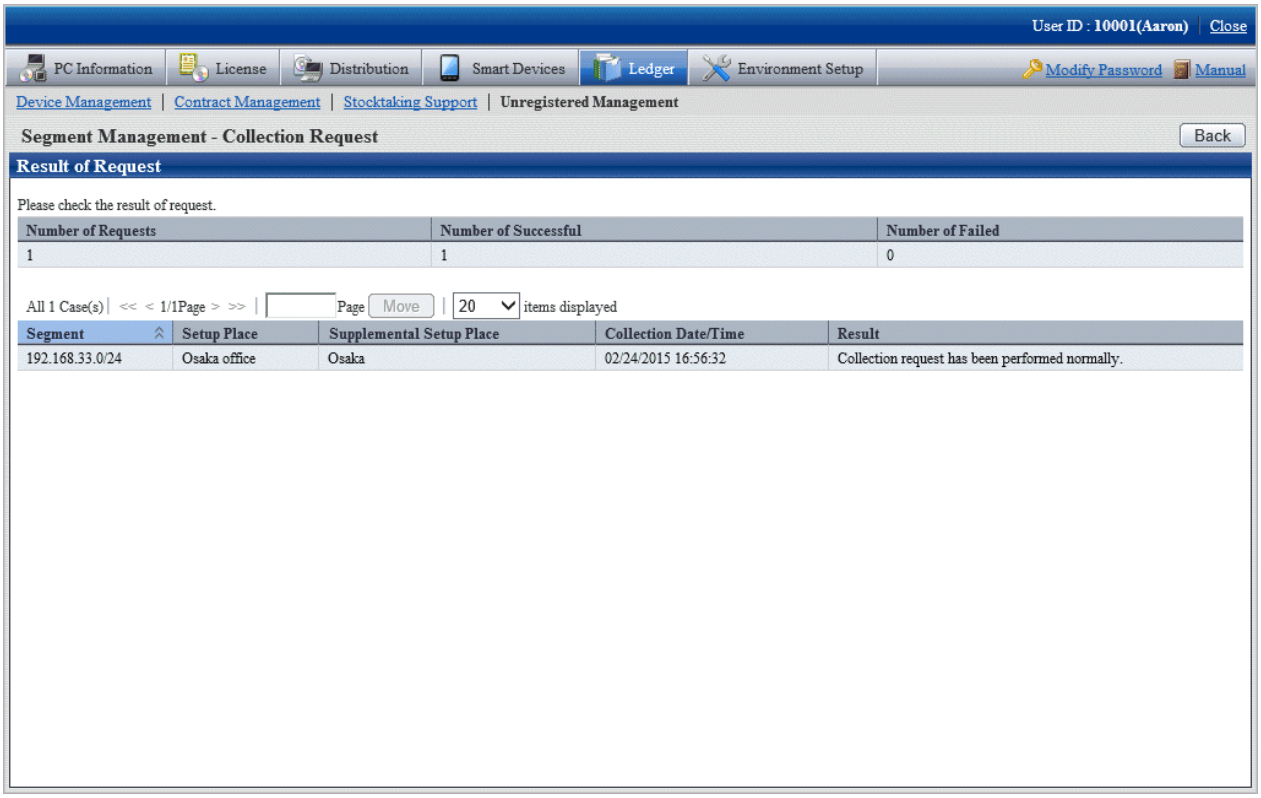
After deleting the network segment information, the device information collected through batch network check/ADT will also be deleted. When the network segment is unnecessary due to network structure modification, etc., delete the network segment information through this function.

Request for collection

After clicking the **Collection** button, the **Segment Management - Collection Request** window will be displayed. Whether the request succeeded can be confirmed in this window.

Note

For network segment whose **Status** is **Collecting**, the request will not be sent out after clicking **Request for Collection**, pay attention.



Click the **Back** button after confirmation, after returning to the **Segment Management** window, the **State** of the network segment requesting for collection will be displayed as **Collecting**.

Click the **Update to the Latest Information** button later. Update the network segment whose **State** is **Collecting** to the latest status.

Note

When the status of **Collecting** continues, even if clicking the **Update to the Latest Information** button, the **Segment Management** window will always be **Collecting**, but it will not be updated. Click the **Update to the Latest Information** button again later for update.

Display/registration function of unregistered device

The following information can be confirmed and set in the display/registration function of the unregistered device.

- Confirm the unregistered device

  The device information can be confirmed in the List of Unregistered Device window.

- Register the unregistered device to the asset ledger

  The unregistered device can be selected in the window and registered to the asset ledger.

  Besides, by using the "Collective Registration/Modification for Asset Information" function, the displayed unregistered device information can also be output to the file that can be registered. For details of "Collective Registration/Modification for Asset Information", refer to "11.2.2 Register/Modify Ledger".

- Set the device not to be registered

  Set not taking the device detected as unregistered as the managed object of asset ledger for processing.

  For example, for device unregistered to the asset ledger such as in case of sharing wireless network card and device brought in temporarily, they can be taken as unregistered device by being set as device not to be registered, and not displayed in the window.

- Confirm device list not to be registered

  The device list set as non registration object can be confirmed.

  Besides, not only the device list not to be registered can be confirmed, but also the following settings can be performed.

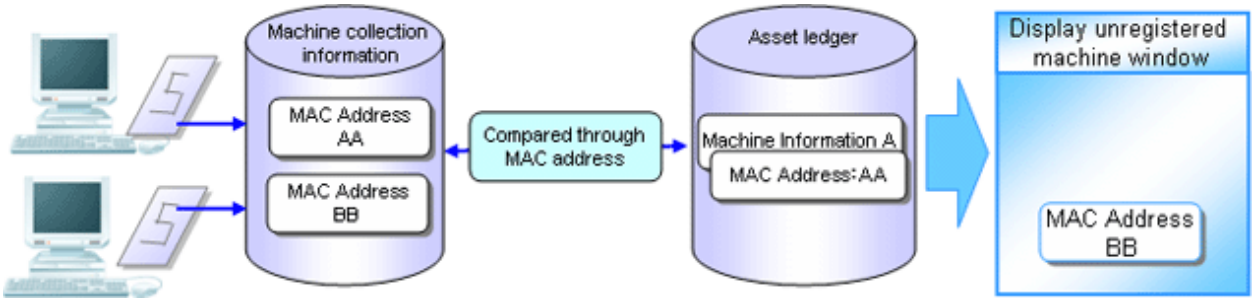
  - Device set as non object for a time can be reset as the managed object of asset ledger.
  - The device set in non object do not exist due to being discarded, etc., they can be deleted from the list of non object device.

Confirm the unregistered device

Confirm the List of Unregistered Device which have not been registered to the asset ledger.

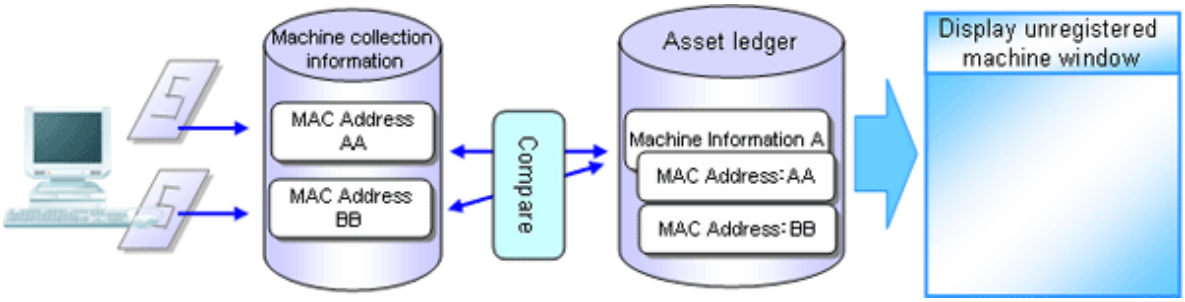
The object device of unregistered device which can be confirmed here are as follows:

[Object of Unregistered Device]
According to MAC address, perform unique management to the device detected automatically through batch network check/ADT. Compare this automatically detected device information (device collected information) with the device information of the asset ledger according to MAC address, and display the device of MAC address which has not been registered to the asset ledger as unregistered device in the window.

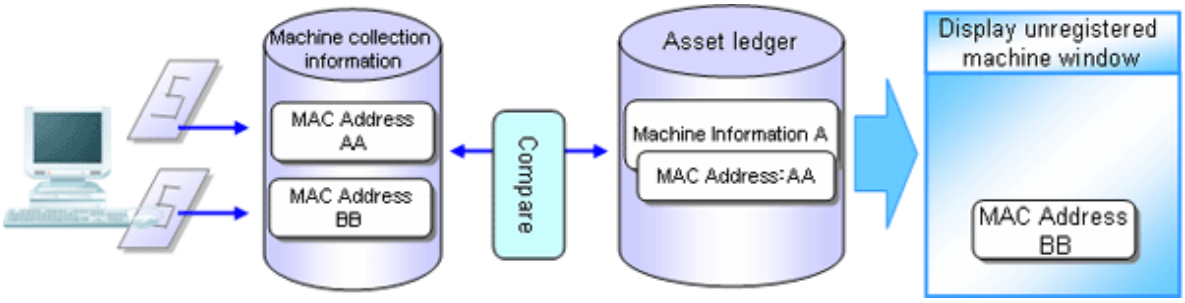


[In case of the device having 2 MAC addresses]

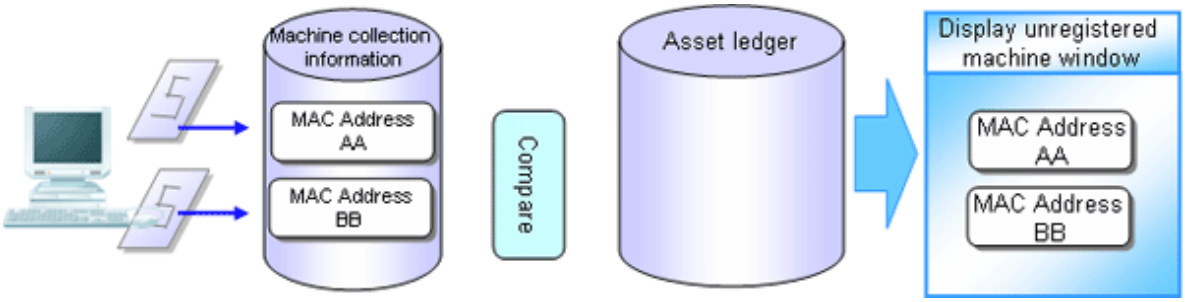
- When the MAC addresses of both parties have been registered to the asset ledger, they will not be displayed as unregistered device in the window.



- When the MAC address of only one party has been registered to the asset ledger, one unregistered device will be displayed in the window. At this time, the MAC address of the device which is displayed as the unregistered device and the device of the asset ledger should be linked and registered.



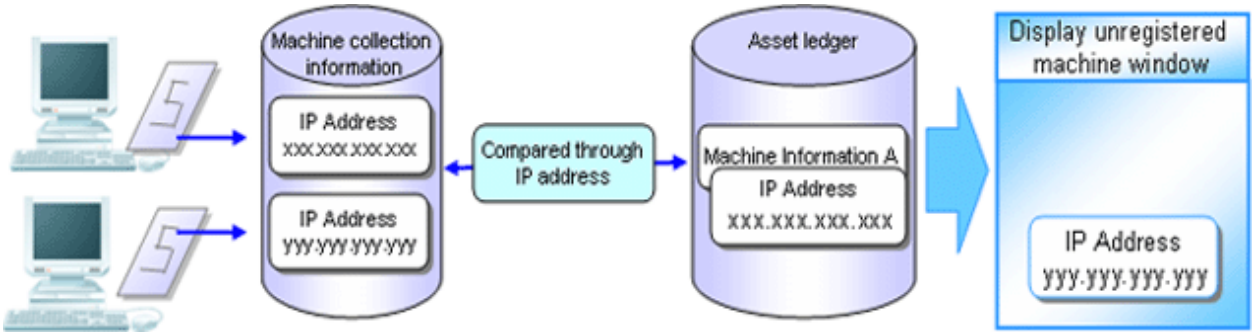
- When the MAC addresses of both parties have not been registered to the asset ledger, the both parties will be displayed as unregistered device in the window. At this time, the MAC addresses of both parties should be registered as one machine.



[In case of the device which has not gotten MAC address]

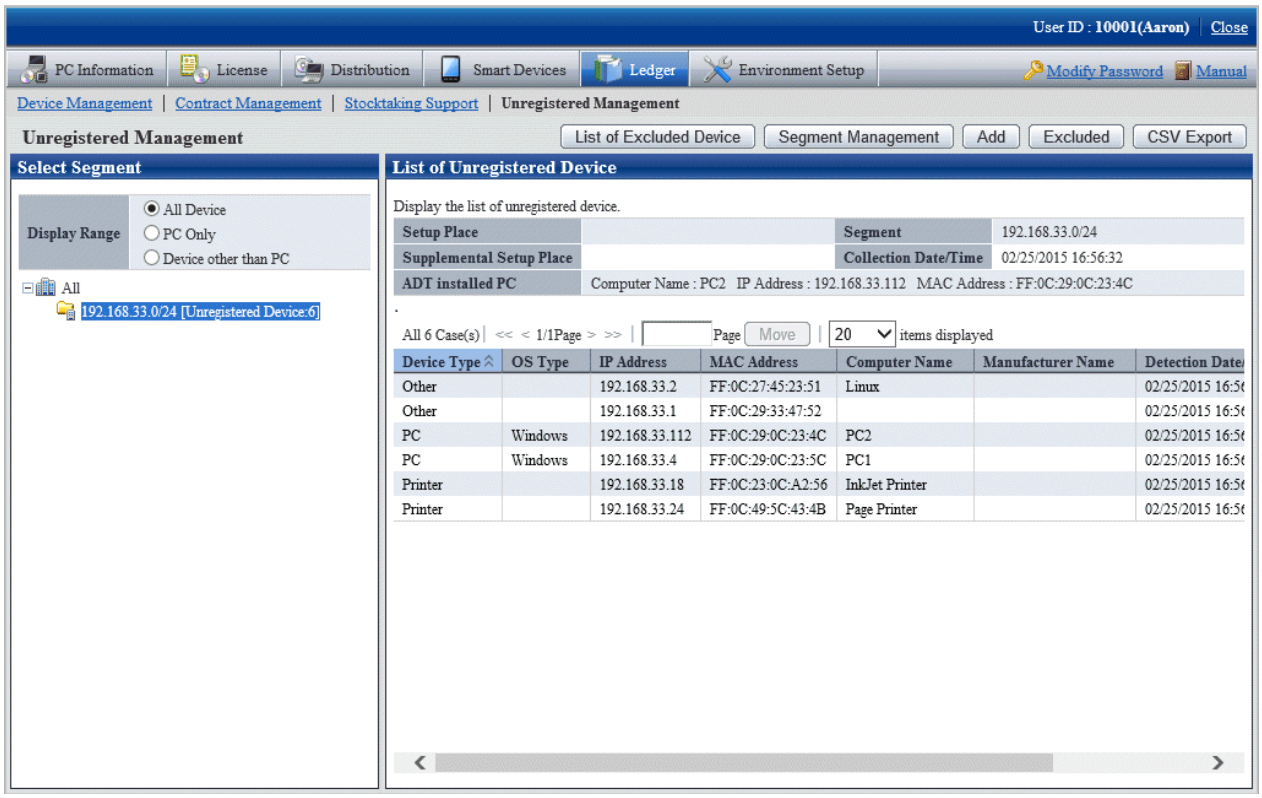
During batch network check, device which cannot get MAC address might be detected.

The device which has not gotten the MAC address is compared with the device of the asset ledger according to IP address, and the device whose IP address has not been registered to the asset ledger is displayed as unregistered device in the window.



The procedure for confirmation is as follows:

1. The following **Unregistered Management** window is displayed.



2. After selecting the network segment and Display Range to be confirmed in the unregistered management window, the **List of Unregistered Device** will be displayed.

Item	Descriptions
List of Excluded Device	Display **List of Excluded Device** window. For details of **List of Excluded Device** window, refer to "Confirm List of Excluded Device".
Segment Management	Display **Segment Management** window. For details of **Segment Management** window, refer to "Linked Network Segment and Setting Location".
Add	Register the unregistered device to the asset ledger. For details, refer to "Register Unregistered Device to Asset Ledger".
Excluded	Set the unregistered device as processing not as unregistered device. For details, refer to "Non Object Setting of Unregistered Device".
CSV Export	Output CVS file for registering collectively the unregistered device. For details, refer to "Register Unregistered Device to Asset Ledger".

[Items Displayed in the List of Unregistered Device Window]

Item	Descriptions
Select Segment	Display the network segment list in the form of tree (display in the descending order of number of unregistered device). Take the whole company as the root directory and display the network segment under which the unregistered device exist in the following format (not display the network segment where unregistered device do not exist).

Item	Descriptions
	The setting location of network segment (supplement for setting location) [Number of Unregistered Device: n] The setting location: setting location name set in the network segment Display IP address when the setting location has not be set. Supplement for setting location: the setting location set in the supplemented network segment Not displayed when the supplement for setting location has not been set. n: detected number of unregistered device By selecting the network segment, display the list of network segment subordinate unregistered device. When the whole company is selected, the list of all registered device will be displayed.
Display Range	As unregistered device, select the device displayed in the right from the following ranges. - **All device** - **PC only** - **Device other than PC** Besides, after modifying this configuration value, it will be displayed again according to the selected Display Range of the network segment selection tree.
Setup Place	Display the setting location name set in the network segment. *In case the network segment of the setting location has not been set in the segment management, it will be blank.
Segment	Display IP address of the network segment.
Collection Date/ Time	Date and time for notifying the device information through batch network check/ADT. Display in the format of mm/dd/ yyyy hh:MM:ss.
Supplemental Setup Place	Display the supplement for the setting location set in the network segment. *In case the network segment of this item has not been set in the segment management, it will be blank.
ADT installed PC	Display the computer name, IP address and MAC address of PC automatically detected through ADT detection machine. When detecting by using the "Batch network check" function, displayed as "(Collective Detection)".
Device Type	Display the device category. The device are divided into the following 3 categories. - **PC** - **Printer** - **Network Machine** - **Other** For device that is non PC, printer and network machine, and device that cannot be determined as PC or printer or network machine, the device type will be **Other**. If the following settings are performed, even if it is PC, situation where it cannot be determined as PC exists.

Item	Descriptions
	- When set as being not able to view computers from external in the settings of Windows - When set as being not able to view from external in the settings of Fire Wall of anti-virus software
OS Type	Display OS category of "Windows", "Solaris", and "Linux" machine. For Windows, the device category that can be determined as PC will be displayed. For Solaris and Linux, device that can get SNMP information will be displayed. If the device is non PC device such as printer and HUB, and device which cannot be determined the OS category, it will be blank.
IP Address	IP address of the machine. IPv6 device information is not displayed.
MAC Address	MAC address of the machine.
Computer Name	Computer name or host name of the machine.
Manufacturer Name	Manufacturer name of the machine. When SNMP unsupported or getting SNMP information limited if the device type is non **PC** and not supporting SNMP, it will be unset. If the value has been set, it will be used as the reference information for determining the device category in the administrator.
Detection Date/ Time	Detect the date and time of the device information. Display in the format of mm/dd/ yyyy hh:MM:ss.
Supplement	Supplement for the machine. Display the device annotation set in SNMP. When SNMP unsupported or getting SNMP information limited if the device type is non **PC** and not supporting SNMP, it will be unset. If the value has been set, it will be used as the reference information for determining the device category in the administrator.

[Notification Content of Unregistered Device]

The automatically detected device information when notifying the device information will be accumulated as the previous detection result after the new information is notified, and the device information previously or earlier is reserved.

Register the unregistered device to the asset ledger

Register the device taken as unregistered device to the asset ledger.

There are 3 methods for registration:

- Register to the asset ledger after confirming the unregistered device one by one

  It is mainly to detect the unregistered device and used when the number of the unregistered device is less.

- Register collectively the unregistered device to the asset ledger.

  It is mainly used when a large number of unregistered device exist such as during installation.

- Register after linking the unregistered device and the device which have been registered to the asset ledger

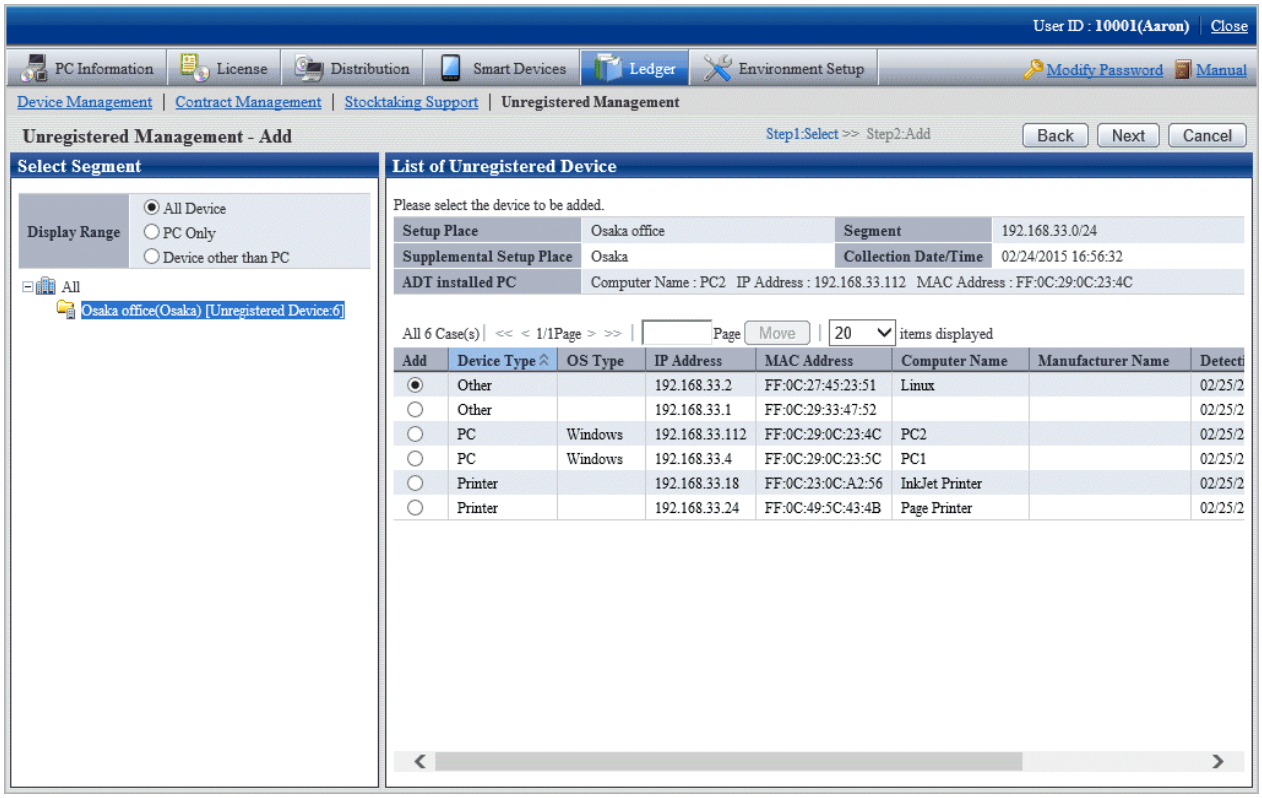
  Since the MAC address of the device has not been registered while the device has been registered to the asset ledger, for device detected as unregistered machine, register it after linking it with the device of the asset ledger.

As registration method, use the **Device Management** > **Modify Device Information** and **Collectively Register/Modify Asset Ledger** function to add and register the MAC address of device to be linked and registered to the current device information. After completing the registration, the correspondent device information will be displayed through the **List of Unregistered Device** window.

The procedure for registering to the asset ledger after confirming the unregistered device one by one:

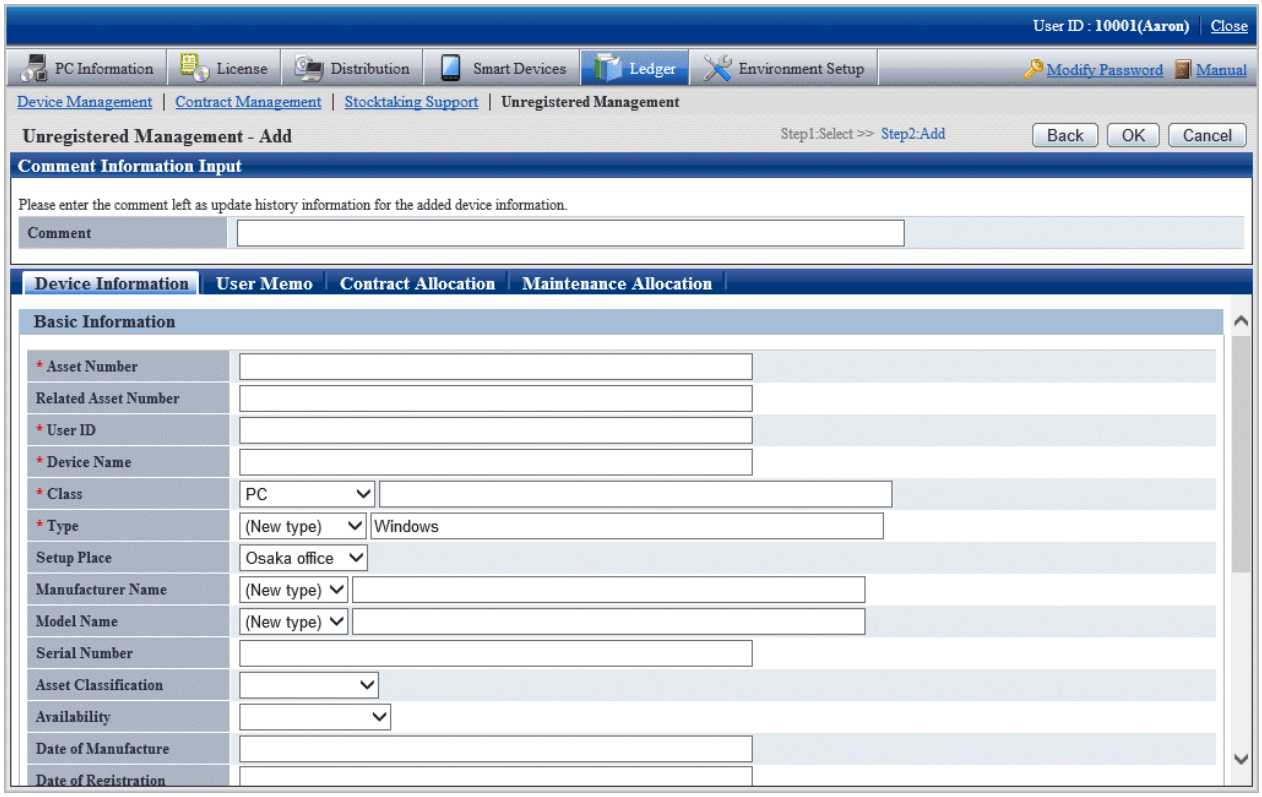
1. Click the **Add** button in the **Unregistered Management** window.

   The following window will be displayed



2. Select the device to be registered and click the **Next** button.

   The following window will be displayed

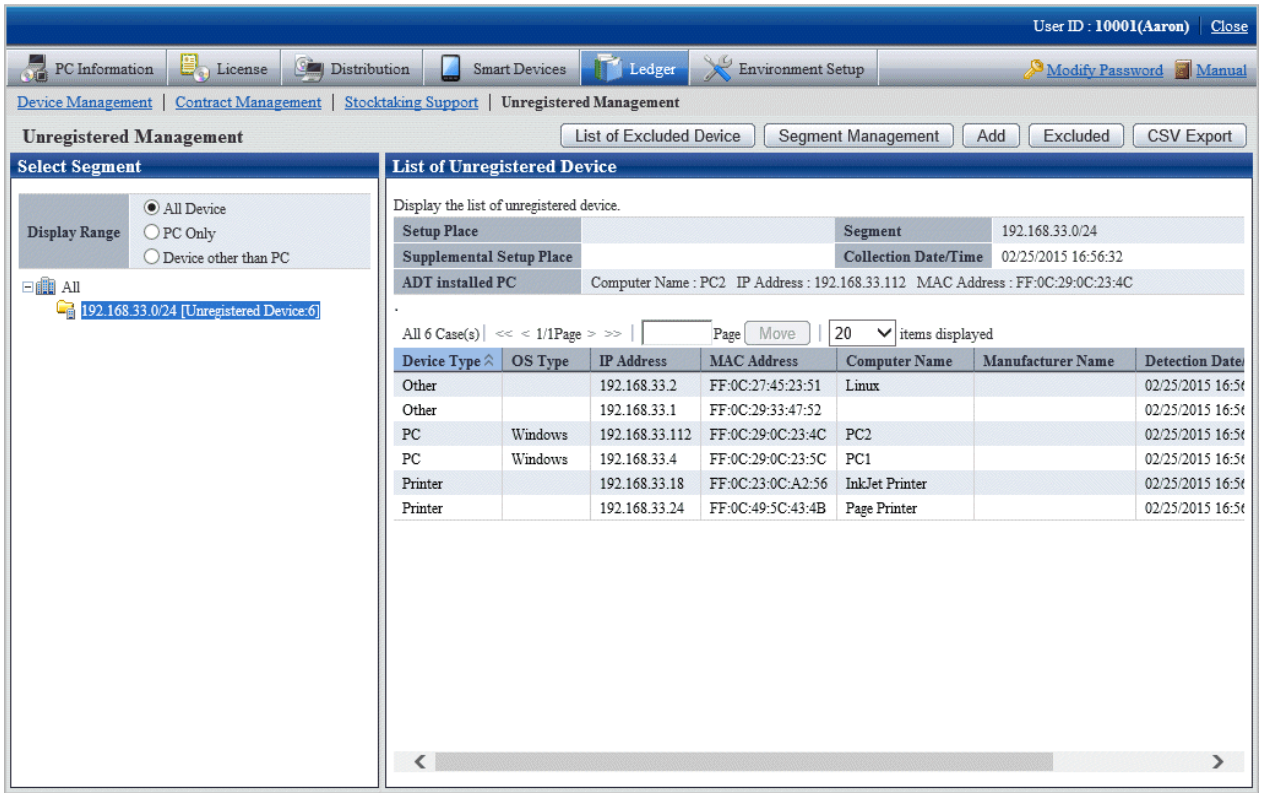


3. Set the necessary information in the input box of the selected device and click the **OK** button.

   The procedure for registering the unregistered device to the asset ledger collectively is as follows:

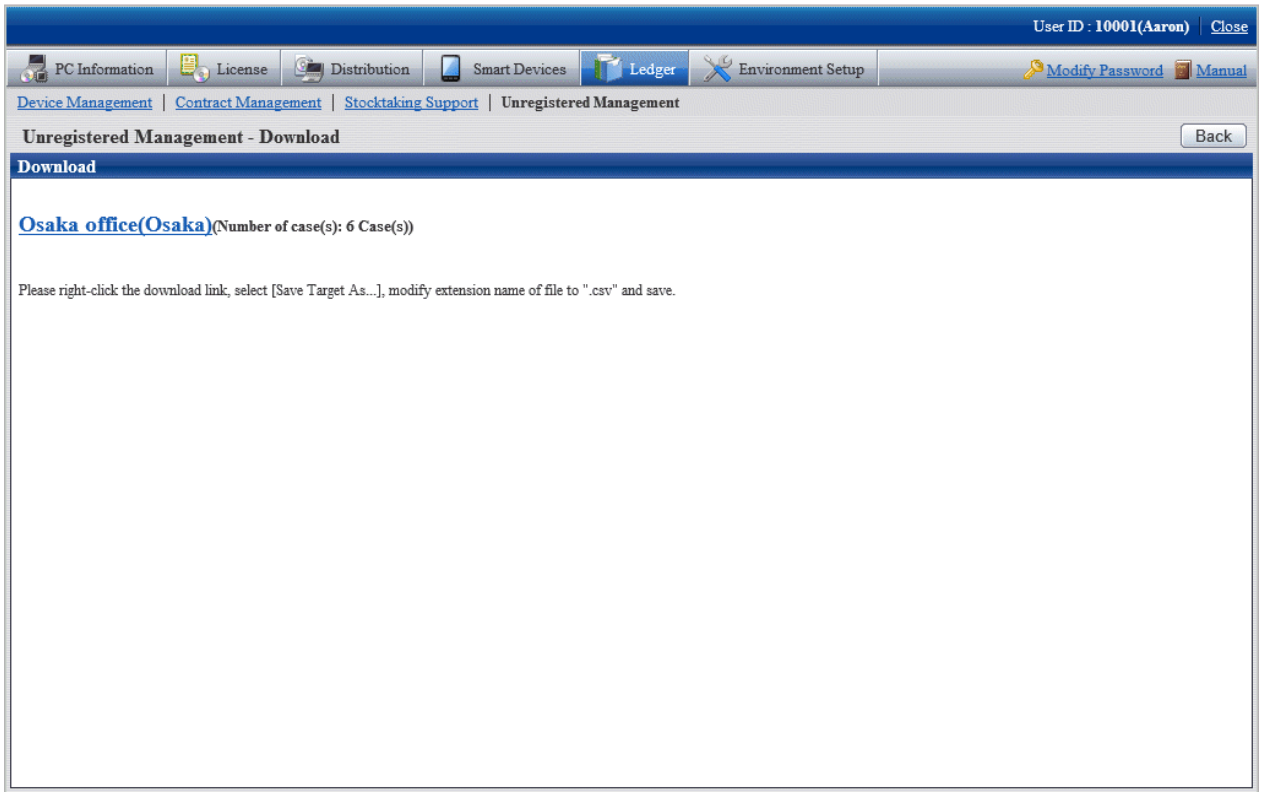
4. Select the network segment and Display Range in the **List of Unregistered Device**, the Unregistered Device List to be registered collectively is displayed.

   The following window will be displayed



5. Click the **CSV Export** button.

   The following window will be displayed



6. The window for outputting CSV files that can be used by the **Collectively Register/Modify Asset Information** feature will be displayed.

   According to the directions in the window, save the file.

7. Use the **Collectively Register/Modify Asset Information** function to set the information required by registration in CSV export file. Besides, if it has been output in CSV, the information collected as the unregistered device information will be set in the following item.

   [Initial value of the output CSV file]

Item	Initial Value
Class	Device classification of the unregistered device
Type	OS category of the unregistered device
Model Name	Supplement for the unregistered device
Setup Place	Setting location of the network segment
Manufacturer Name	Manufacturer name of the unregistered device
IP Address 1 (for IPv4)	IP address of the unregistered machine
MAC Address 1	MAC address of the unregistered machine

8. By using the **Collectively Register/Modify Asset Information** function, register the file edited in Procedure 7.

   After completing the registration, device which have been registered to the **List of Unregistered Device** window will not be displayed.

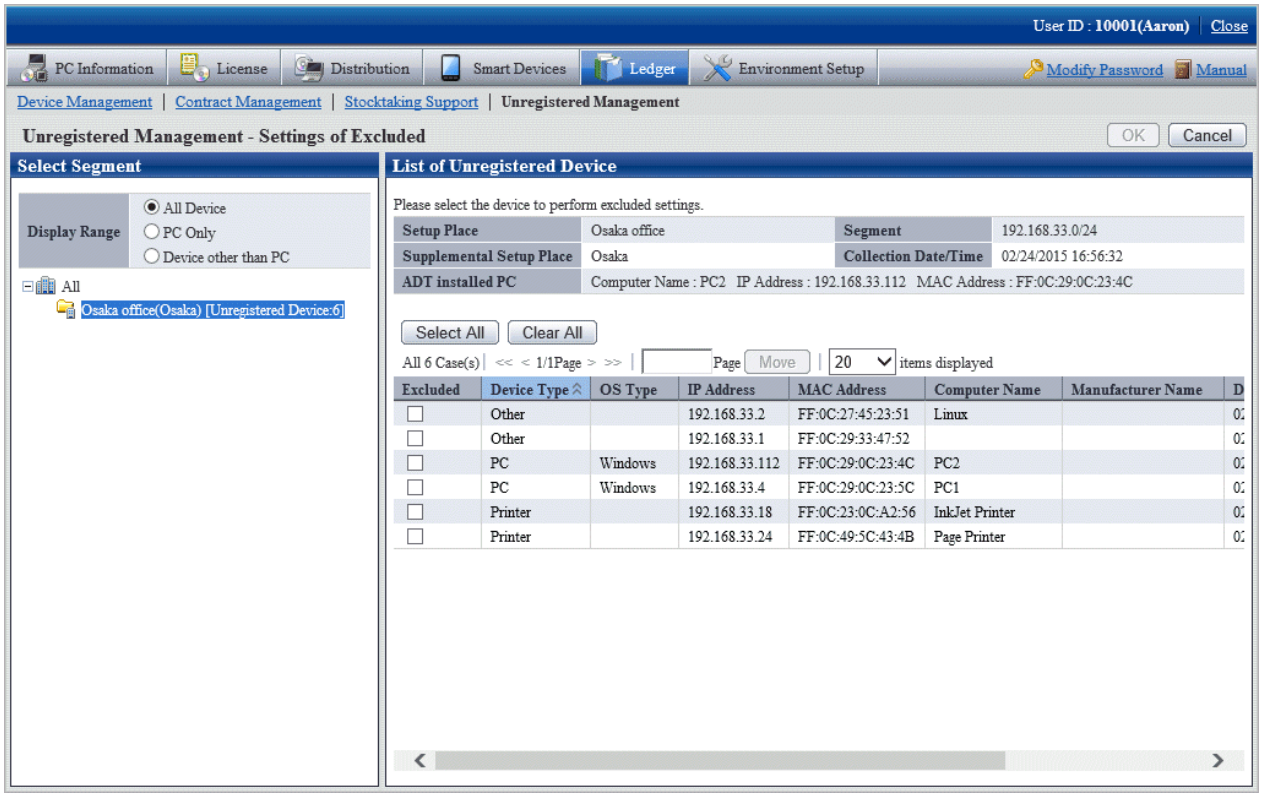
Set device not to be registered

Set the device not to be registered of the asset ledger.

The procedure for setting is as follows:

1. Click the **Excluded** button in the **Unregistered Management** window.

   The following window will be displayed



2. Select the device to be the object and click the **OK** button.

   The selected device is set as the device not to be registered of the asset ledger.

   The device which has been set as non object will not be displayed in the **List of Unregistered Device**.

Confirm excluded device list

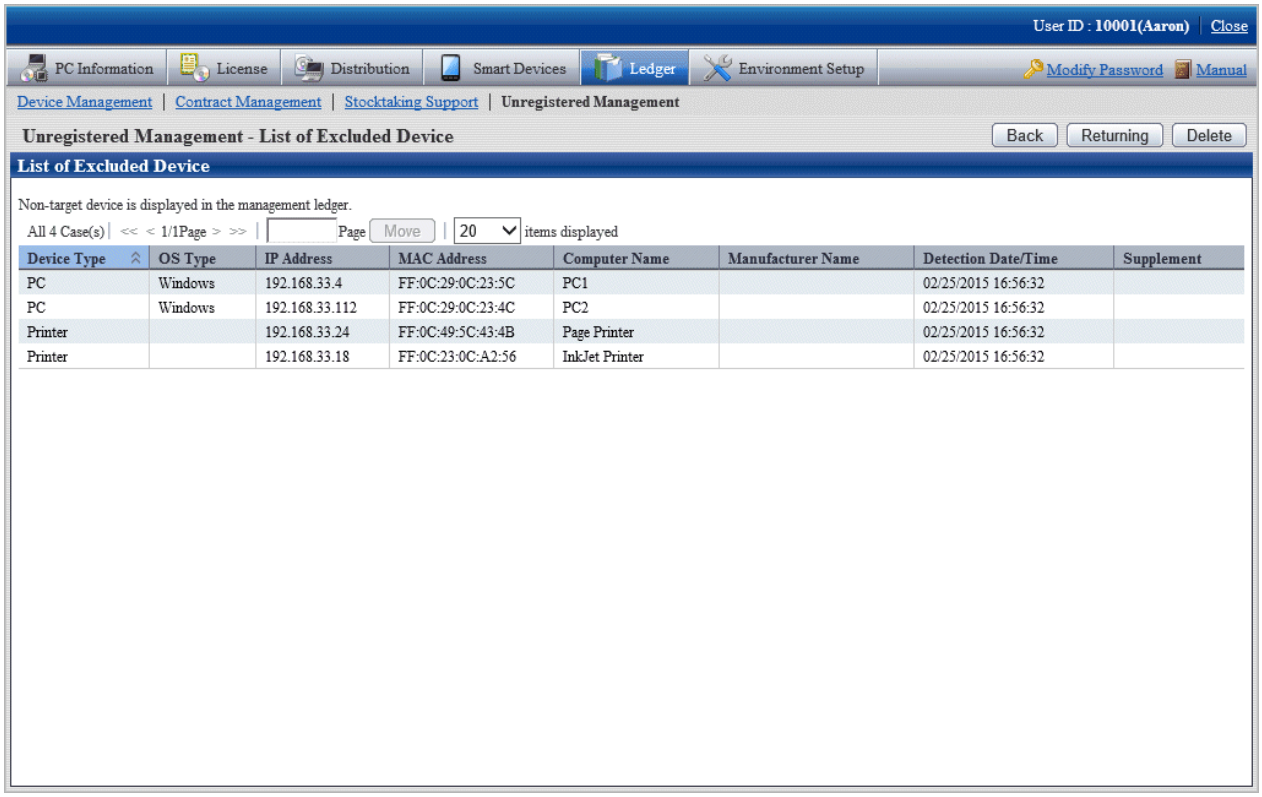
Confirm the excluded device list of the asset ledger.

Besides, the device which are not object can be restored as object and deleted from the list of non object.

The method for confirmation is as follows:

1. Click the **List of Excluded Device** button in the **Unregistered Management** window.

   The following window will be displayed



   - Independent from the user authority for displaying this window, information of device not to be registered will be displayed.
   - Device which have been registered to the asset ledger will not be displayed in this window.
   - Apart from the MAC address displayed here, the information will be updated when notifying the device information detected automatically through batch network check/ADT every time.

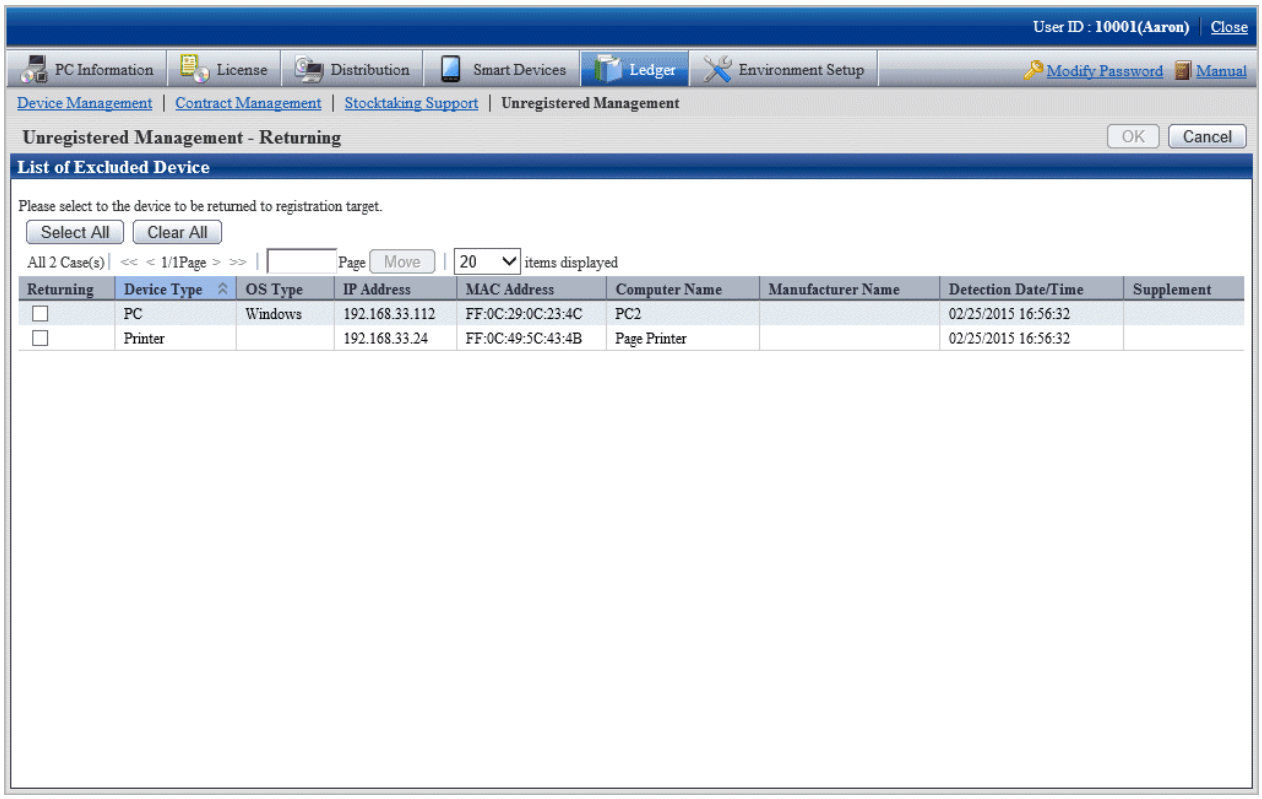
When restored as object

The device which are not the object can be restored as object.

1. Click the **Restoring** button in the **List of Excluded Device** window.

   The following window will be displayed

Only the device which can be restored as the object (device that can be detected) are displayed in the list.



2. Select the device to be restored as asset ledger registration object and click the **OK** button.

   The selected device is restored as registration object.

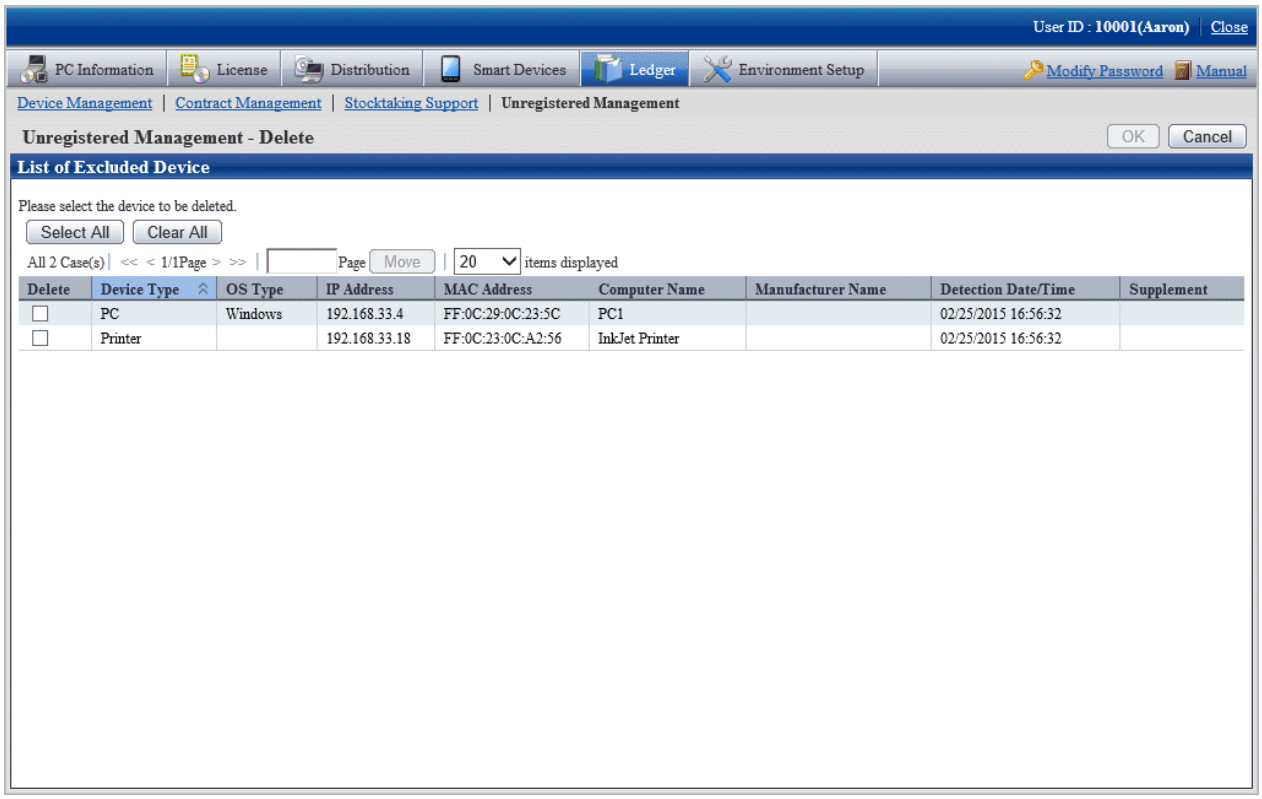
When deleted

Device which are not the object can be deleted.

1. Click the **Delete** button in the **List of Excluded Device** window.

   The following window will be displayed

Only the device which can be deleted (device which cannot be detected) are displayed in the list.



2. Select the device to be deleted and click the **OK** button.

   The selected device is deleted.

11.3 Device Management

This section describes how to manage the device information registered in the management ledger.

Point

IPv6 address information

PC information that contains IPv6 address information can also be managed by the management ledger.

11.3.1 Confirm/Delete Device Information

The method for confirming/deleting the registered device information is described according to the following operation procedure.

- "11.3.1.1 Confirm Various Device Information"
- "11.3.1.2 Confirm List of Device"
- "11.3.1.3 Confirm Device Details"
- "11.3.1.4 Confirm History Information"
- "11.3.1.5 Delete Device Information"

11.3.1.1 Confirm Various Device Information

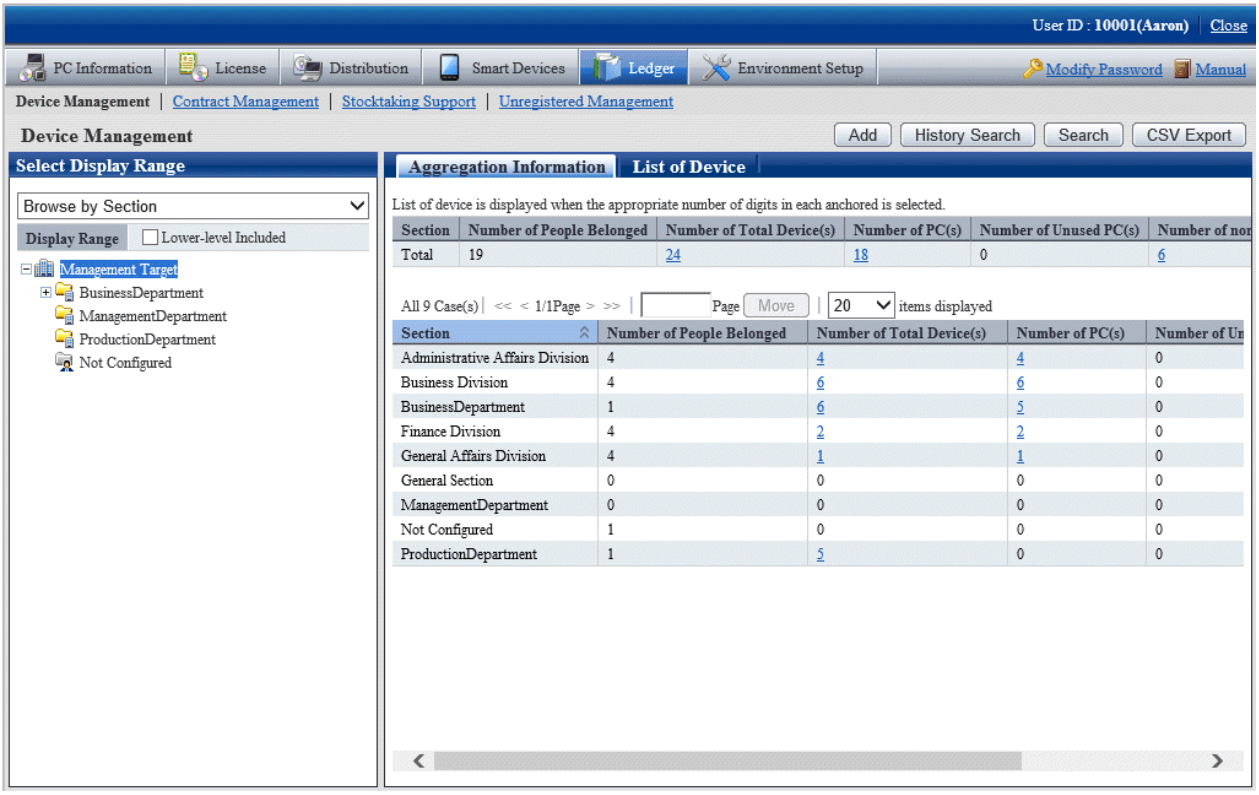
The procedure for confirming various device information of "By Section", "By Location" and "By Category":

1. Log onto the main menu, click **Ledger**.

   The **Ledger** window will be displayed

2. Click **Device Management**.

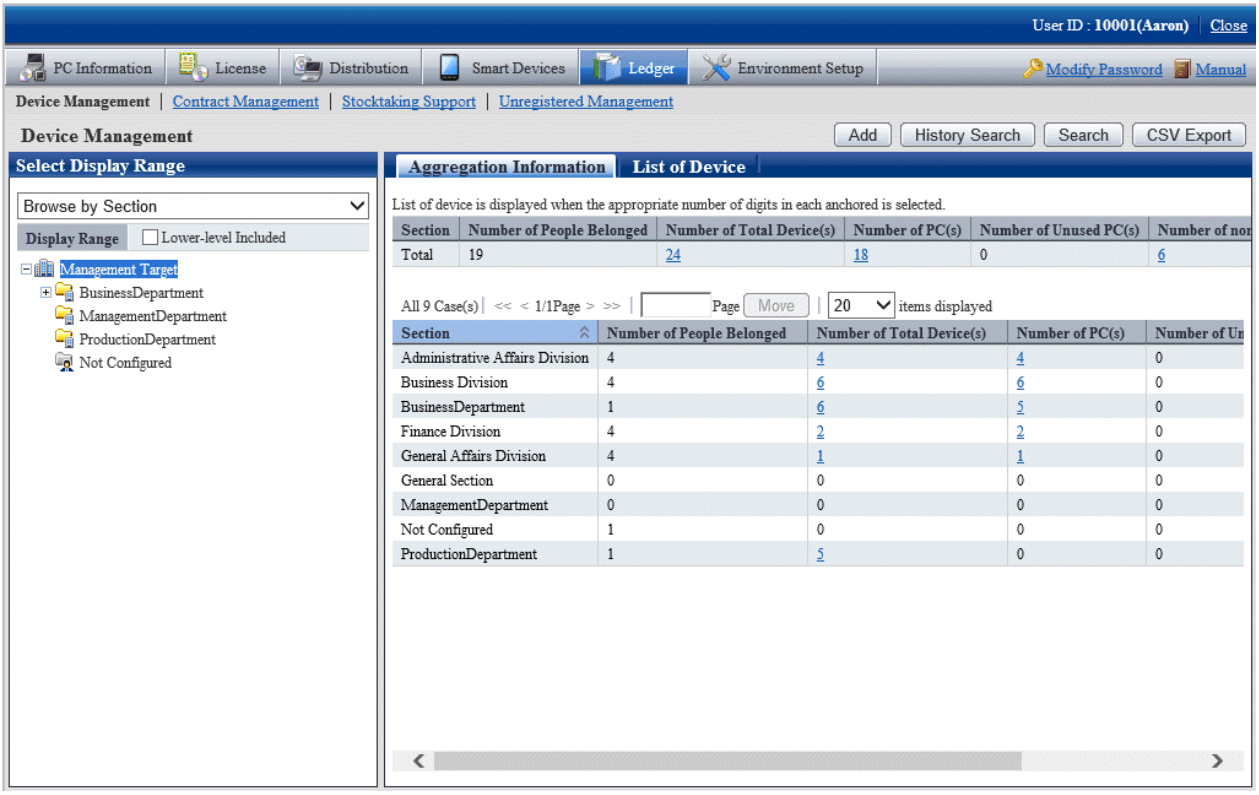
   The following window will be displayed



3. Confirm the device information by section.

   According to the drop-down menu on the left of the window, select **Browse by Section** from the list.

The following window will be displayed



The meaning of each item is as follows: besides, it describes the situation of all display item(s).

Item	Descriptions
Section	Section information.
Number of People Belonged	Number of users subordinate to the section.
Number of Total Device(s)	Total number of device managed in the section.
Number of PC(s)	Total Number of PC(s) managed in the section. The **Class** item registered as device information is the sum of **PC** values.
Number of Unused PC(s)	Total number of unused PC managed in each section. The **Availability** item registered as device information is the sum of values excluding **In Use**.
Number of non-PC(s)	Total Number of non-PC(s) managed in each section. The **Class** item registered as device information is the sum of values excluding "PC".

Besides, the function of each button is as follows:

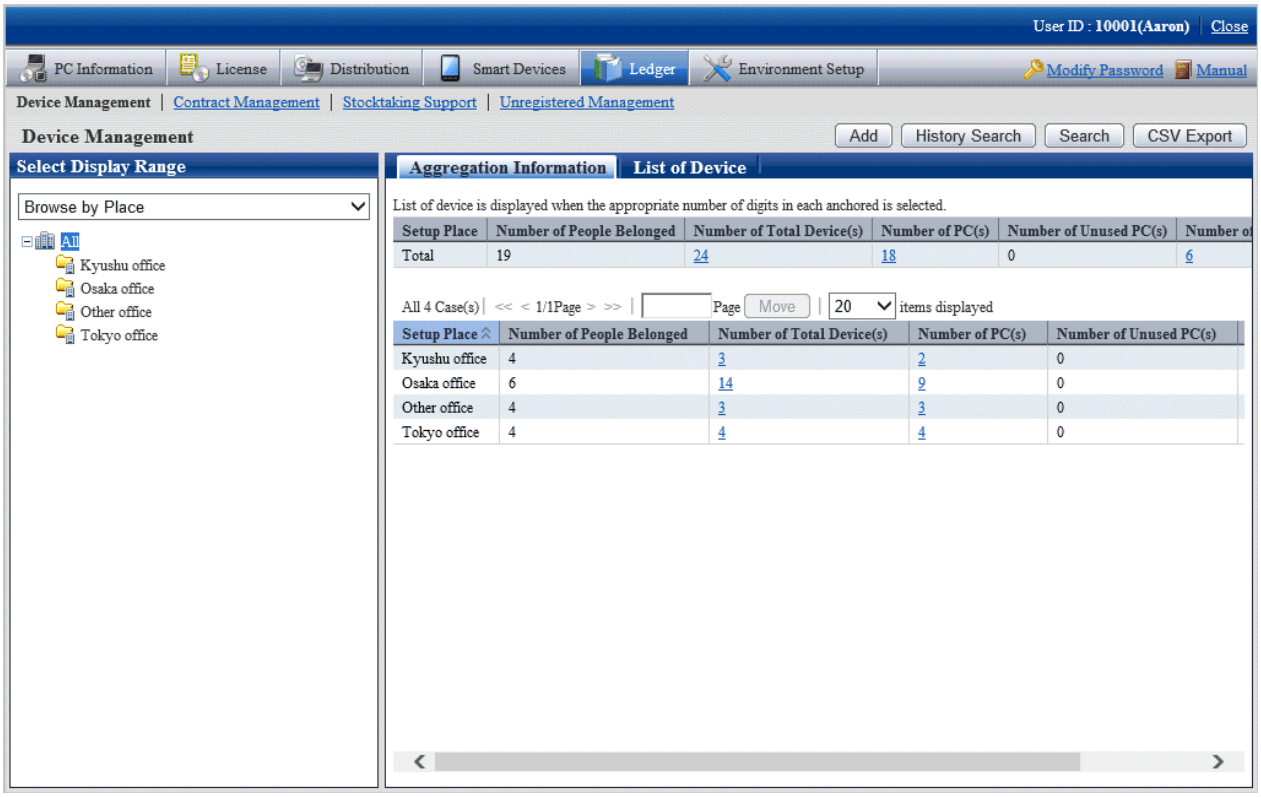
Item	Descriptions
Add	Register the device information. For details, refer to "11.3.2 Register/Modify Device Information".
History Search	Filter to display the history information. For details, refer to "11.3.1.4 Confirm History Information".

Item	Descriptions
Search	Filter to display the device displayed in the window. For details, refer to "Filter device".
CSV Export	Save the information displayed in the window as the ledger. For details, refer to "11.3.3 Save Device Information as Ledger".

4. Confirm the device information by location.

   According to the drop-down menu on the left of the window, select **Browse by Place** from the list.

   The following window will be displayed



The meaning of each item is as follows:

Besides, it describes the situation of all display item(s). And the action of the button is the same as the window of device confirmation by section described previously.

Item	Descriptions
Setup Place	The setting location of the machine.
Number of People Belonged	Number of users subordinate to the setting location.
Number of Total Device(s)	Total number of device managed in the setting location.
Number of PC(s)	Total Number of PC(s) managed in the setting location. The **Class** item registered as device information is the sum of **PC** values.
Number of Unused PC(s)	Total Number of Unused PC(s) managed in each setting location. The **Availability** item registered as device information is the sum of values excluding **In Use**.

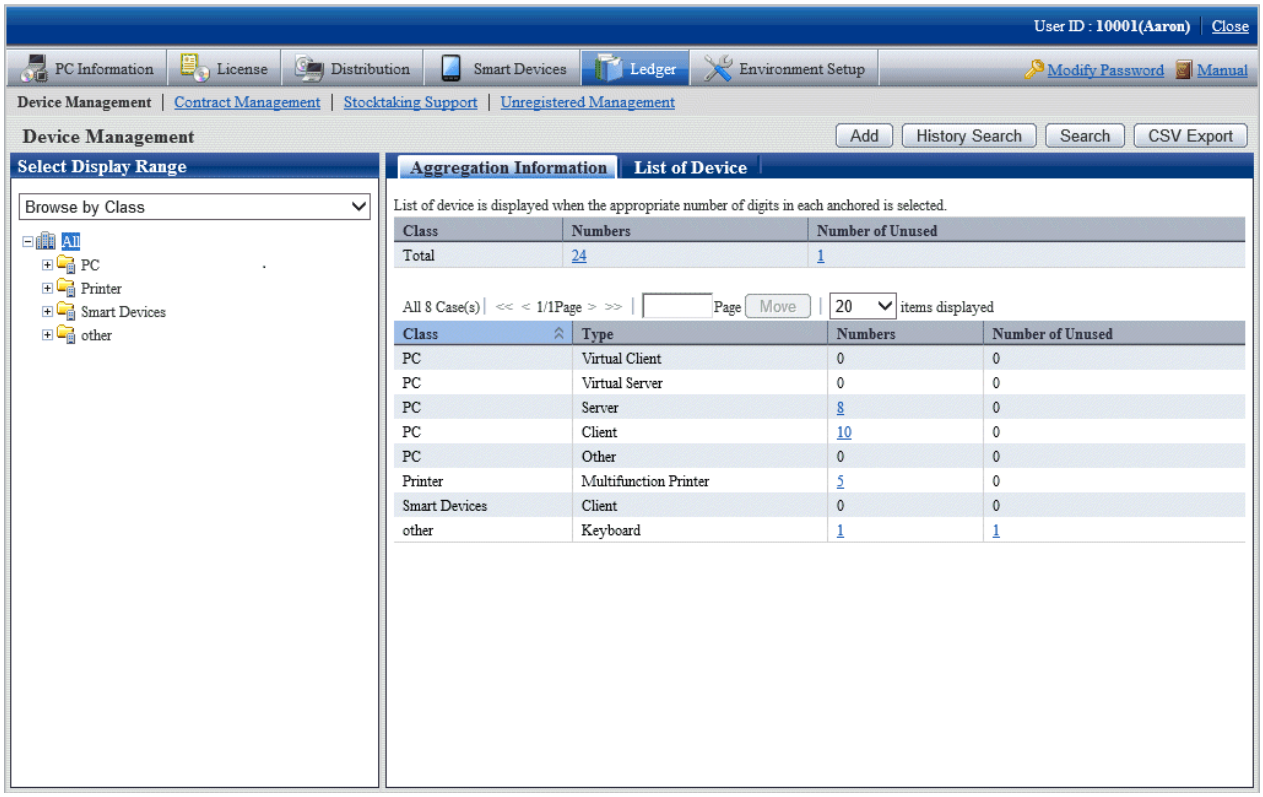
Item	Descriptions
Number of non-PC(s)	Total Number of non-PC(s) managed in each setting location. The **Class** item registered as device information is the sum of values excluding **PC**.

Remarks. When selecting the whole company, number of device with the setting location unset will be aggregated in the sum.

5. Confirm the device information by classification.

According to the drop-down menu on the left of the window, select **Browse by Class** from the list.

The following window will be displayed



The meaning of each item is as follows:

Besides, it describes the situation of all display item(s). Besides, the function of the button is the same as the window of device confirmation by section described previously.

Item	Descriptions
Class	Device classification information. The **Class** information registered as device information.
Type	Device category information. The **Type** information registered as device information.
Numbers	Total number of device managed in the classification and category unit. Sum of values of each **Class** and **Type** registered as device information.
Number of Unused	Total number of unused device managed in the classification and category unit. The **Usage Status** item registered as device information is the sum of values excluding **In Use**.

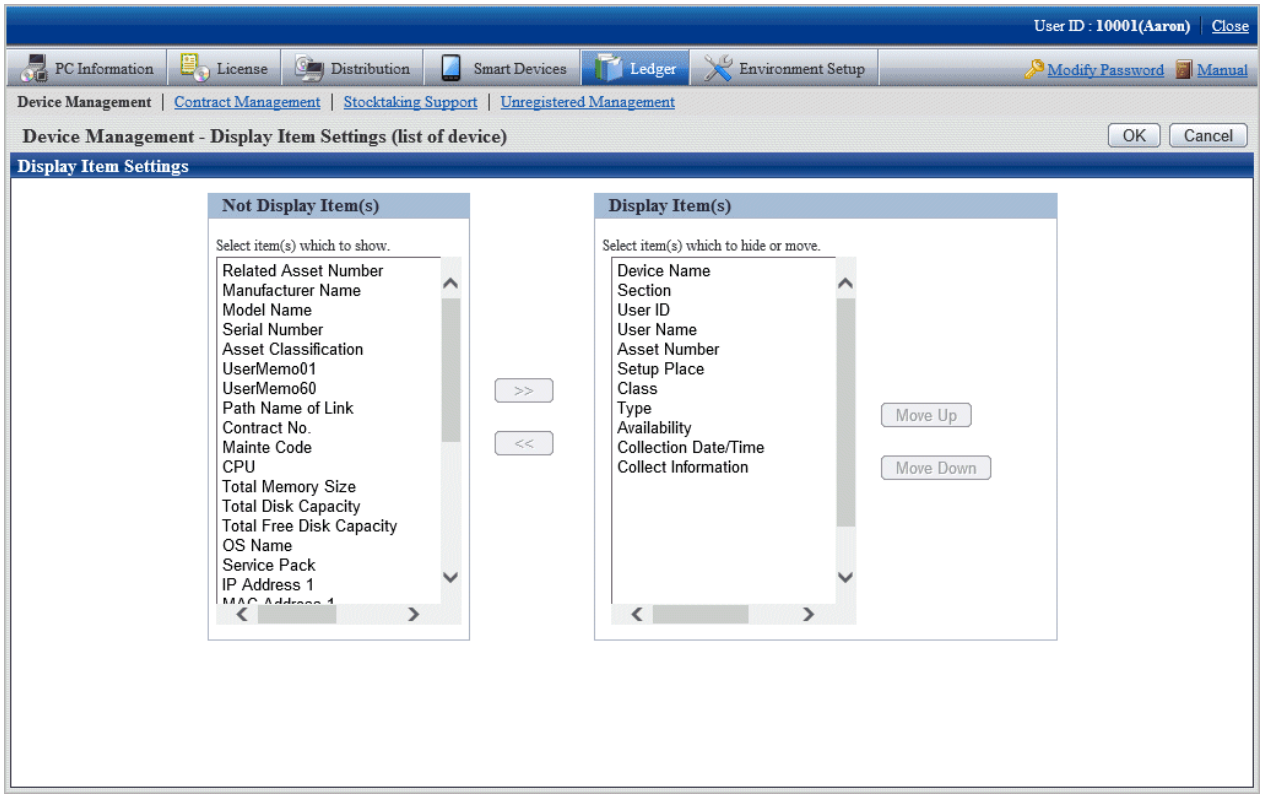
Set display item(s)

It describes how to set the items displayed in the window.

1. Click the **Displayed Item Settings** button.

   The following window will be displayed

   Besides, the window when clicking the **Displayed Item Settings** button in the following window of device confirmation by section will be displayed.



2. Set the display item(s) according to the following procedure.

   a. Select items displayed in the device list from the **Not Display Item(s)** list on the left side of the window and click the >> button in the center of the window. Multiple items can be selected.

      The selected items are added to **Display Item(s)** on the right side of the window.

   b. Select items not displayed in the device list from the **Display Item(s)** on the right side of the window, and click the << button in the center of the window. Multiple items can be selected.

      The selected items are deleted from **Display Item(s)** on the right side of the window.

   c. When modifying the order of **Display Item(s)**, select items from the **Display Item(s)** list on the right side of the window and click the **Move Up** or **Move Down** button.

3. After completing the setting of display item(s), click the **OK** button.

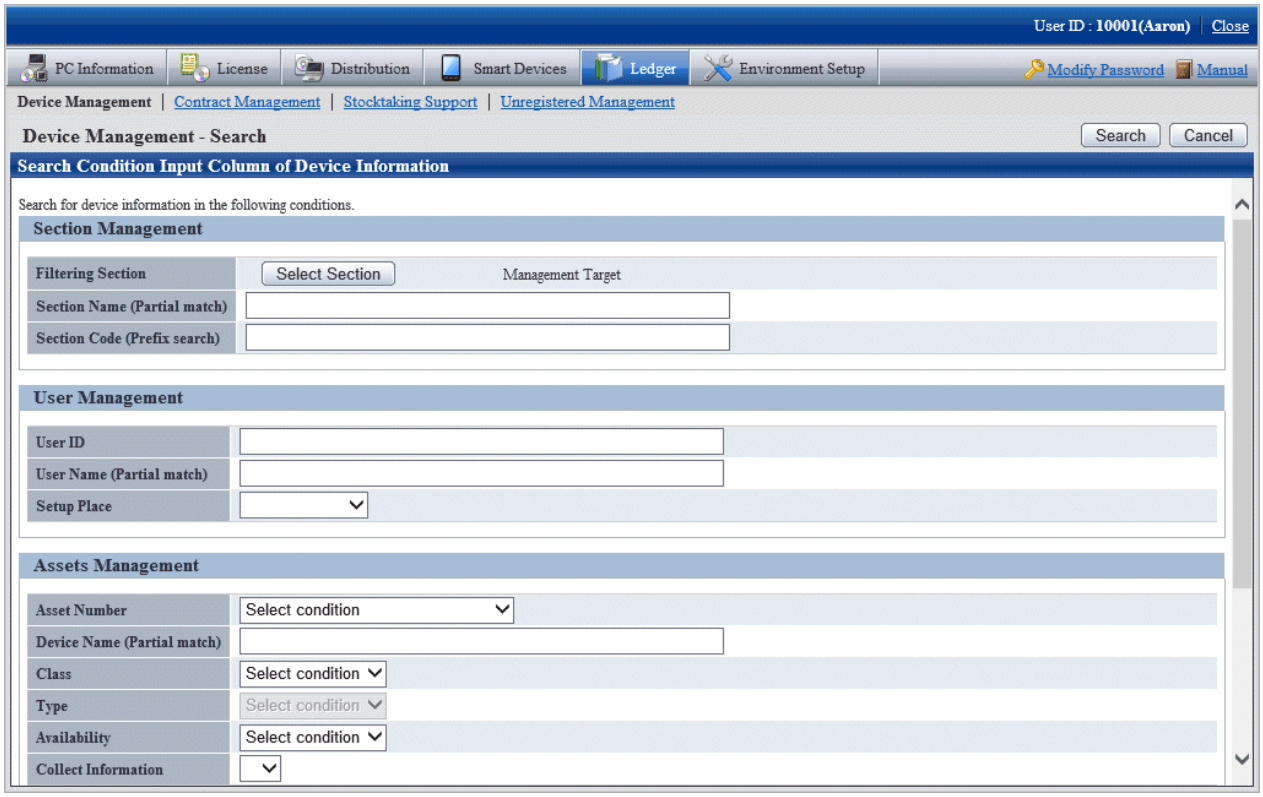
   The display item(s) of list of device are added to the set items.

Filter device

It describes how to filter the device displayed in the window.

1. Click the **Search** button.

   The following window will be displayed



2. Set filtering aggregation.

   Set the following information and click the **Search** button.

Item		Descriptions
Section Management	**Filtering Section**	Set conditions when filtering by section.
	Section Name	Set conditions when filtering by section name.
	Section Code	Set conditions when filtering by section code.
User Management	**User ID**	Set conditions when filtering by user ID.
	User Name	Set conditions when filtering by user name.
	Setup Place	Set conditions when filtering by setting location.
Assets Management	**Asset Number**	Set conditions when filtering by asset number. Set filtering conditions through the list on the left side. - **Partial match Search** Set when searching asset number by partial match - **Search the device that is not input.** Set when searching asset number as device which have not been input
	Device Name	Set conditions when filtering by device name.
	Class	Set conditions when filtering by classification. Set the filtering conditions through the list on the left side. - **Match**

Item		Descriptions
		Set when searching the device matching the classification selected from the list on the right side. - **Not Match** Set when searching the device not matching the classification selected from the list on the right side.
	Type	Set conditions when filtering by category. Set the filtering conditions through the list on the left side. - **Match** Set when searching the device matching the category selected from the list on the right side. - **Not Match** Set when searching the device not matching the category selected from the list on the right side.
	Availability	Set conditions when filtering by Usage Status. Set the filtering conditions through the list on the left side. - **Match** Set when searching the device matching the Usage Status selected from the list on the right side. - **Not Match** Set when searching the device not matching the Usage Status selected from the list on the right side.
	Collect Information	Set conditions when filtering according to whether PC Inventory information exists. Set **o** when searching a PC with Inventory information, set **x** when searching a PC without Inventory information.
PC Spec	**Match with all conditions** or **Match with some conditions**	For conditions set in the **PC Specification** bar, select **All Conditions Match** with all containing multiple conditions or **Any Condition Match** containing 1 or more conditions.
	CPU Clock Speed	Set conditions when filtering by CPU Clock Speed. Including the decimal point, 6 single-byte numbers at most can be set.
	Total Memory Size	Set conditions when filtering by total free disk capacity. Including the decimal point, 6 single-byte numbers at most can be set.
	Total Disk Capacity	Set conditions when filtering by total disk capacity. Including the decimal point, 6 single-byte numbers at most can be set.
	Total Free Disk Capacity	Set conditions when filtering by total free disk capacity. Including the decimal point, 6 single-byte numbers at most can be set.

Only the items matching the search will be displayed in the window.

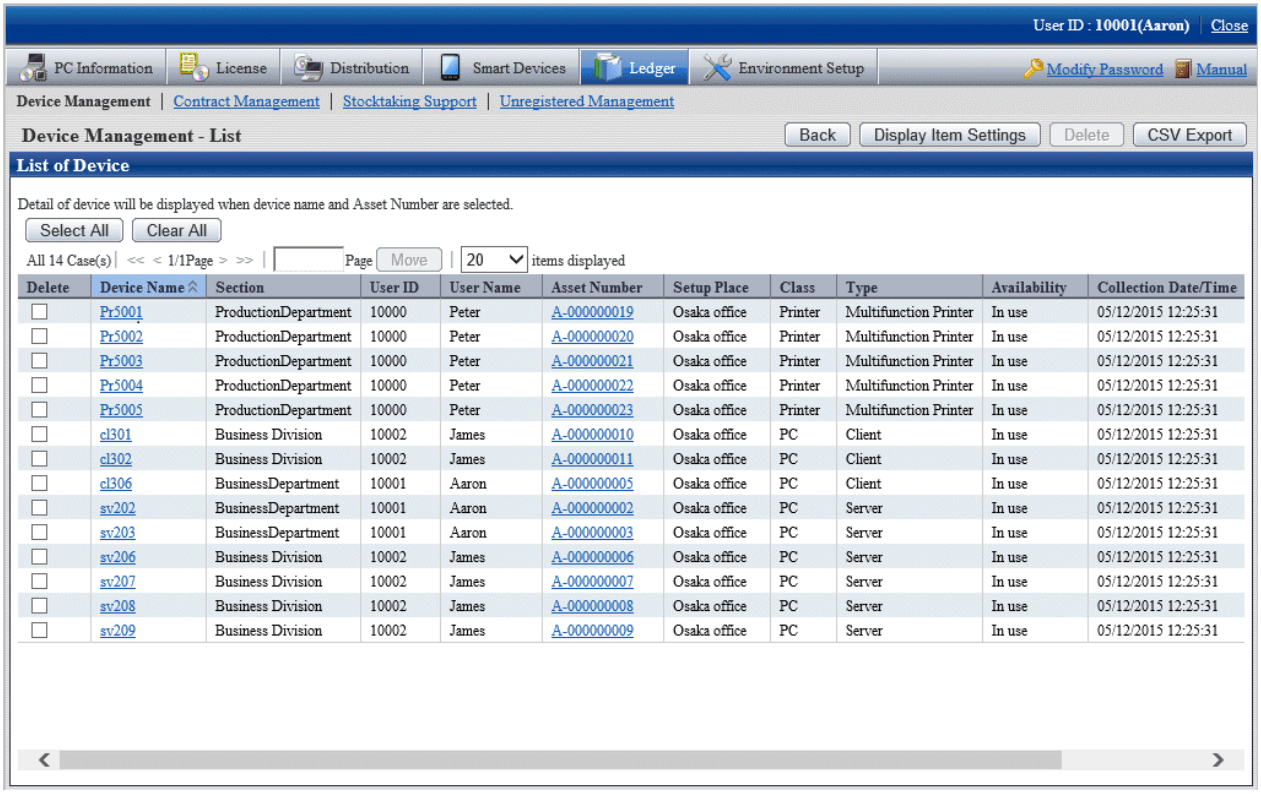
11.3.1.2 Confirm List of Device

The procedure for confirming list of various device of "In Section", "In Classification" and "In Location" are as follows:

Besides, the procedure will be followed "11.3.1.1 Confirm Various Device Information". The following is described according to the window of "In Section". The order of the display item(s) of "In Classification" is different from that of "In Location", but they can be confirmed according to the same procedure.

1. Click the values of items to be confirmed (**Number of Total Device(s)**, **Number of PC(s)**, **Number of Unused PC(s)** and **Number of non-PC(s)**).

   The following window will be displayed



2. Confirm the device list of the selected items.

   Confirm the following information.

   It describes the situation of all display item(s).

Item	Descriptions
Section	Section information.
User ID	User ID of the user who uses the machine. The **User ID** information registered as device information.
User Name	Name of the user who uses the machine.
Asset Number	Asset management number of the machine. The **Assets Management No.** information registered as device information.
Related Asset Number	Related asset number of the machine. The **Related Assets Management No.** registered as device information.
Setup Place	Device setting location information.

Item	Descriptions
Class	Device classification information. The **Class** information registered as device information.
Type	Device category information. The **Type** information registered as device information.
Availability	Device Usage Status. The **Usage status** information registered as device information.
Device Name	Name of the machine. The **Device Name** information registered as device information.
Manufacturer Name	Device manufacturer name. The **Manufacturer Name** information registered as device information.
Model Name	Device Model Name. The **Model Name** information registered as device information.
Serial Number	Device serial number. The **Serial Number** information registered as device information.
Asset Classification	Device asset classification. The **Asset Classification** information registered as device information.
User Memo 1~60	Device inherent information . The **User Memo 1~60** information registered as device information.
Path Name of Link	Data related to the device (example: device image) or these input directory and URL. The **Path Name of Linkage Target** information registered as device information.
Contract No.	Contract number information. The **Contract No.** information registered as device information.
Maintenance Code	Device maintenance code. The **Maintenance Code** registered as device information.
CPU	CPU Clock Speed of PC.
Total Memory Size	Total memory capacity of PC.
Total Disk Capacity	Total hard disk capacity of PC.
Total Free Disk Capacity	Available hard disk capacity of PC.
OS Name	OS name of PC.
Service Pack	Service Pack applied in PC.
IP Address 1	IP address set in PC. - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/). - IPv6 addresses are separated with a semicolon (;).
IP Address 2	IP address set in PC. - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/).

Item	Descriptions
	- IPv6 addresses are separated with a semicolon (;).
MAC Address 1	MAC address set in PC.
MAC Address 2	MAC address set in PC.
Date of Manufacture	Device date of manufacture.
Date of Registration	Date for registering to the device asset ledger.
Collection Date/Time	Date and time for collecting information.
Collect Information	Indicate whether PC Inventory information exists. **o** indicates PC Inventory information exists, while **x** indicates PC Inventory information does not exist. The Inventory information has been deleted manually, it is still displayed as **x**.
User Definition Inherent Item	As Inventory information, it is the user memo set by the user arbitrarily. The user is displayed as the set item and user memo. For example, after the user has set **Asset Number**, **Asset Number** will be displayed.

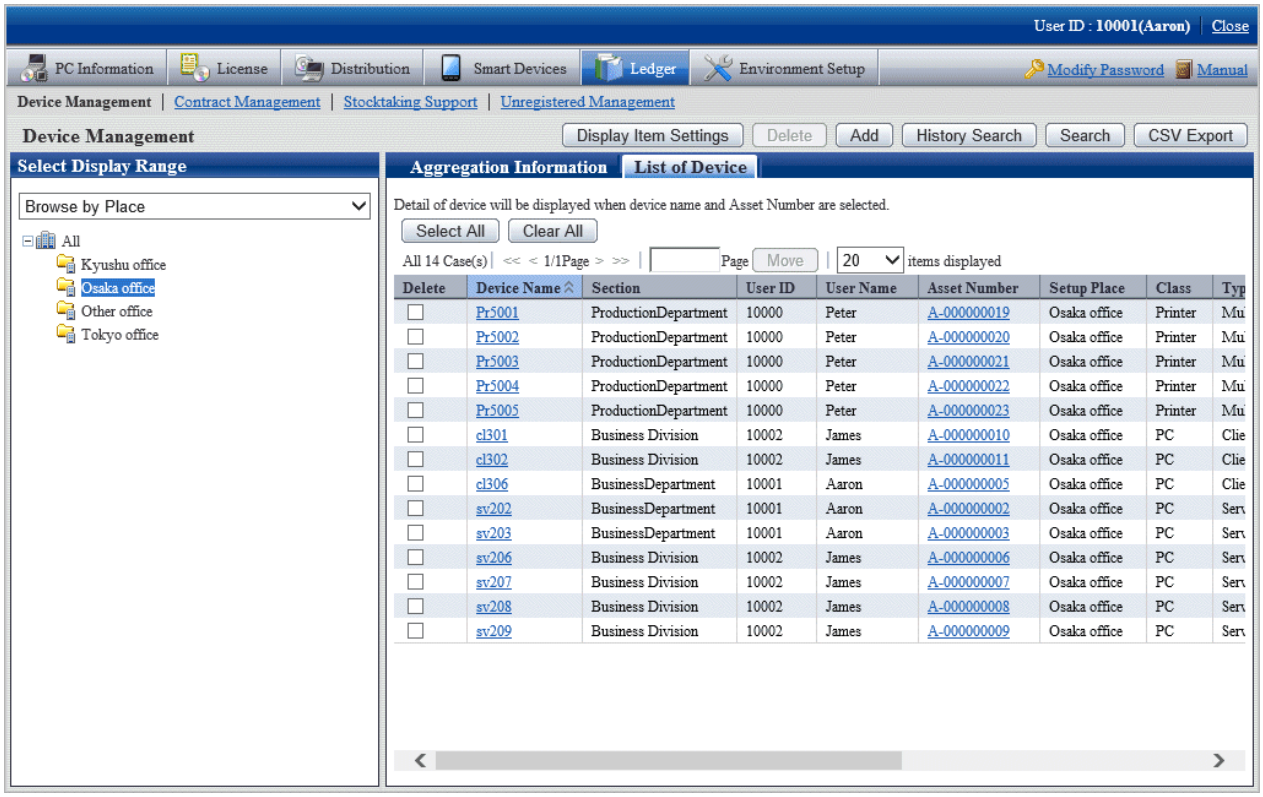
Besides, the function of each button is as follows:

Item	Descriptions
Back	Display the previous window.
Display Item Settings	Set the items displayed in the window. For details, refer to "Set display item(s)".
Delete	Delete the device information. For details, refer to "11.3.1.5 Delete Device Information".
CSV Export	Save the information displayed in the window as the ledger. For details, refer to "11.3.3 Save Device Information as Ledger".

Besides, the list of device can also be confirmed according to the following procedure. Operate when confirming in the unit of section.

1. Click the **List of Device** tab.

   The following window will be displayed



2. Confirm the device list of the selected items.

11.3.1.3 Confirm Device Details

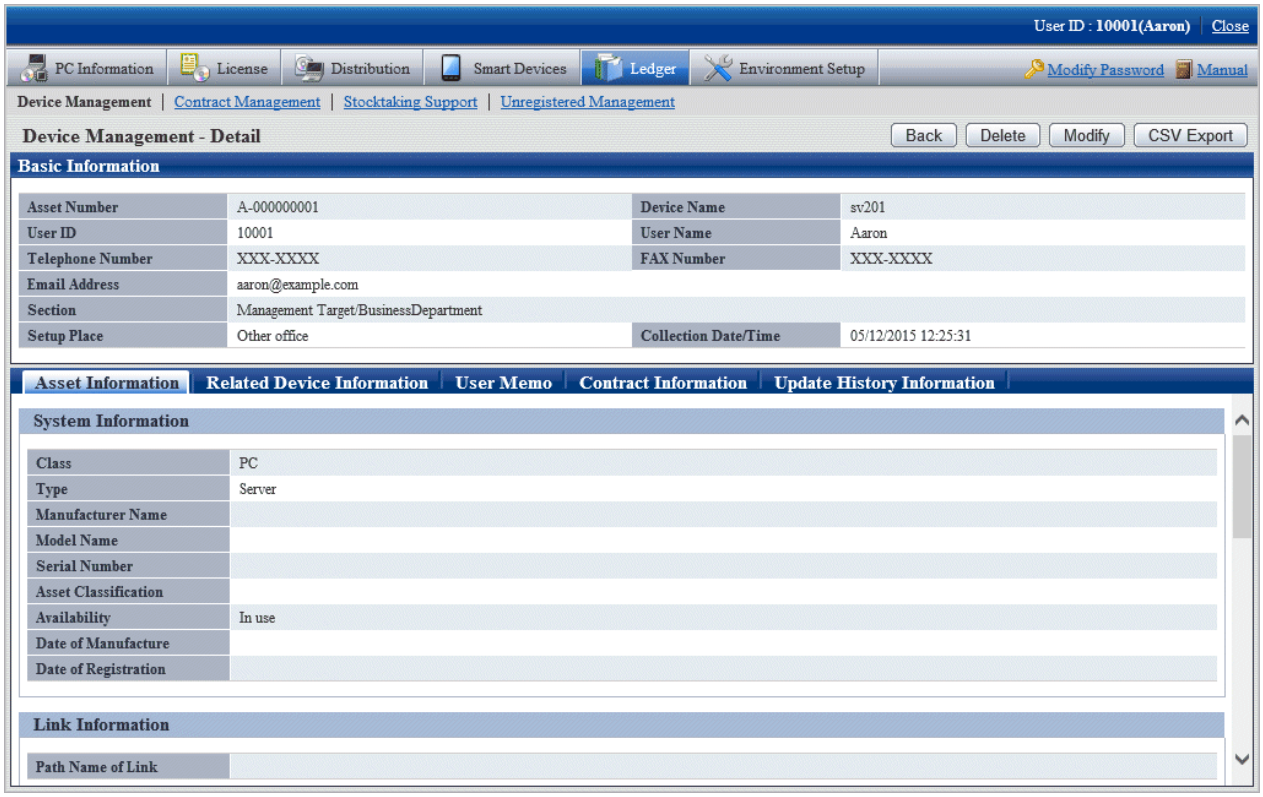
The procedure for confirming the device details are as follows.

Besides, the unnecessary device information can be deleted during confirmation.

Or the procedure is followed "11.3.1.2 Confirm List of Device", "11.3.1.4 Confirm History Information", "11.4.1.3 Confirm Details of Contract", "11.5.1.2 Confirm List of Stocktaking".

1. Click the asset number of device to be confirmed.

   The following window will be displayed



   The function of each button is as follows:

Item	Descriptions
Back	Display the previous window.
Delete	Delete the device information. For details, refer to "11.3.1.5 Delete Device Information".
Modify	Modify the device information. For details, refer to "11.3.2 Register/Modify Device Information".
Modify Comment	This button is displayed only in case the **Update History Information** tab is selected. Set the **Annotation** for update history. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. Besides, when the annotation has been set for the update history modified multiple items by one operation, annotation will be set for all update history of this operation.
PC Information	Display PC information window. Device with Inventory information are displayed only through this button.
CSV Export	Save the information displayed in the window as ledger. For details, refer to "11.3.3 Save Device Information as Ledger".

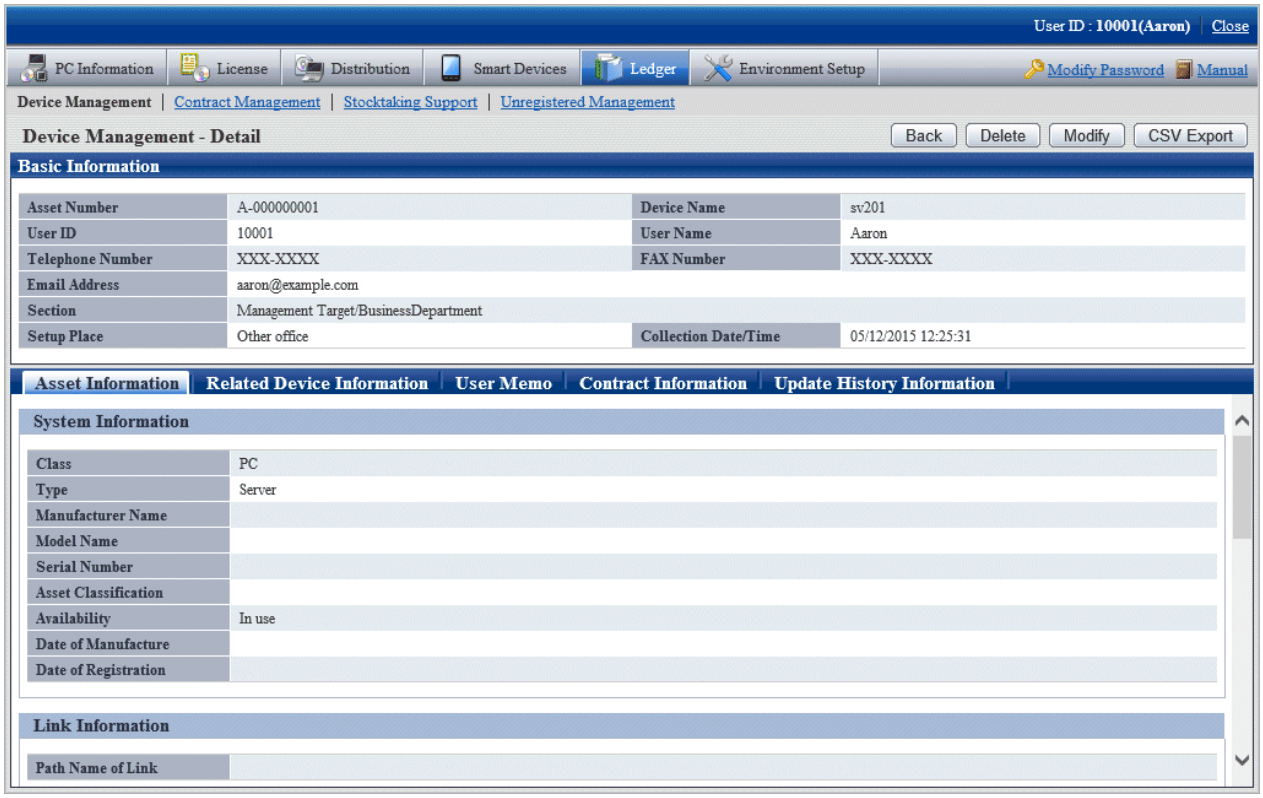
2. Confirm the device details of selected items.

   Besides, when **Setup Place** meets the following 2 conditions at the same time, **Supplemental Setup Place** set in the segment management window will be enclosed by brackets.

   - Conditions for display: device which has been set IP address and whose setting location has been confirmed through IP address and the setting location matches.
   - Example of display: Shikoku Branch Office (8F South)

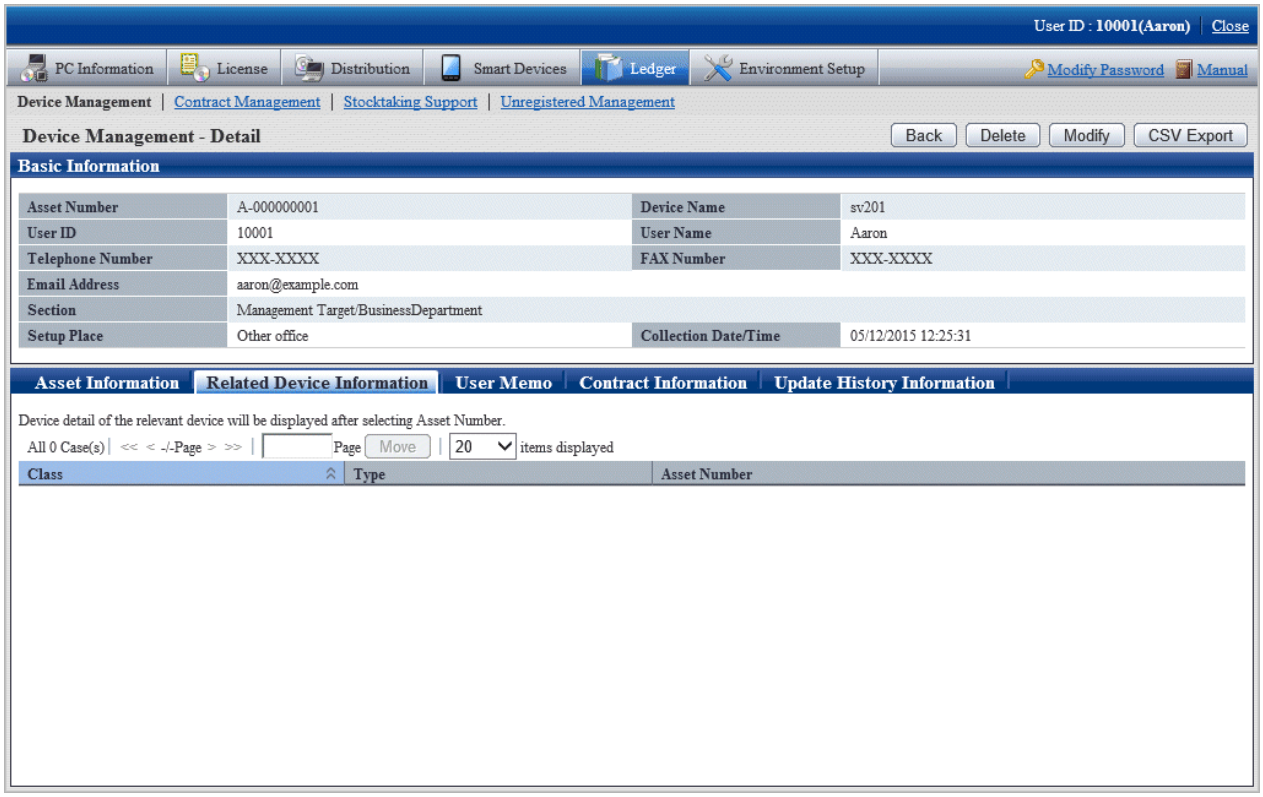
3. When selecting the **Asset Information** tab

   The asset information is displayed. Main-body Information and network information of the device can be viewed.



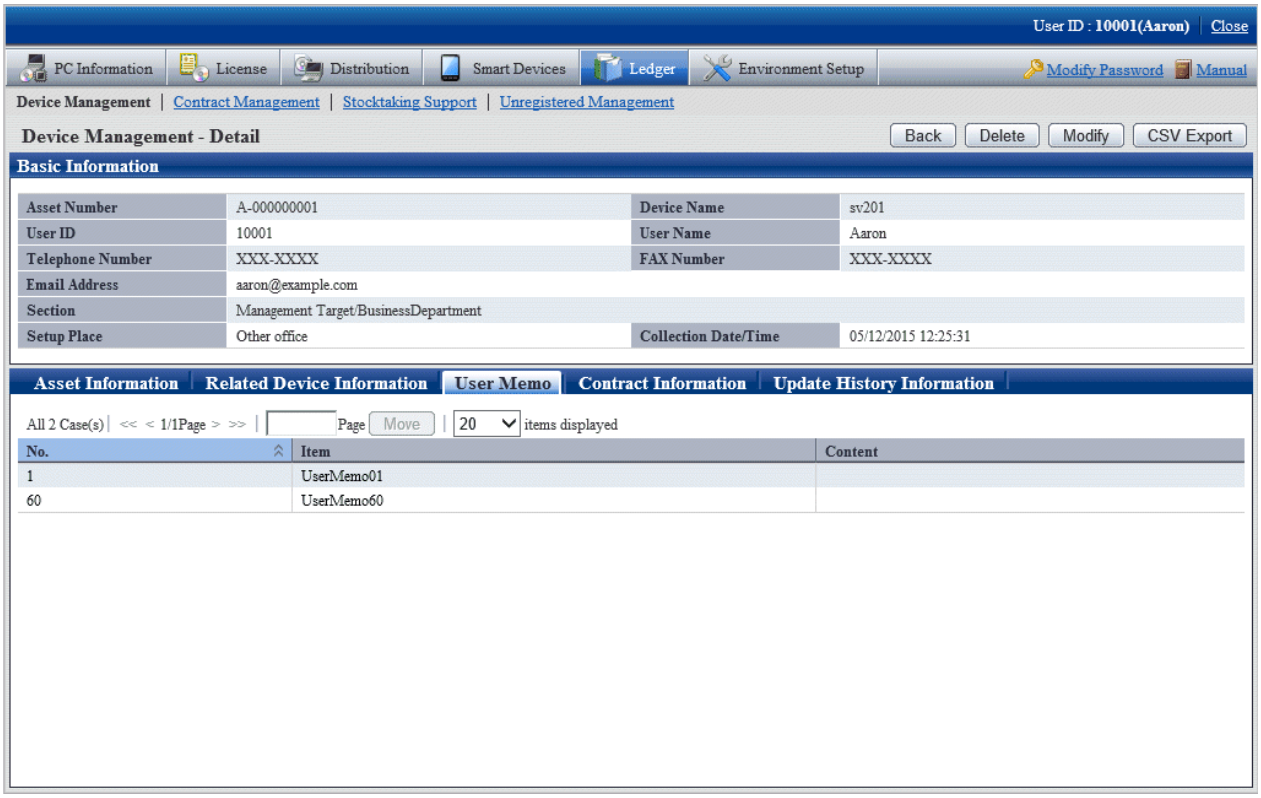
4. When selecting the **Related Device Information** tab

   The related device information is displayed. Device list information related to the organization can be viewed.



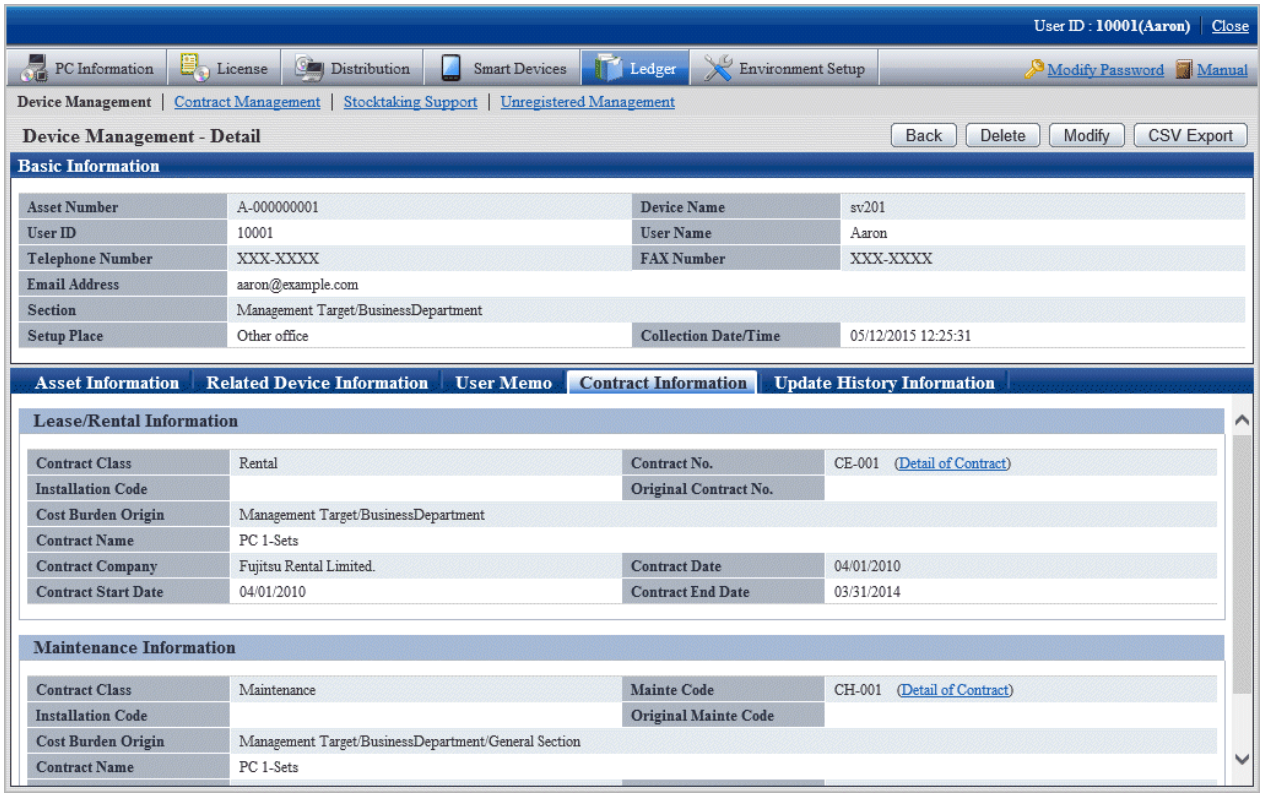
5. When selecting the **User Memo** tab

   The user memo is displayed. **User Memo 1~60** registered as device information can be viewed.



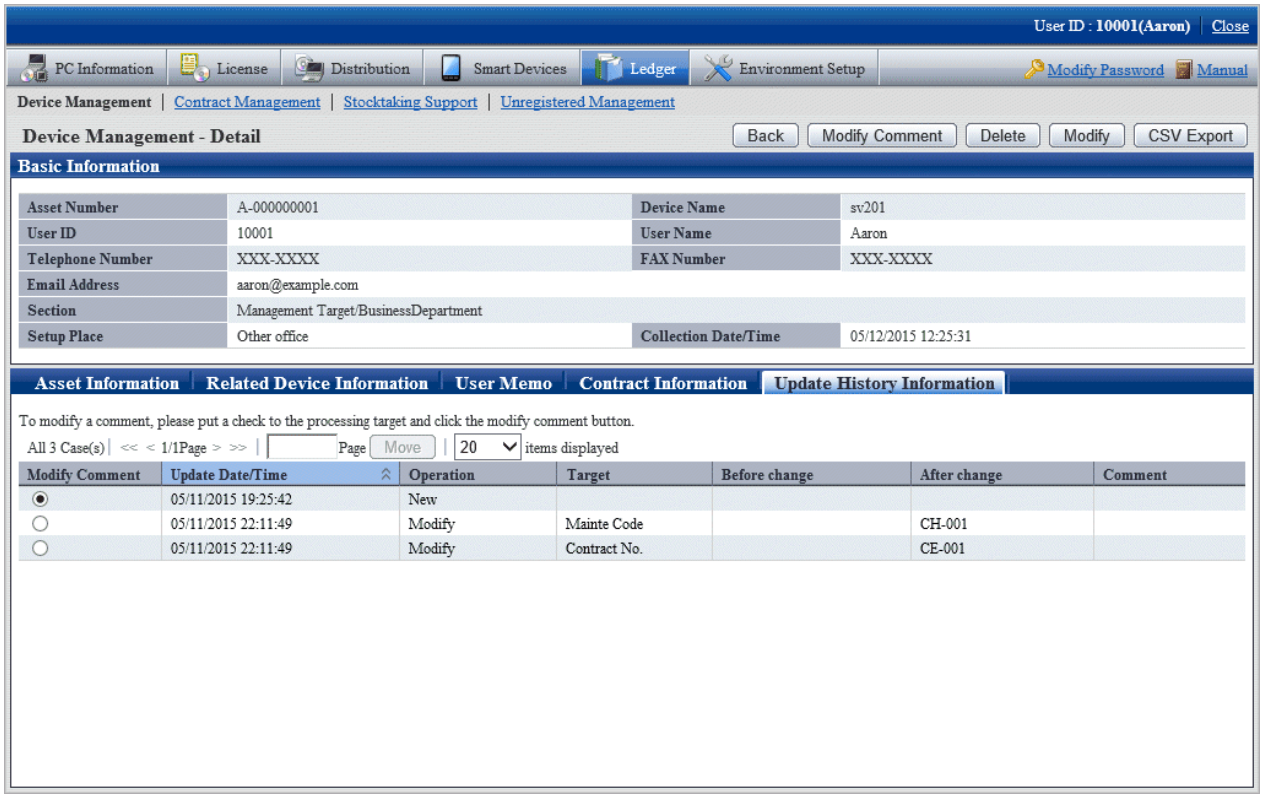
6. When selecting the **Contract Information** tab

   The contract information is displayed. The contract information distributed in the device can be viewed.



7. When selecting the **Update History Information** tab

   The update history information is displayed. The update history information of the device can be viewed.



11.3.1.4 Confirm History Information

When confirming the update history of the device information, through the filter specified according to the range of the unit and modification date of asset information/device information/contract information, extract the correspondent device list.

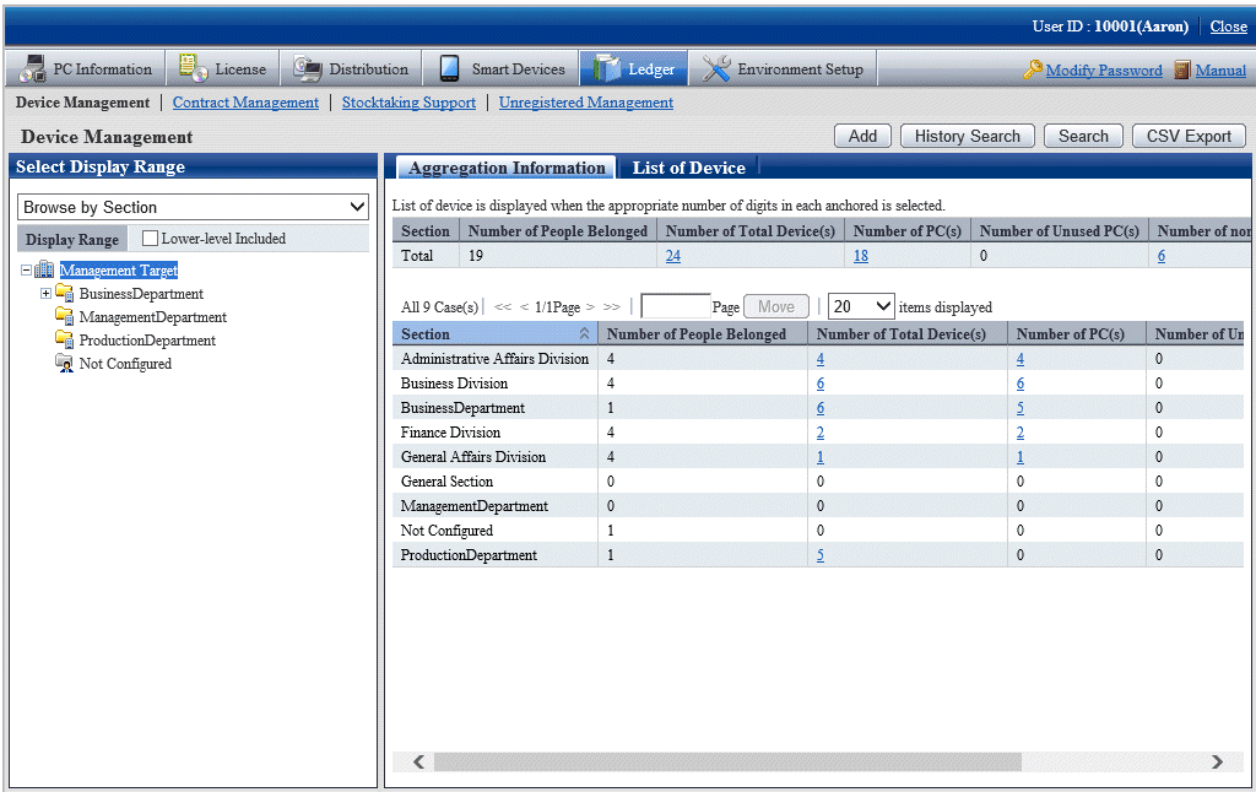
Confirm the device list by filtering update history

1. Log onto the main menu and click **Ledger**.

   The **Ledger** window will be displayed

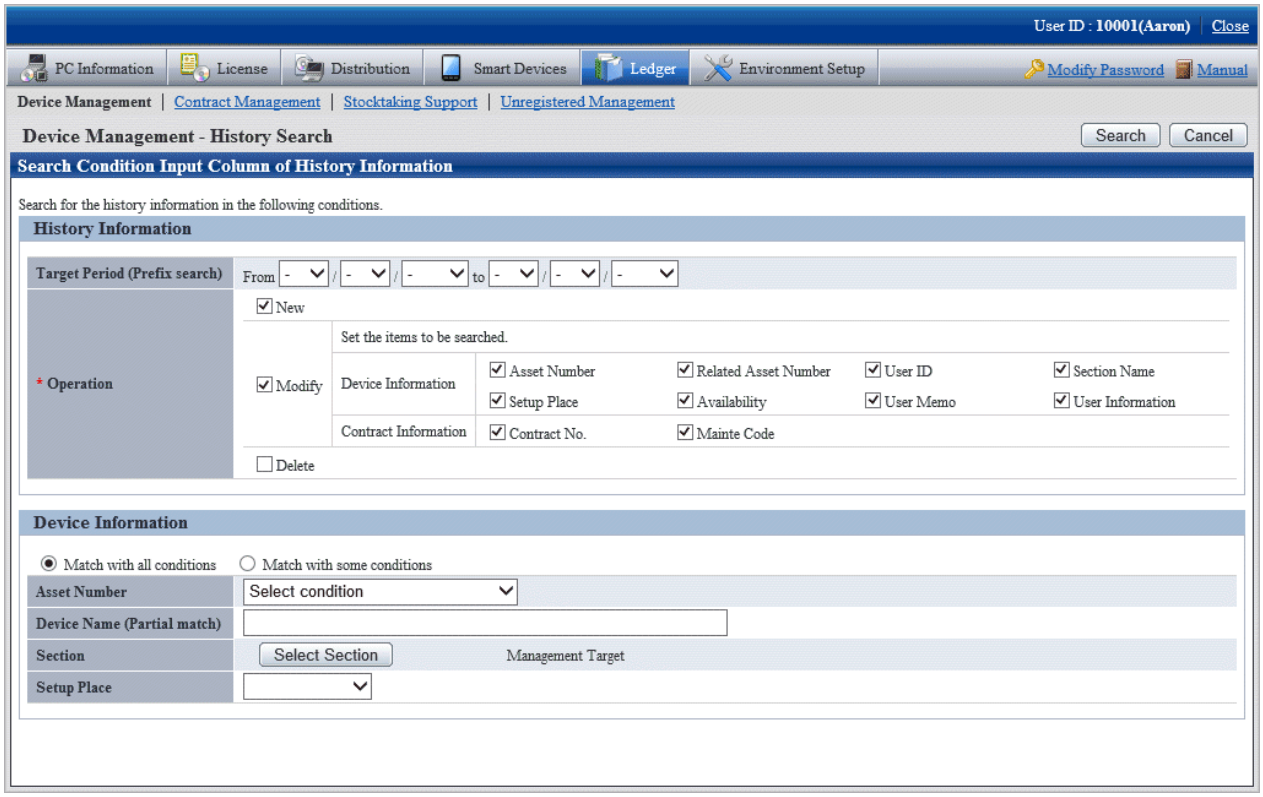
2. Click **Device Management**.

   The following window will be displayed



3. Click the **History Search** button.

   The following window will be displayed



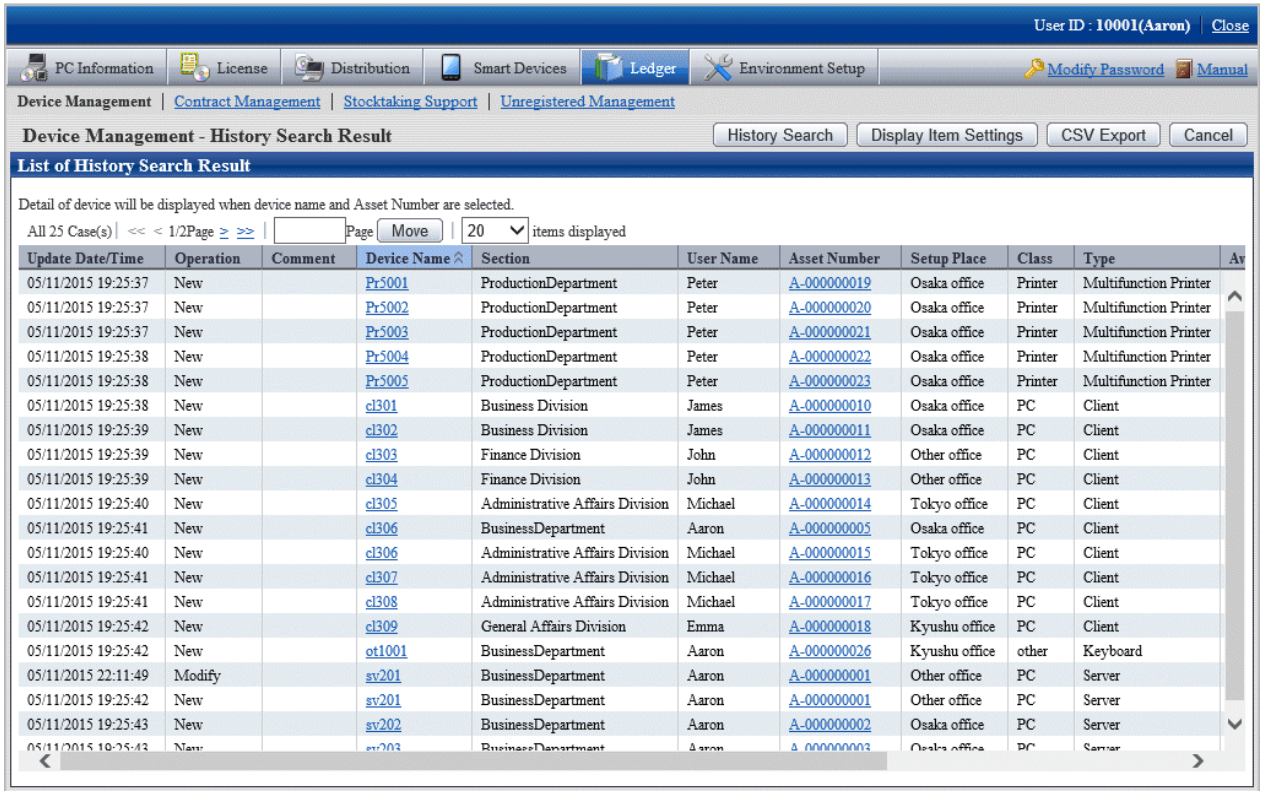
4. Set the following filtering conditions and click the **Search** button.

Item		Descriptions
History Information	**Target Period**	Selected when filtering through the object period with device information modified.
	New	Selected when the new added operation history is contained in the filtering object.
	Modify	Selected when the modified operation history is contained in the filtering object. Or select whether to search the modification of a certain item through **Asset Number** on the right side, etc.
	Delete	Selected when the deleted operation history is contained in the filtering object.
Device Information	**Match with all conditions** or **Match with some conditions**	For conditions set in the **Device Information** bar, select **All Conditions Match** with all containing multiple conditions or **Any Condition Match** containing 1 or more conditions.
	Asset Number	Set conditions when filtering by asset number. Set the filtering conditions through the list on the left side. - **Partial match Search** Set when searching the asset number by partial match - **Search the device that is not input**
	Device Name	Set conditions when filtering by device name.
	Section	Set conditions when filtering by section.

Item		Descriptions
	Setup Place	Set conditions when filtering by setting location.

The filtering items specified in the device information (asset number, section, etc.) filter the current device status.

The **Device Management - History Search Result** window will be displayed



5. Confirm the following information.

   It describes the situation of all display item(s).

Item	Descriptions
Update Date/Time	Date and time for update.
Operation	Operation to the device information. Any of the following is displayed. - **New** - **Modify** - **Delete**
Comment	Annotation for device information modification history. When registering/modifying/deleting the device information in **Annotation**, the annotation set automatically or set by the user will be displayed. In the following operations, the annotation will be set automatically. - Modify PC adding/PC information through automatic reflection The annotation is changed to "Automatic Synchronization". - Access the setting location through inventory result - Register or remove distribute through the **Contract Information Distribution** window The annotation is changed to "Modify through Contract Information Distribution".
Section	Section information.

Item	Descriptions
User ID	The user ID of the user who uses the machine. The **User ID** information registered as device information.
User Name	Name of the user who uses the machine.
Asset Number	Asset management number of the machine. The **Asset Management No.** information registered as device information.
Related Asset Number	Related asset number of the machine. The **Related Assets Management No.** information registered as device information. Not displayed in the deleted machine.
Setup Place	Device setting location information.
Class	Device classification information. The **Class** information registered as device information.
Type	Device category information. The **Type** information registered as device information.
Availability	Device Usage Status. The **Usage Status** information registered as device information. The deleted device will be displayed as **Deleted**. Device deleted by sequencing according to **Usage Status** only can be extracted.
Device Name	Name of the machine. The **Device Name** information registered as device information.
User Memo 1~60	Device inherent information . The **User Memo 1~60** information registered as device information. Not displayed in the deleted machine.
Contract No.	Contract number information. The **Contract No.** information registered as device information.
Maintenance Code	Device maintenance code. The **Maintenance Code** registered as device information.
Collection Date/ Time	Date and time for collecting information. Not displayed in the deleted machine.
Collect Information	Indicate whether PC Inventory information exists. **o** indicates PC Inventory exists, while **x** indicates PC Inventory information does not exist. Not displayed in the deleted machine.
User Definition Inherent Items	As Inventory information, it is the user memo set by the user arbitrarily. The user is displayed as the set item and inherent information. For example, after the user has set **Asset Number**, **Asset Number** will be displayed. Not displayed in the deleted machine.

Besides, the action of each button is as follows:

Item	Descriptions
History Search	Filter to display the device displayed in the window.

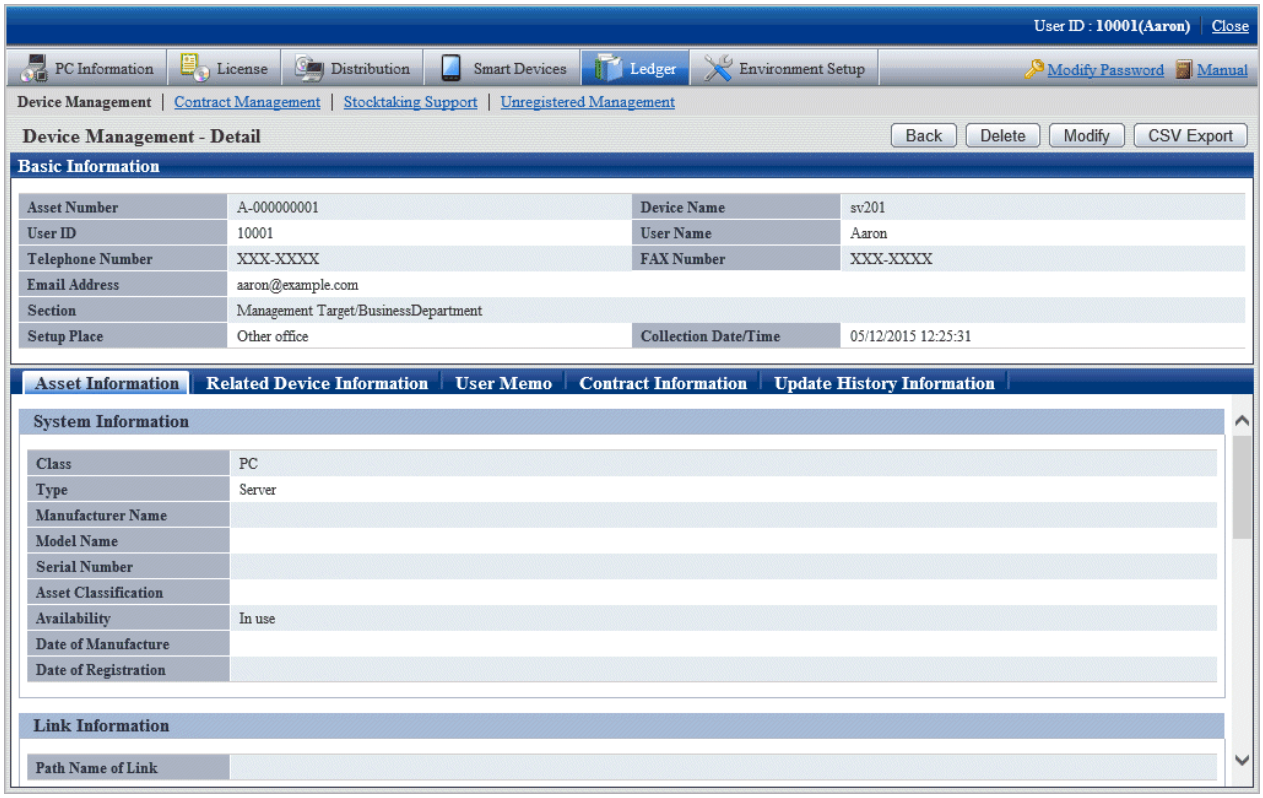
Item	Descriptions
Display Item Settings	Set the items displayed in the window. For details, refer to "Set display item(s)".
CSV Export	Save the information displayed in the window as the ledger. For details, refer to "11.3.3 Save Device Information as Ledger".
Cancel	Display **Management Target**.

The list of device output from the **Device Management - History Search Result** window is output in one line per operation. Even if multiple items are modified in one operation, one line of result will be displayed.

6. When other application and so on are using history filtering result, click the **CSV Export** button, files in Excel/CSV format are output.

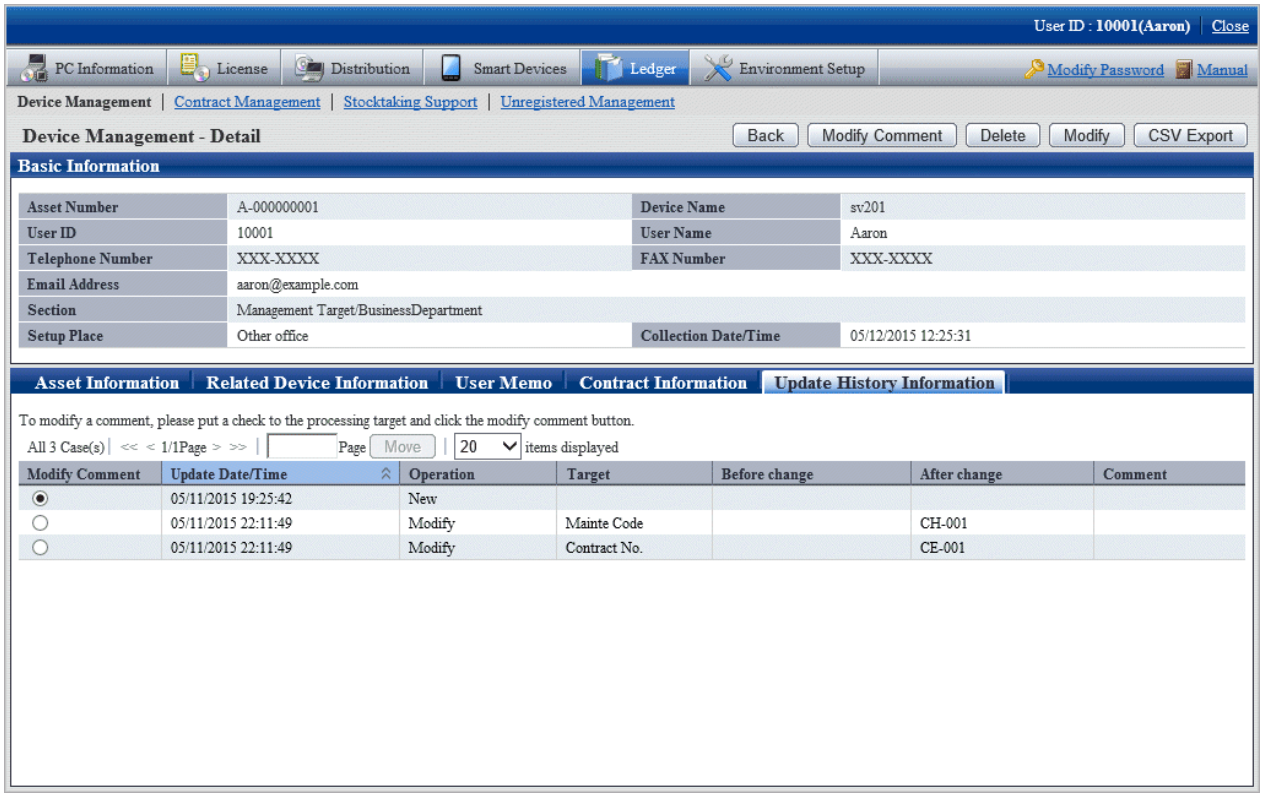
7. When viewing update history by device unit, click the link of device name (or asset number) to be viewed.

   The following window will be displayed



8. Click the **Update History Information** tab.

   The following window will be displayed



   The information before and after modification output to the **Update History Information** window will display the updated information.

9. Confirm the update history of the selected machine.

   Confirm the following information.

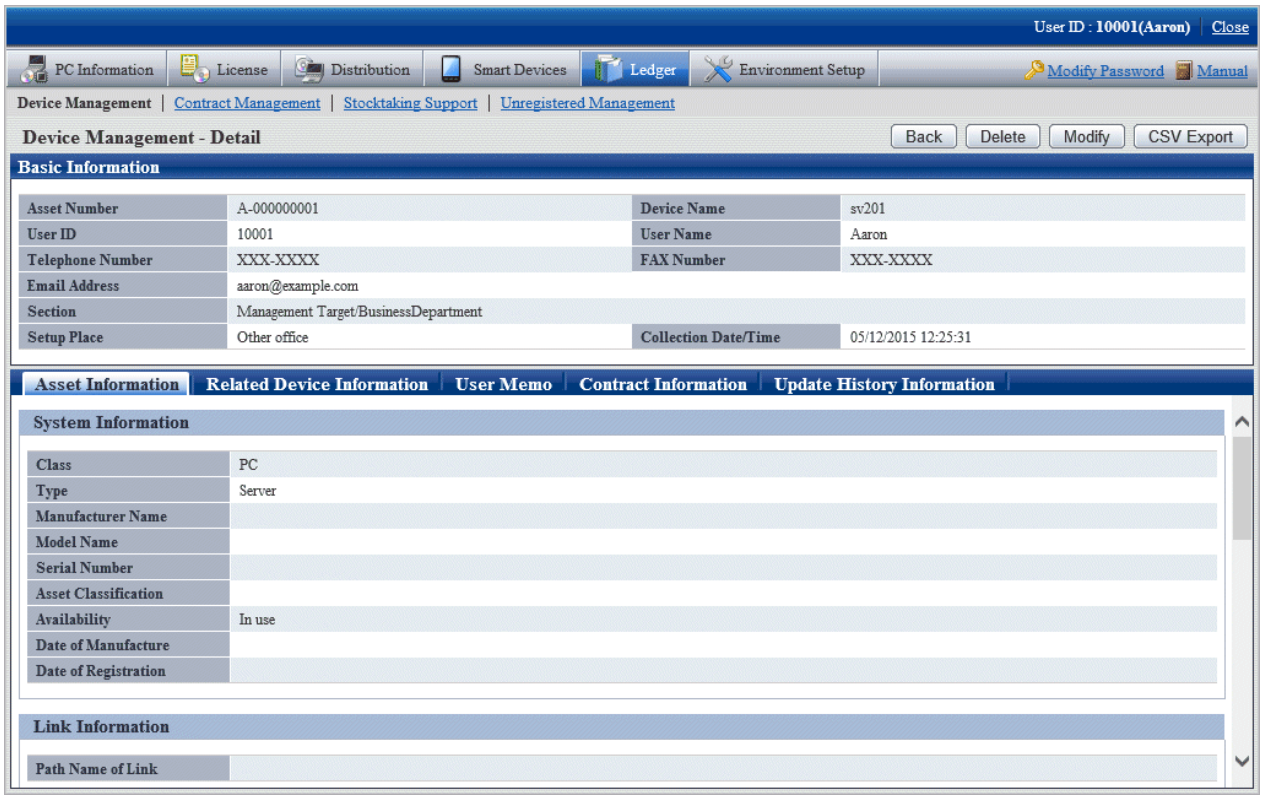
Item	Descriptions
Update Date/Time	Date and time for update.
Operation	Operations to the device information. Any of the following will be displayed. - **New** - **Modify** - **Delete**
Target	Name of item which has been modified.
Before change	Information before modification.
After change	Information after modification.
Comment	Annotation of device information modification history. When registering/modifying/deleting the device information in **Comment**, the annotation set automatically or set by the user will be displayed. In the following operations, the annotation will be set automatically. - Modify PC adding/PC information through automatic reflection The annotation is "Automatic Synchronization". - Access the setting location through the inventory result

Item	Descriptions
	- Register or remove distribution through the **Contract Information Distribution** window The annotation is "Modify through Contract Information Distribution". - Contract Extension through **Extend Contract** The annotation is "Modify by Extending Contract".

11.3.1.5 Delete Device Information

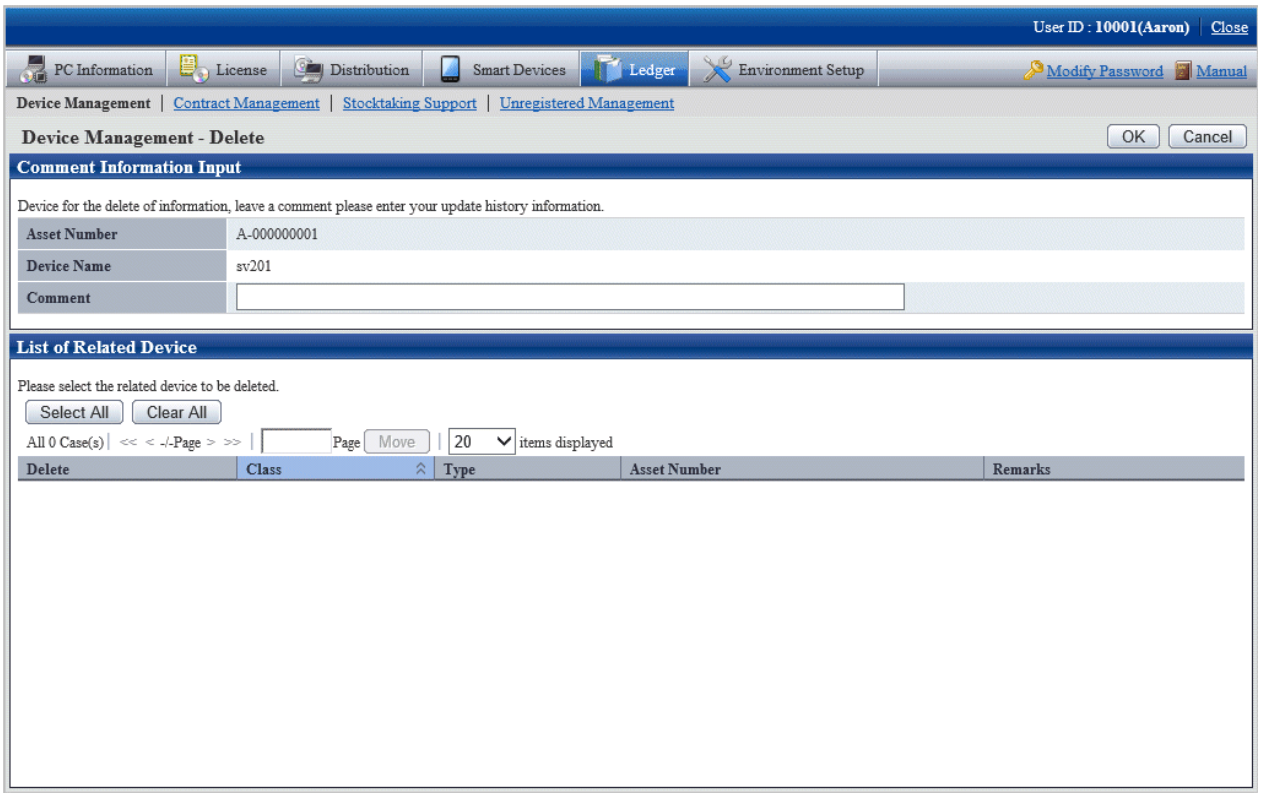
The procedure for deleting device information is as follows. The deletion of the device information will be the procedure after "11.3.1.2 Confirm List of Device".

1. Start the window for confirming device details.



2. Click the **Delete** button in the window above.

   The following window will be displayed



3. Input the annotation for the operation of deleting the device information.

   Including single-byte alphanumeric characters, single-byte symbols and multi-byte characters, up to 32 fullwidth or 64 halfwidth characters can be set for the annotation.

   The information input as the annotation can be confirmed the update history window. For the update history window, refer to "11.3.1.4 Confirm History Information".

   When deleting the related device also, select the related device to be deleted.

4. Click the **OK** button.

   The device information is deleted.

Note

The section administrator cannot delete the related device of other section

The device information which can be deleted by the section administrator is limited to this section and its subordinate machine.

Even if the related device is managed by this section itself, but when this related device is managed by other section, it cannot be deleted.

In this case, "Cannot Delete Device of Other Section" will be displayed in the remarks of the window above.

Note

If a device to be deleted contains PC or smart device inventory information, delete the inventory information as well as the device information.

11.3.2 Register/Modify Device Information

This section describes how to register or modify the information of one machine.

Besides, when collectively registering or modifying, refer to "11.2.1 Procedures for Registering/Modifying Asset Information".

Procedures

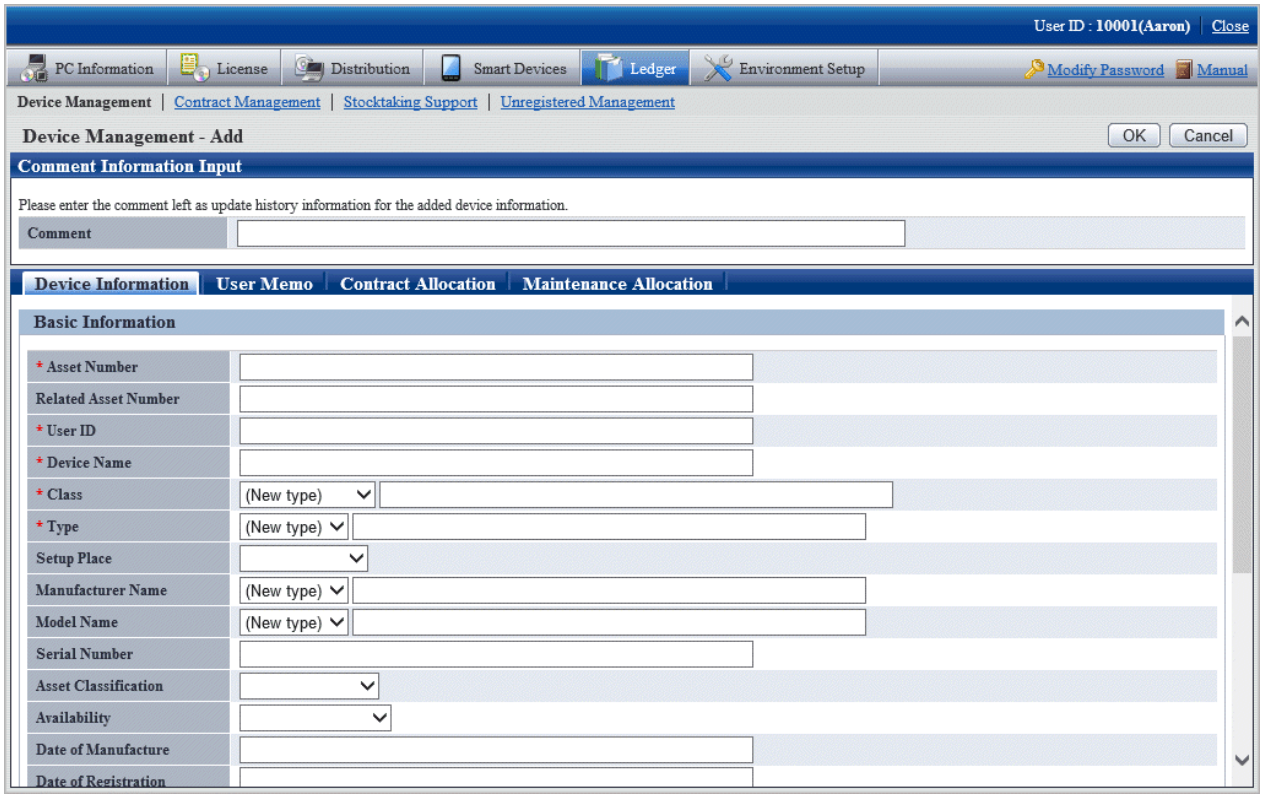
The procedure for registering or modifying the information of one device is as follows.

Besides, by operation of clicking the **Add** or **Modify** button in "11.3.1 Confirm/Delete Device Information", describe the procedure.

1. Click the **Add** or **Modify** button.

   The following window will be displayed

   Besides, the following displays the window when clicking the **Add** button.



2. Input the command.

   Set the following information.

Item	Descriptions
Comment	Input the annotation for the content of device information to be registered or modified. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The information input as the annotation can be confirmed in the update history window. For the update history window, refer to "11.3.1.4 Confirm History Information".

3. Register or modify the device information.

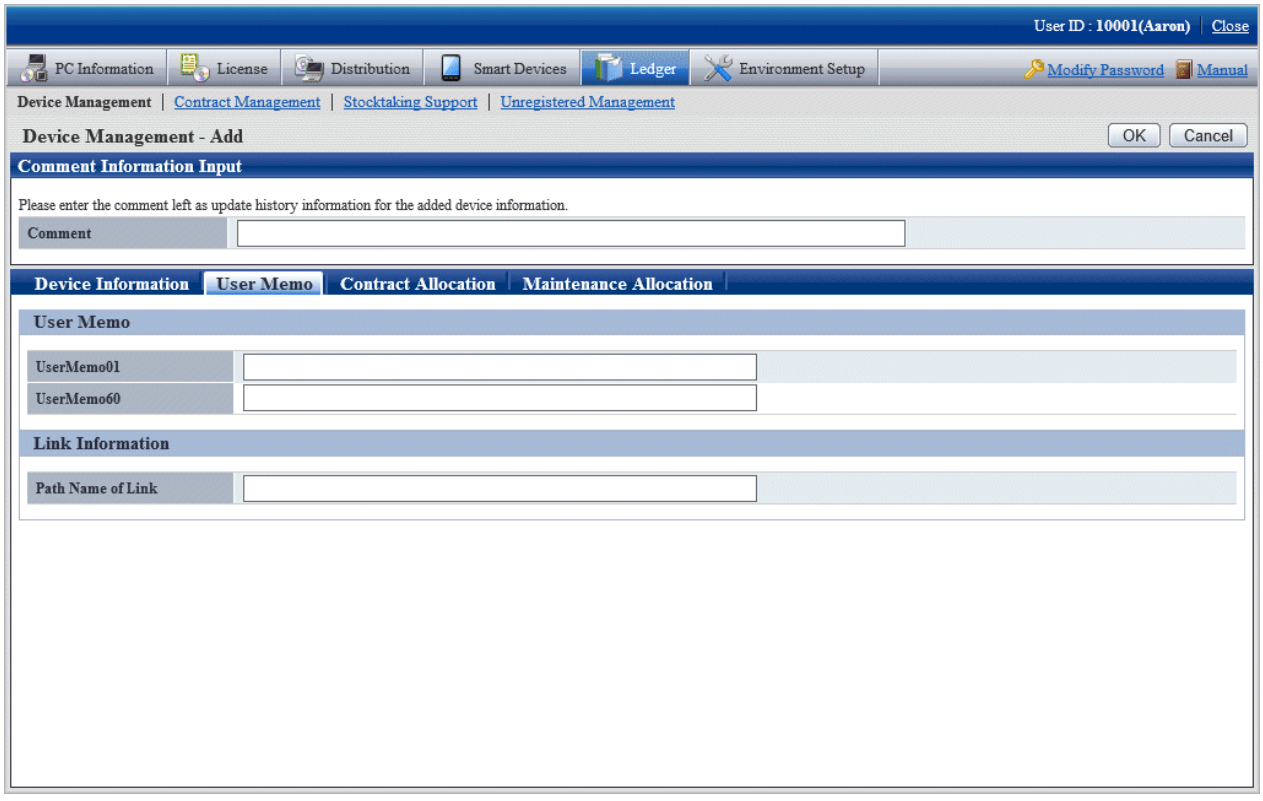
   Set the information in each tab.

Tab Name	Item	Descriptions
Device Information	**Asset Number** (Required)	Set the asset number for the machine. Specify up to 24 halfwidth alphanumeric characters and symbols. But for English letters, it is case insensitive. When using lower-case characters, they will be registered or modified as upper-case ones. For example, "a001" will become "A001". Besides, the asset number will be set automatically when the automatic setting for asset number has been started, so it will be set arbitrarily. For automatic setting, refer to "11.1.2 Set Registration for Device Information".
	Related Asset Number (Arbitrarily)	Set the asset number for related machine. For example, as the device based on "PC Itself" and to be linked with "Keyboard" and "Mouse", set the asset number for "PC Itself" of the basic device in the "Related Asset Number" of "Keyboard" and "Mouse". **Related Asset Number** need not be set specially in the device information of the basic machine. The conditions for the input characters are the same as **Asset Number** above. Besides, when the related asset number has not been input, the value same as the asset number will be the related asset number. When the following related asset number has been input, the input value error will occur. - When multi-byte characters are contained - When the device with the input related asset number does not exist - When the number of related device correspondent to the device with the input related asset number exceeds 100 - When the device with the input related asset number has been the related device of other machine - (Only during modification) in case the input related asset number is different from the asset number, when the asset number before modification is being used as the related asset number of other machine
	User ID (Required)	Set the user ID for the user who uses the machine. Errors will occur if the value which has not been registered to Systemwalker Desktop Patrol is set. Specify up to 20 halfwidth alphanumeric characters and symbols. Besides, when modifying the device information, in case of the device information existing as Inventory information, it cannot be modified. The device information can only be modified when it has not been existing as Inventory information.
	Device Name (Required)	Set the device name. Specify up to 10 fullwidth or 20 halfwidth characters. Besides, when modifying the device information, in case of the device information existing as Inventory information, it cannot be modified. The device information can only be modified when it has not been existing as Inventory information.

Tab Name	Item		Descriptions
	Class (Required)		Select or set new classification from the list. Specify up to 16 fullwidth or 32 halfwidth alphanumeric characters and symbols. The list information is **Class** information registered as the device information. Besides, if **PC** has been set, error will occur after **Device Name** and **User ID** match the other registered PC. Or in the device set as **PC**, it cannot be modified as the classification as non **PC**. On devices for which **Smart device** has been set, the class cannot be changed.
	Type (Required)		Select or set new category from the list. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The list information is **Type** information registered as the device information.
	Setup Place		Set the setting location for the machine.
	Manufacturer Name		Select or set new manufacturer name from the list. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The list information is **Manufacturer Name** information registered as the device information.
	Model Name		Select or set new Model Name from the list. Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The list information is **Model Name** information registered as the device information.
	Serial Number		Set the serial number for the machine. Specify up to 12 fullwidth or 24 halfwidth alphanumeric characters and symbols.
	Asset Classification		Select from the list. The list information is **Asset Classification** information registered as the device information.
	Availability		Select from the list.
	Network Information	**IP Address 1** **IP Address 2**	Set the IP address in the following format. - IPv4 address: XXX.XXX.XXX.XXX XXX: single-byte numbers within 0~255 can be set. - IPv6 address: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX XX: Only hexadecimal values between 00 and FF can be specified. Both uppercase and lowercase halfwidth letters can be specified. The abbreviated format can also be specified.

Tab Name	Item		Descriptions
		MAC Address 1 **MAC Address 2**	Set the MAC address in the following format. XX:XX:XX:XX:XX:XX XX: only hexadecimal description from 00 to FF can be set. For single-byte letters, it is case insensitive. The separator can also be set as "-". Besides, the separator can also be omitted. When the separator "-" is omitted, the address will be registered in the management ledger with the separator as ":". Example for setting: FF:0B:5D:D0:D7:13 FF-0B-5D-D0-D7-13 FF0B5DD0D713
	Date of Manufacture		Set the date of manufacture for the machine. Specify up to 10 fullwidth or 20 halfwidth alphanumeric characters and symbols.
	Date of Registration		Set the date for registering to the device asset ledger. Specify up to 10 fullwidth or 20 halfwidth alphanumeric characters and symbols.

The following is the window when selecting the **User Memo** tab.



Set the following information.

Tab Name	Item	Descriptions
User Memo	**User Memo**	Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The displayed information is **User Memo** information registered as the device information.
	Path Name of Link	Data related to the device (for example, device image) or the input network path and URL which can be set arbitrarily. Specify UNC description using up to 127 fullwidth or 255 halfwidth characters. When the specified path cannot be viewed through CS, error will occur. When the specified path is started as "http:" or "https:", without detecting whether the file exists, it is determined as URL.

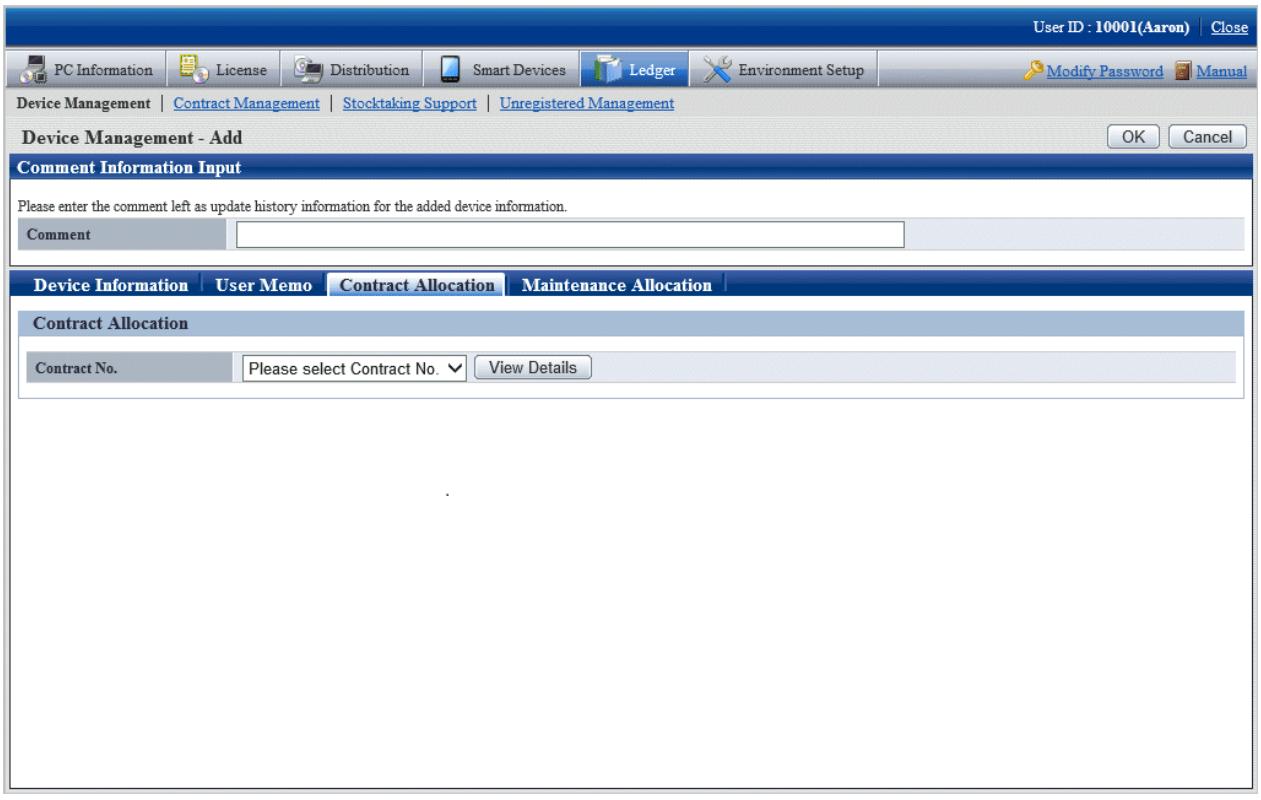
Note

User Memo cannot be registered/modified in the initial settings

For **User Memo** which can be registered or modified as the device information, if **User Memo Related** has not been set in the settings of window item name, it cannot be registered or modified.

For window item name setting, refer to "11.1.6 Set Window Item Name".

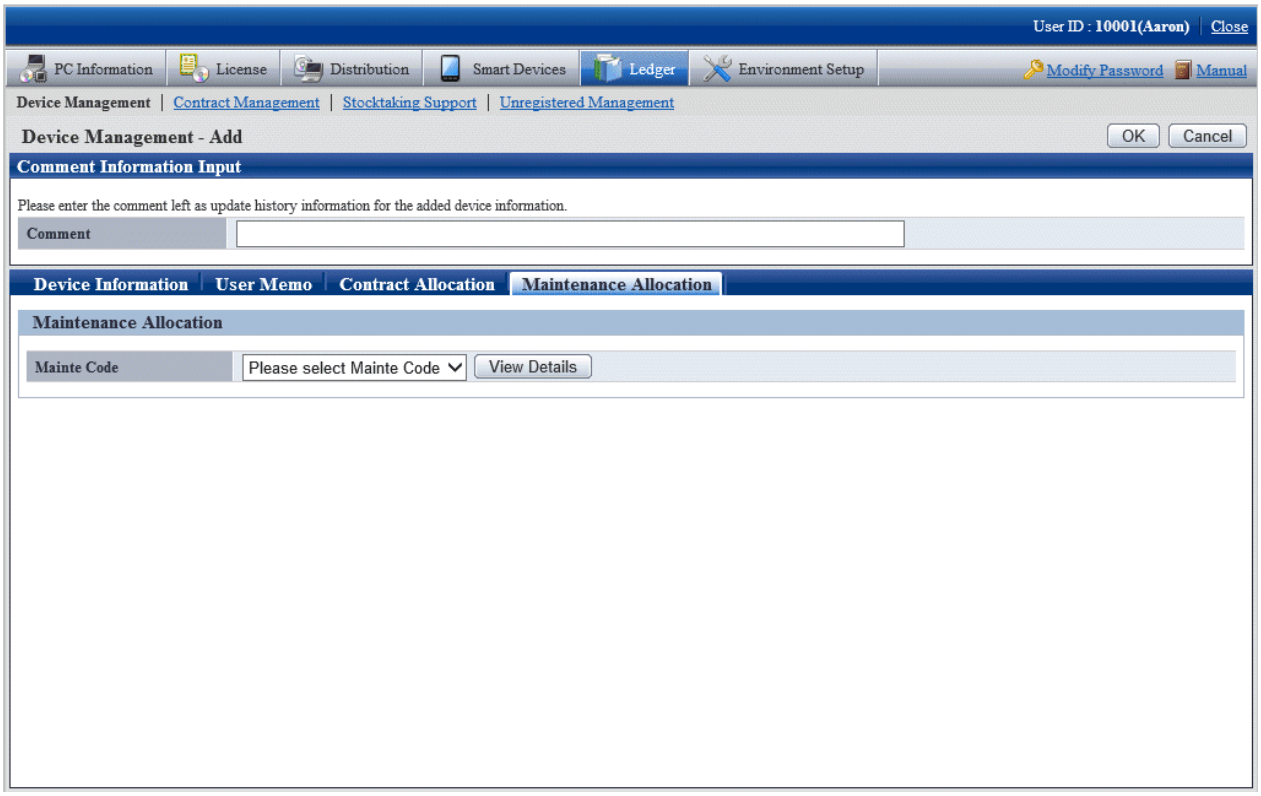
The following is the window when selecting the **Contract Allocation** tab.



Set the following information.

Tab Name	Item	Descriptions
Contract Allocation	**Contract No.**	Select the contract information distributed to the device information through the list. The list information is **Contract No.** related information registered as the contract information.

The following is the window when selecting the **Maintenance Allocation** tab.



Set the following information.

Tab Name	Item	Descriptions
Maintenance Allocation	**Maintenance Code**	Select the contract information distributed to the device information through the list. The list information is **Maintenance Code** related information registered as the contract information.

4. Click the **OK** button.

   The set or modified information is reflected.

11.3.3 Save Device Information as Ledger

This section describes how to save the device information displayed in the window as ledger.

Besides, the ledger saved in the EXPORT file format can be registered through "11.2.2 Register/Modify Ledger", and information can be updated collectively.

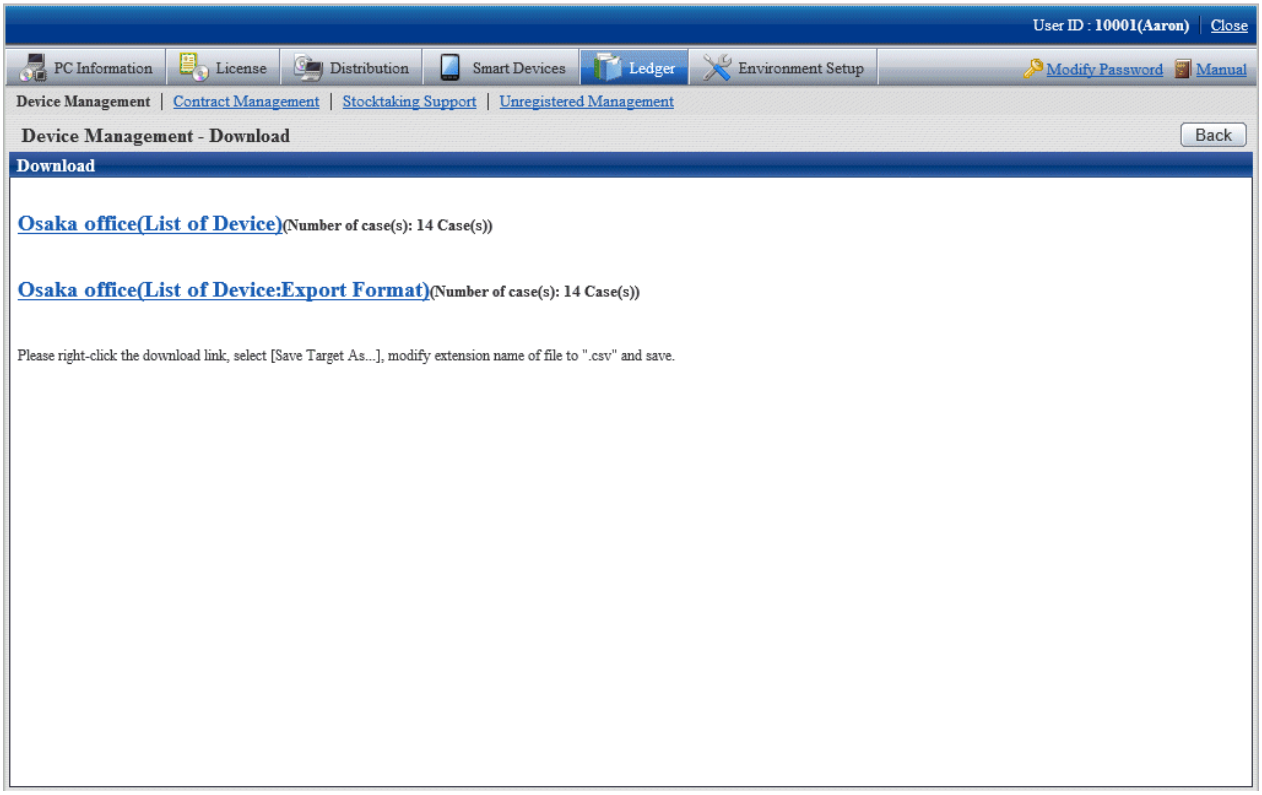
Procedures

The procedure for saving the device information displayed in the window as ledger is as follows.

Besides, the procedure will be described by the operation of clicking the **CSV Export** button in "11.3.1 Confirm/Delete Device Information".

1. Click the **CSV Export** button.

   The following window will be displayed



2. Right click the download link, select **Save Target As...**, modify extension of file as '.csv' and save. The following files can be downloaded.

   - CSV file (*.csv)

     Saved as CSV file.

   - EXPORT file (*.csv) (download only in case of the device list window)

     Saved in the format registered in "11.2.2 Register/Modify Ledger".

   For details of saved files, refer to "Device Confirmation File", "Device List File" or "Device Details File" of *Systemwalker Desktop Patrol Reference Manual*.

11.4 Contract Management

This section describes how to manage the contract information registered in the management ledger.

11.4.1 Confirm Contract Information

For the method for confirming the registered contract information as "By Section" and "By Classification", it describes the following items in the operation procedure.

- "11.4.1.1 Confirm Various Contract Information"
- "11.4.1.2 Confirm List of Contract"
- "11.4.1.3 Confirm Details of Contract"
- "11.4.1.4 Delete Contract Information"

11.4.1.1 Confirm Various Contract Information

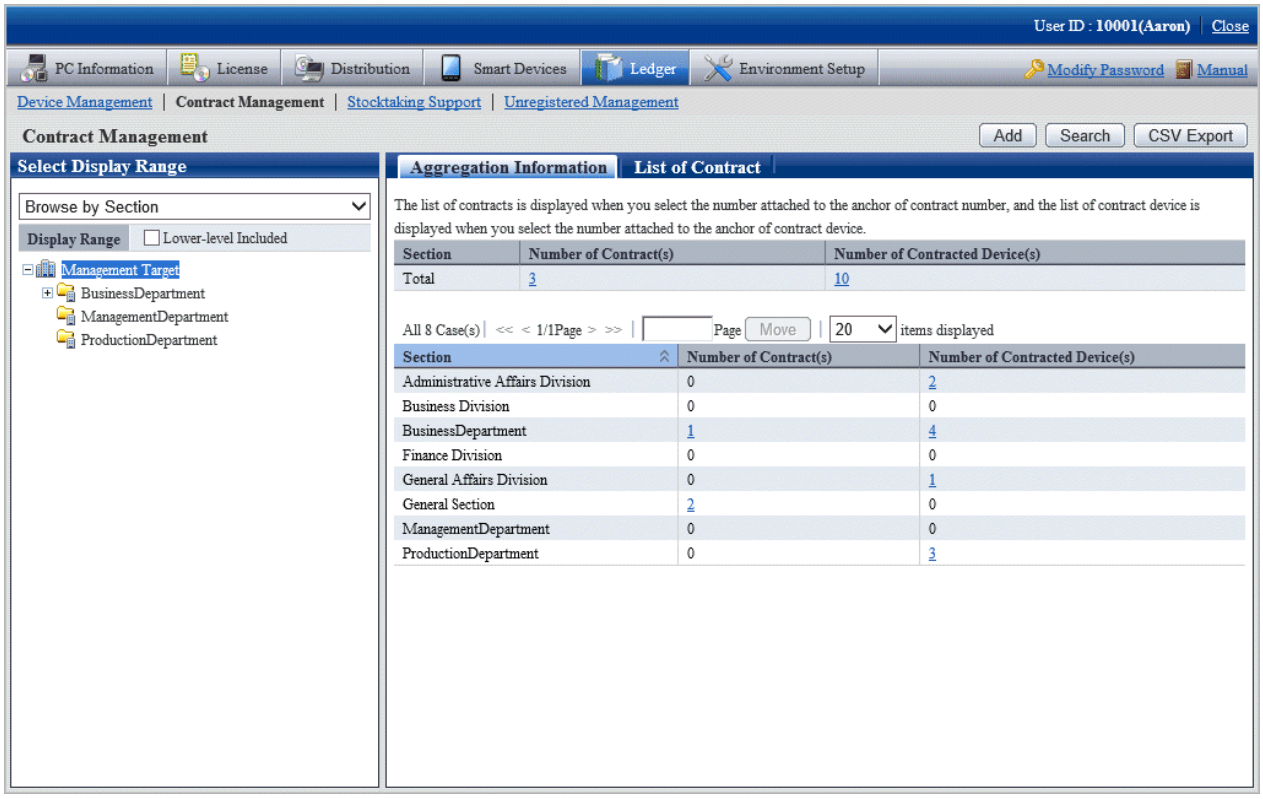
The procedure for confirming various contract information of "By Section" and "By Category" is as follows:

1. Log onto the main menu, click **Ledger**.

   The **Ledger** window will be displayed

2. Click **Contract Management**.

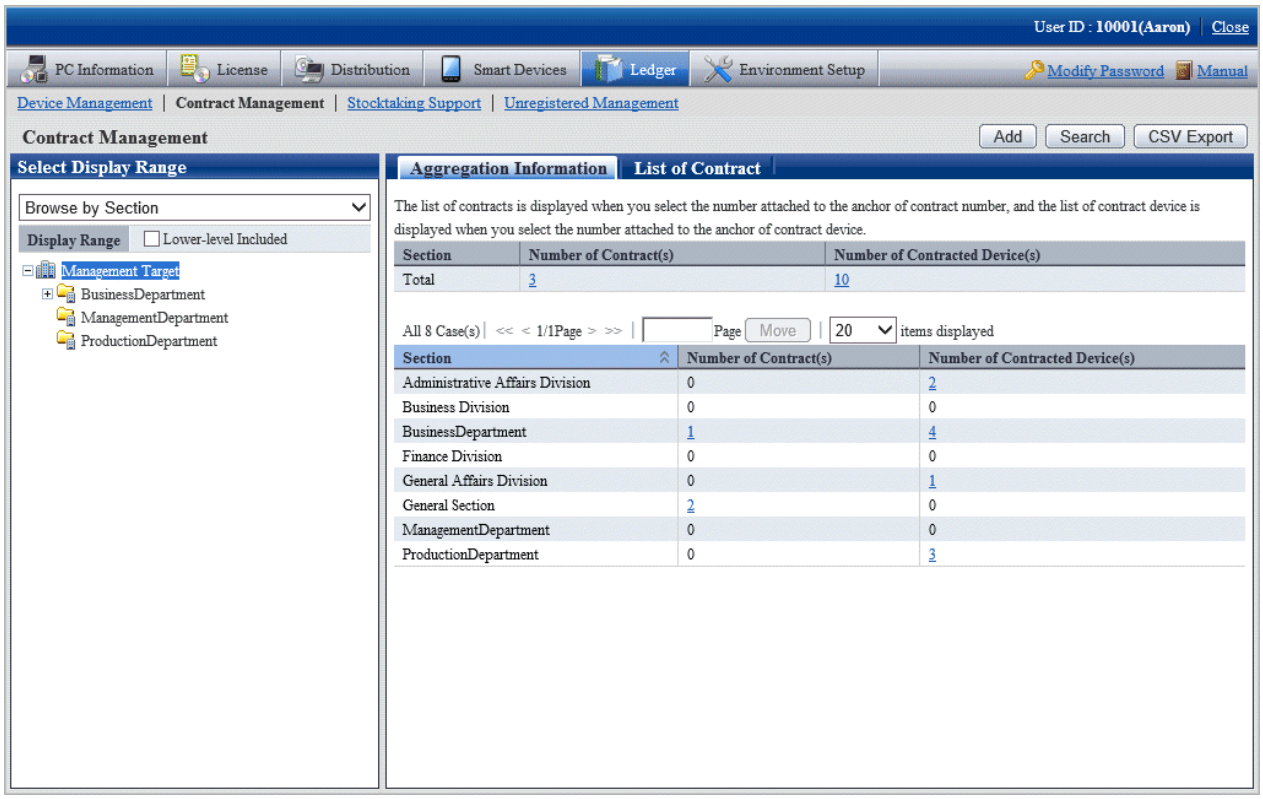
   The following window will be displayed



3. Confirm the contract information by section.

   According to the drop-down menu on the left side of the window, select **Browse by Section** from the list.

The following window will be displayed



The meaning of each item is as follows:

Besides, it describes the situation of all display item(s).

Item	Descriptions
Section	Section information.
Number of Contract(s)	Number of contract managed in the section.
Number of Contracted Device(s)	Number of device distributed to the contract among the device managed in the section.

Remarks.

When the system administrator selects the management target, in the total **Number of Contract(s)**, the number of contract with the defrayal party as the management target will also be aggregated.

Besides, when selecting the management target, in the total **Number of Section Contracted Device(s)**, number of device of the not configured section will also be aggregated.

Besides, the action of each button is as follows:

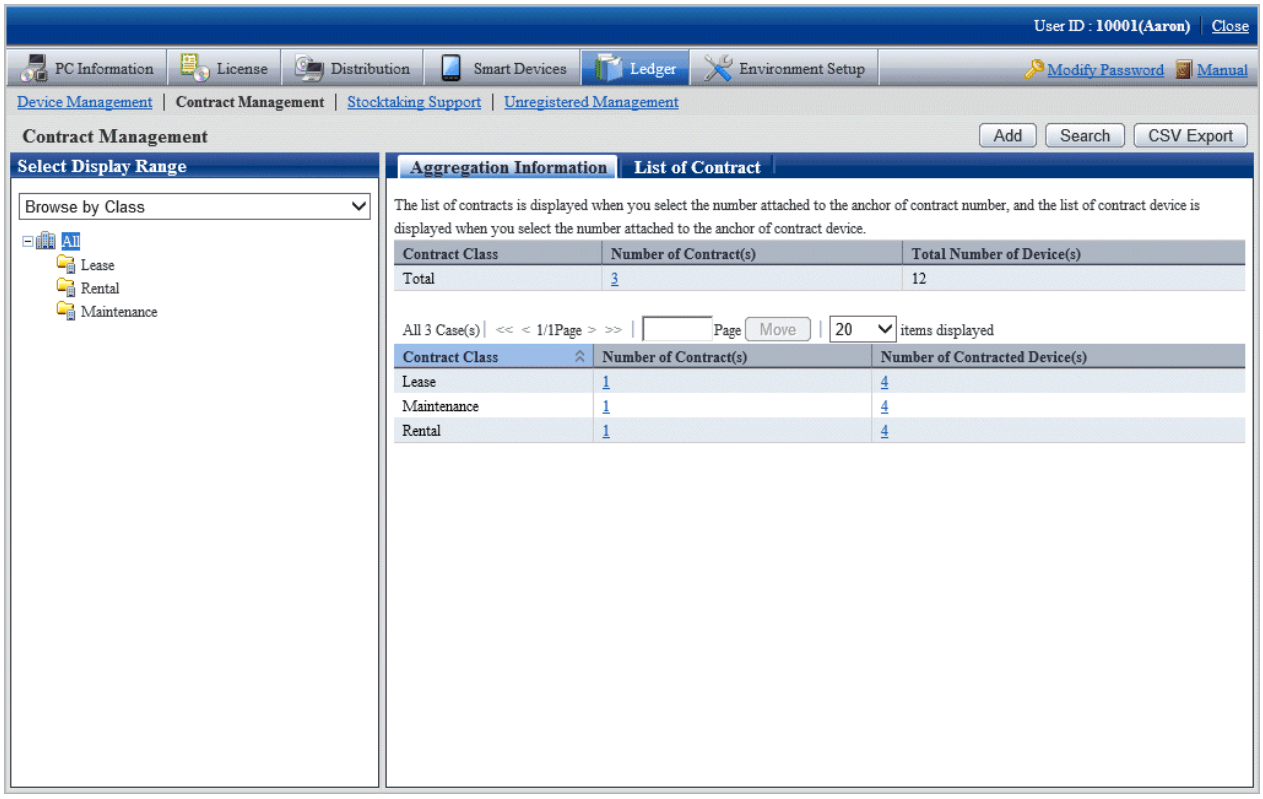
Item	Descriptions
Add	Register the contract information. For details, refer to "11.4.2 Register/Modify Contract Information".
Search	Filter to display the contract displayed in the window. For details, refer to "Screen contract".
CSV Export	Save the information displayed in the window as ledger.

Item	Descriptions
	For details, refer to "11.4.4 Save Contract Information as Ledger".

4. Confirm the contract information by classification.

   According to the drop-down menu on the left side of the window, select **Browse by Class** from the list.

   The following window will be displayed



   The meaning of each item is as follows:

   Besides, it describes the situation of all display item(s). And the action of the button is the same as that of the window above for contract confirmation by section.

Item	Descriptions
Contract Class	Information of contract classification. **Contract Class** information registered as the contract information.
Number of Contract(s)	Number of contracts of contract classification unit.
Total Number of Device(s)	Total number of contract device of lease/rent/maintenance contract. When the lease contract and maintenance contract are distributed in one machine, it is aggregated as 2.
Number of Contract Device(s)	Number of device distributed in the contract of the contract classification unit.

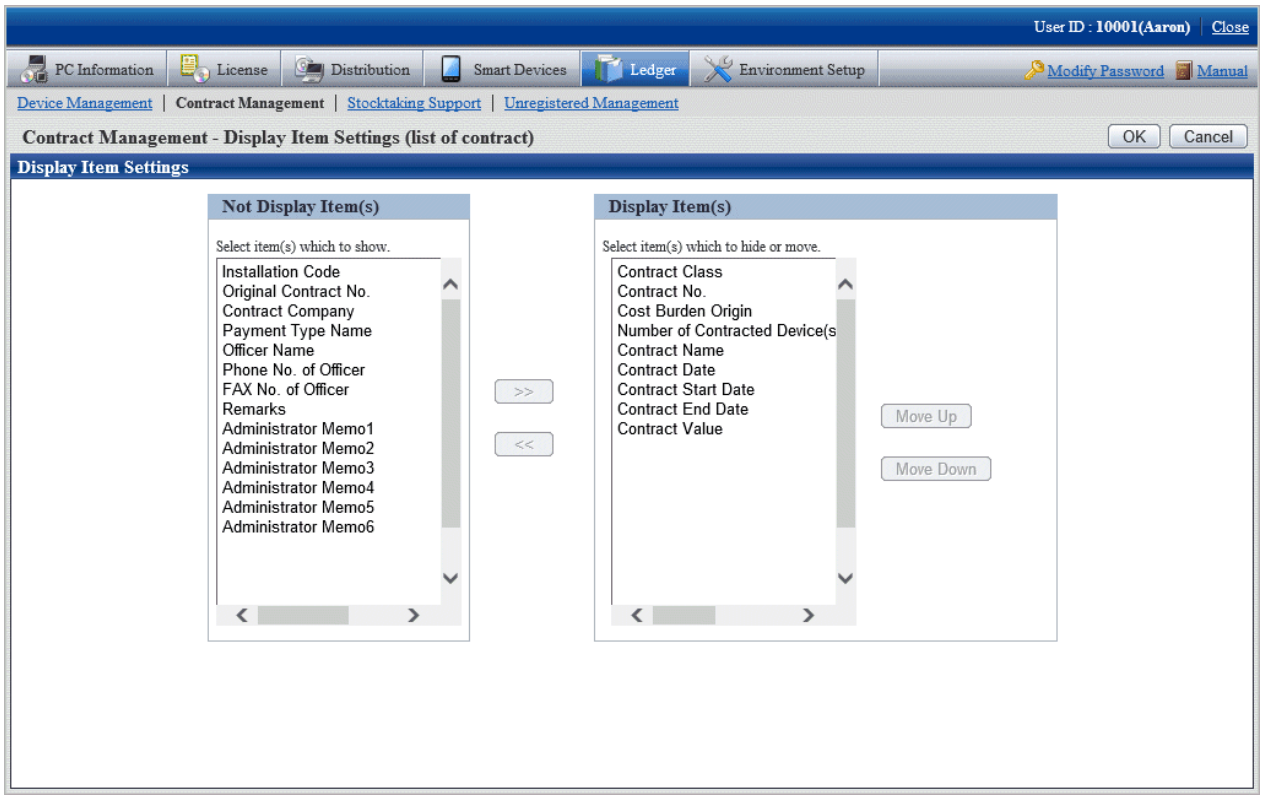
Set display item(s)

It describes how to set the items displayed in the window.

1. Click the **Display Item Settings** button.

   The following window will be displayed

   Besides, the window when clicking the **Display Item Settings** button in the window for contract confirmation by section will be displayed.



2. Set the display item(s) according to the following procedure.

   a. Select the items displayed in the contract list from the **Not Display Item(s)** list on the left side of the window, and click the >> button in the center of the window. Multiple items can be selected.

      The selected items are added to **Display Item(s)** on the right side of the window.

   b. Select the items not displayed in the contract list from the **Items That Can be Displayed** list on the left side of the window, and click the << button in the center of the window. Multiple items can be selected.

      The selected items are deleted from **Display Item(s)** on the right side of the window.

   c. When modifying the order of **Display Item(s)**, select the items from **Display Item(s)** on the right side of the window and click the **Move Up** or **Move Down** button.

3. After completing the setting of display item(s), click the **OK** button.

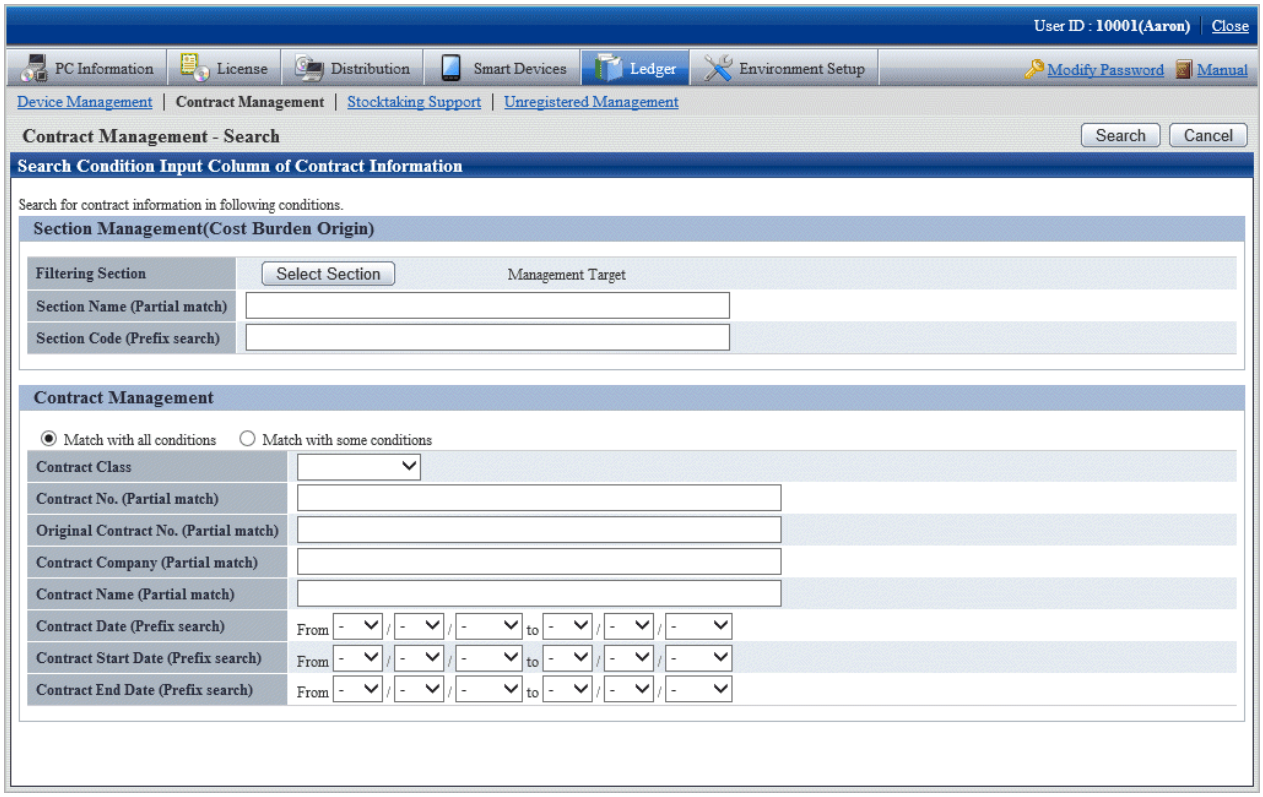
   The display item(s) of contract list are added to the set items.

Screen contract

It describes how to screen the contract displayed in the window.

1. Click the **Search** button.

   The following window will be displayed



2. Set the screening aggregation.

   Set the following information and click the **Search** button.

   Only the items matching the search will be displayed in the window.

Item		Descriptions
Section Management (Cost Burden Origin)	**Filtering Section**	Set conditions when screening defrayal party by section.
	Section Name	Set conditions when screening defrayal party by section name.
	Section Code	Set conditions when screening defrayal party by section code.
Contract Management	**Match with all conditions** or **Match with some conditions**	For conditions set in the **Contract Management** bar, select **All Conditions Match** with all containing multiple conditions or **Any Condition Match** containing one or more conditions.
	Contract Class	Set conditions when screening by contract classification. The value of **Contract Class** registered as the contract information will be displayed in the list.
	Contract No.	Set conditions when screening by contract number.
	Original Contract No.	Set conditions when screening by original contract number.
	Contract Company	Set conditions when screening by contract company name.
	Contract Name	Set conditions when screening by item name.
	Contract Date	Set conditions when screening by contract date.

Item		Descriptions
	Contract Start Date	Set conditions when screening by contract start date.
	Contract End Date	Set conditions when screening by contract expiry date.

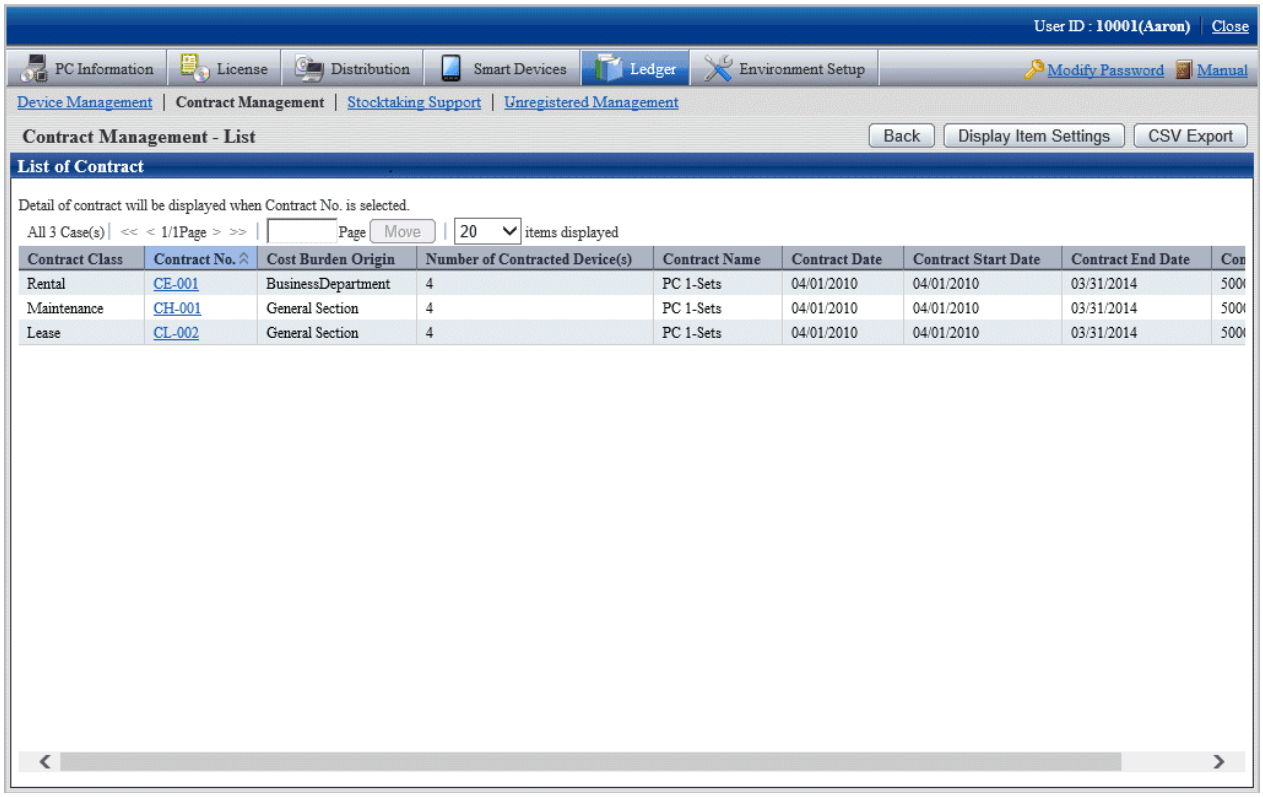
11.4.1.2 Confirm List of Contract

The procedure for confirming the various lists of contract of "In Section" and "In Classification" are as follow:

Besides, it will be the procedure after "11.4.1.1 Confirm Various Contract Information". Or the following describes according to the window "In Section". The order of items displayed "In Location" is different, but it can be confirmed according to the same procedure.

1. Click the value of **Number of Contract(s)**.

   The following window will be displayed



2. Confirm the contract list of the selected items.

   Confirm the following information.

   Besides, it describes the situation of all display item(s).

Item	Descriptions
Cost Burden Origin	Information of the contract defrayal party, **Cost Burden Origin** information registered as the contract information.
Contract No.	Contract No. information. **Contract No.** information registered as the contract information.
Original Contract No.	Contract number information before contract extension. **Original Contract No.** information registered as the contract information.

Item	Descriptions
Contract Class	Contract classification information. **Contract Class** information registered as the contract information.
Number of Contract Device(s)	The number of distributed device in the contract. Number of device distributed in the contract managed by the section.
Contract Company	Name of company signing the contract. **Contract Company** information registered as the contract information.
Contract Name	Name of items in the signed contract. **Item Name** information registered as the contract information.
Contract Date	The contract date for signing the contract. **Contract Date** information registered as the contract information.
Contract Start Date	The contract start date in the signed contract. **Contract Start Date** information registered as the contract information.
Contract End Date	The contract expiry date in the signed contract. **Contract Expiry Date** information registered as the contract information.
Contract Value	The contract amount in the signed contract. **Contract amount** information registered as the contract information.
Installation Code	The contract No. when signing the contract managed by the company. **Installation Code** registered as the contract information.
Payment Type Name	Method of payment such as monthly payment and yearly payment. **Payment Classification Name** information registered as the contract information.
Officer Name	Name of the contract principal. **Contract Principal** information registered as the contract information.
Phone No. of Officer	Telephone number of the contract principle. **Telephone of Contract Principal** information registered as the contract information.
Fax No. of Officer	Fax number of the contract principal. **Fax number of Contract Principal** information registered as the contract information.
Remarks	Remarks information of the contract, **Remarks** information registered as the contract information.
Administrator Memo 1~6	Remarks information of the contract. **Administrator Memo 1~6** information registered as the contract information.

Besides, the action of each button is as follows:

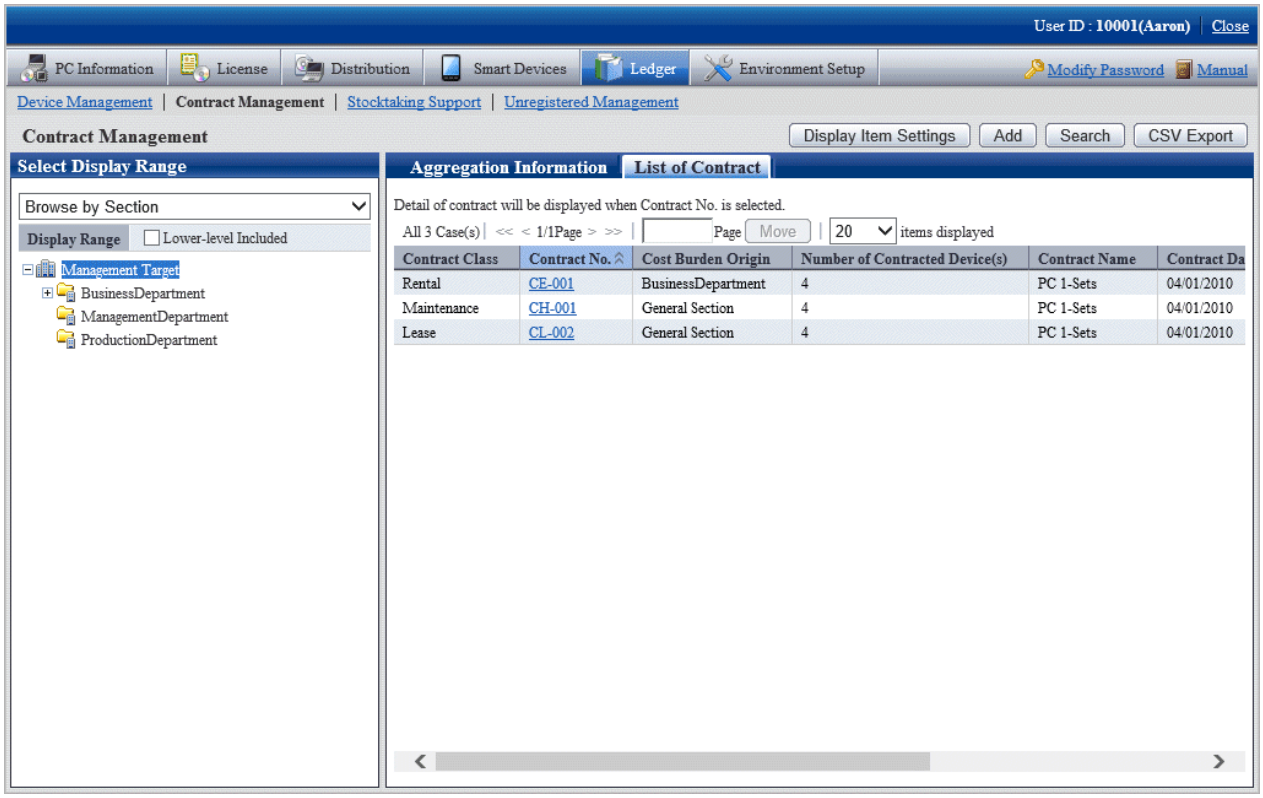
Item	Descriptions
Back	Display the previous window.
Display Item Settings	Set the items displayed in the window. For the details, refer to "Set display item(s)".

Item	Descriptions
CSV Export	Save the information displayed in the window as ledger. For details, refer to "11.4.4 Save Contract Information as Ledger".

Besides, the list of contract can also be confirmed according to the following procedure. Operate when confirming in the unit of section.

1. Click the **List of Contract** tab.

   The following window will be displayed



11.4.1.3 Confirm Details of Contract

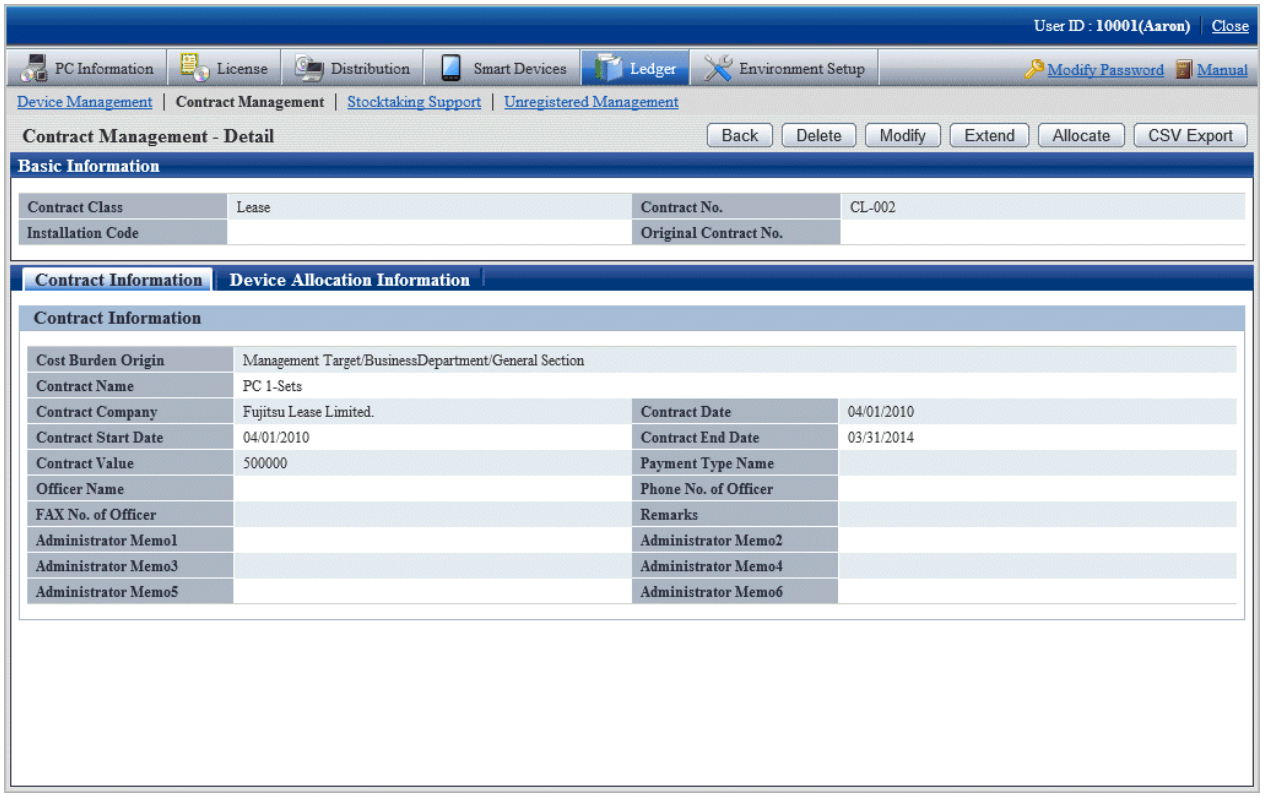
The procedure for confirming the details of contract are as follows.

Besides, the unnecessary contract information can be deleted during confirmation.

And it will be the procedure after "11.4.1.2 Confirm List of Contract" or "11.3.1.3 Confirm Device Details".

1. Click the **Contract No.** link for confirming the contract information.

   The following window will be displayed

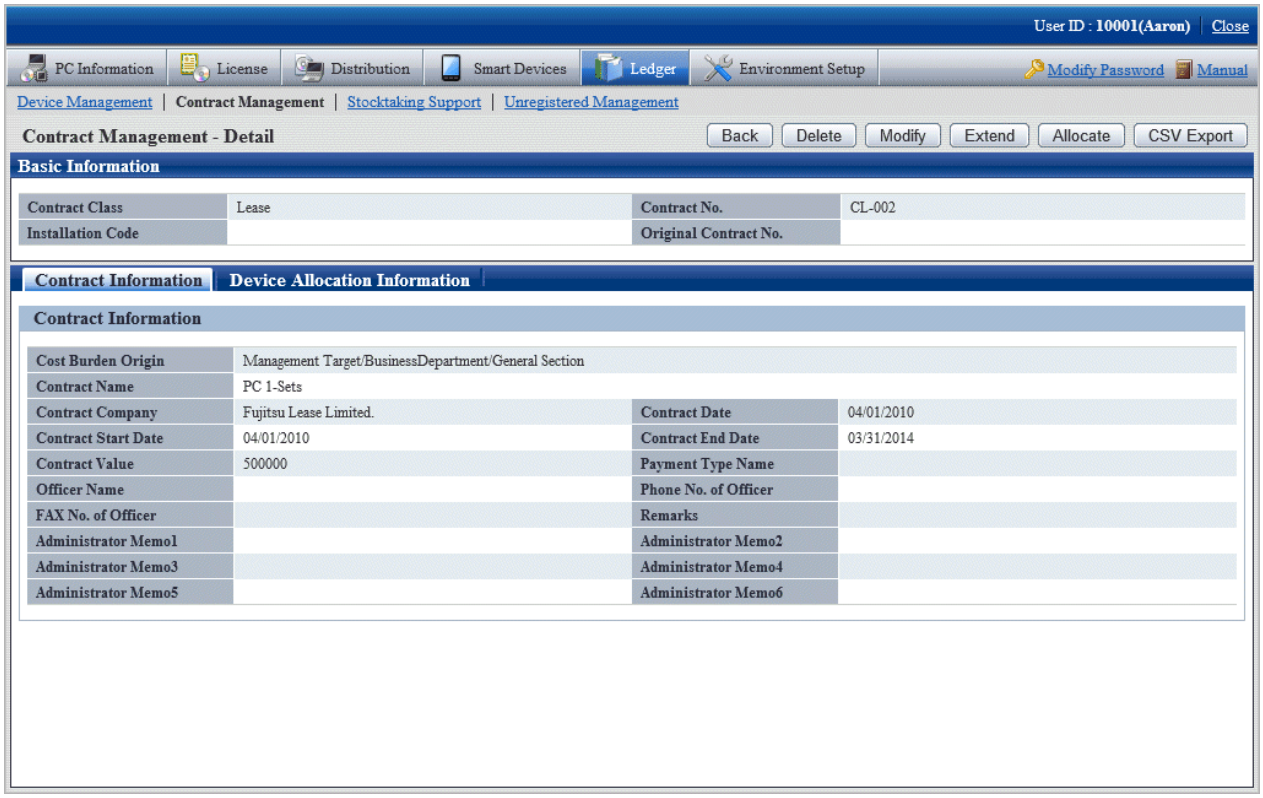


   The action of each button is as follows:

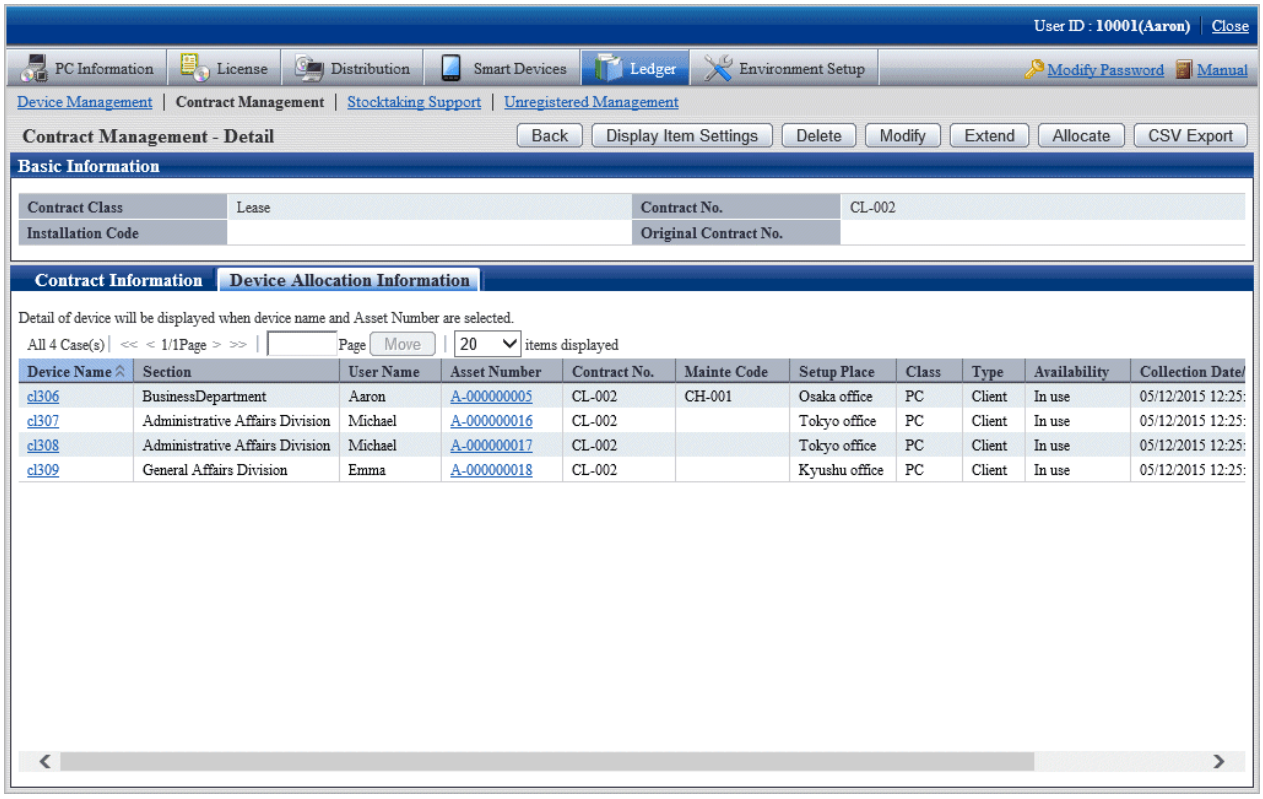
Item	Descriptions
Back	Display the previous window.
Displayed Item Setting	This button is displayed when selecting the **Device Allocation Information** tab. Set the items displayed in the window. For details, refer to "Set display item(s)".
Delete	Delete the contract information. For details, refer to "11.4.1.4 Delete Contract Information".
Modify	Modify the contract information. For details, refer to "11.4.2 Register/Modify Contract Information".
Extend	Extend the contract. For details, refer to "11.4.5 Extend Contract".
Allocate	Distribute the device information to the contract. For details, refer to "11.4.3 Distribute Contract Information".
CSV Export	Save the information displayed in the window as ledger. For details, refer to "11.4.4 Save Contract Information as Ledger".

2. Confirm the details of contract of the selected contract.

   When selecting the **Contract Information** tab, the contract information will be displayed.



3. When selecting the **Device Allocation Information** tab, the allocation device information will be displayed.



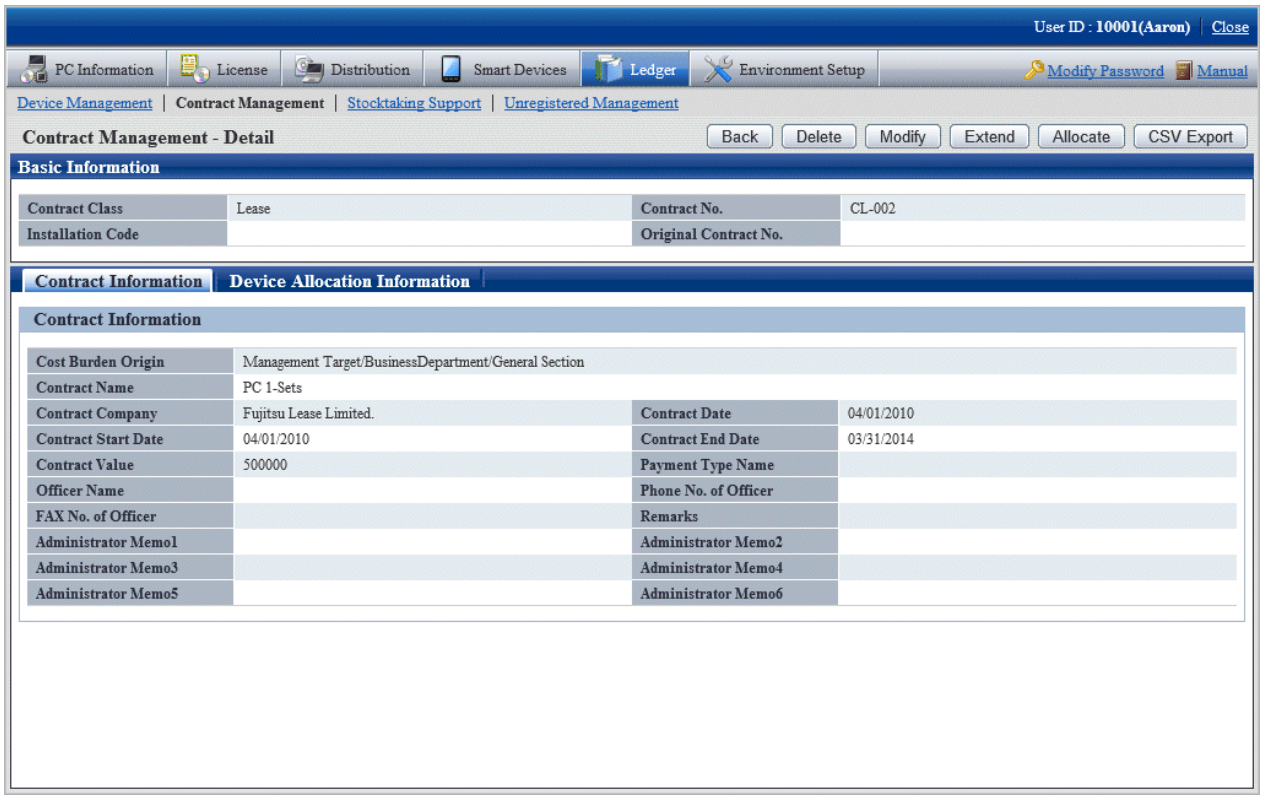
   Remarks. In case of section administrator, for device out of the range of Subordinate section, only the following information can be confirmed.

- **Asset Number**
- **Related Asset Number**
- **User ID**
- **User Name**
- **Device Name**
- **Section**
- **Class**
- **Type**
- **Contract No.**
- **Maintenance Code**

11.4.1.4 Delete Contract Information

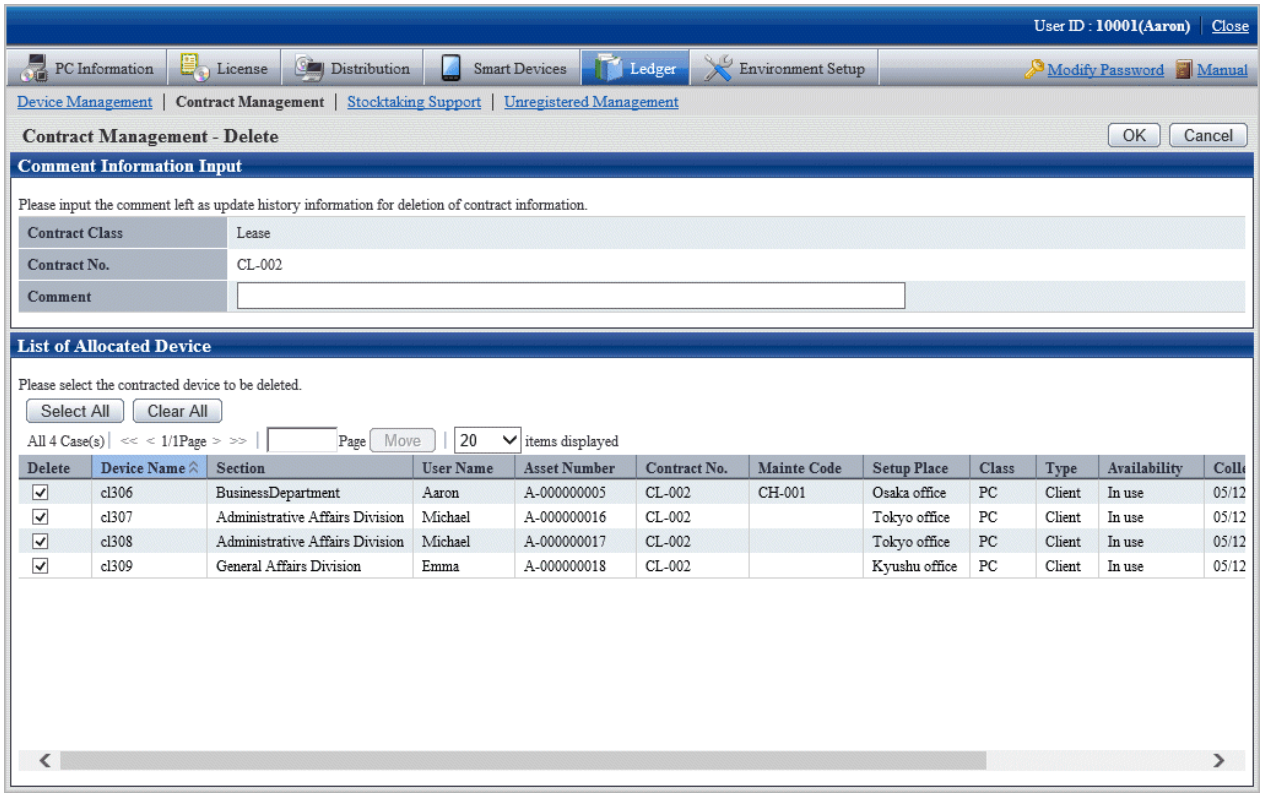
The procedure for deleting the contract information are as follows. The deletion of the contract information is the procedure after "11.3.1.3 Confirm Device Details".

1. Start the window for confirming the details of contract.



2. Click the **Delete** button in the window above.

   The following window will be displayed



3. Input the annotation for the operation of deleting the contract information.

   Specify up to 32 fullwidth or 64 halfwidth alphanumeric characters and symbols. The input annotation is valid only when deleting the contract information with the device information distributed.

   The information input as the annotation can be confirmed in the update history window. For the update history window, refer to "11.3.1.4 Confirm History Information".

   Besides, select the list of distributed device list to be deleted.

4. Click the **OK** button.

   The contract information is deleted.

11.4.2 Register/Modify Contract Information

This section describes how to register or modify the information of a contract.

Besides, when registering collectively, refer to "11.2.1 Procedures for Registering/Modifying Asset Information".

Procedures

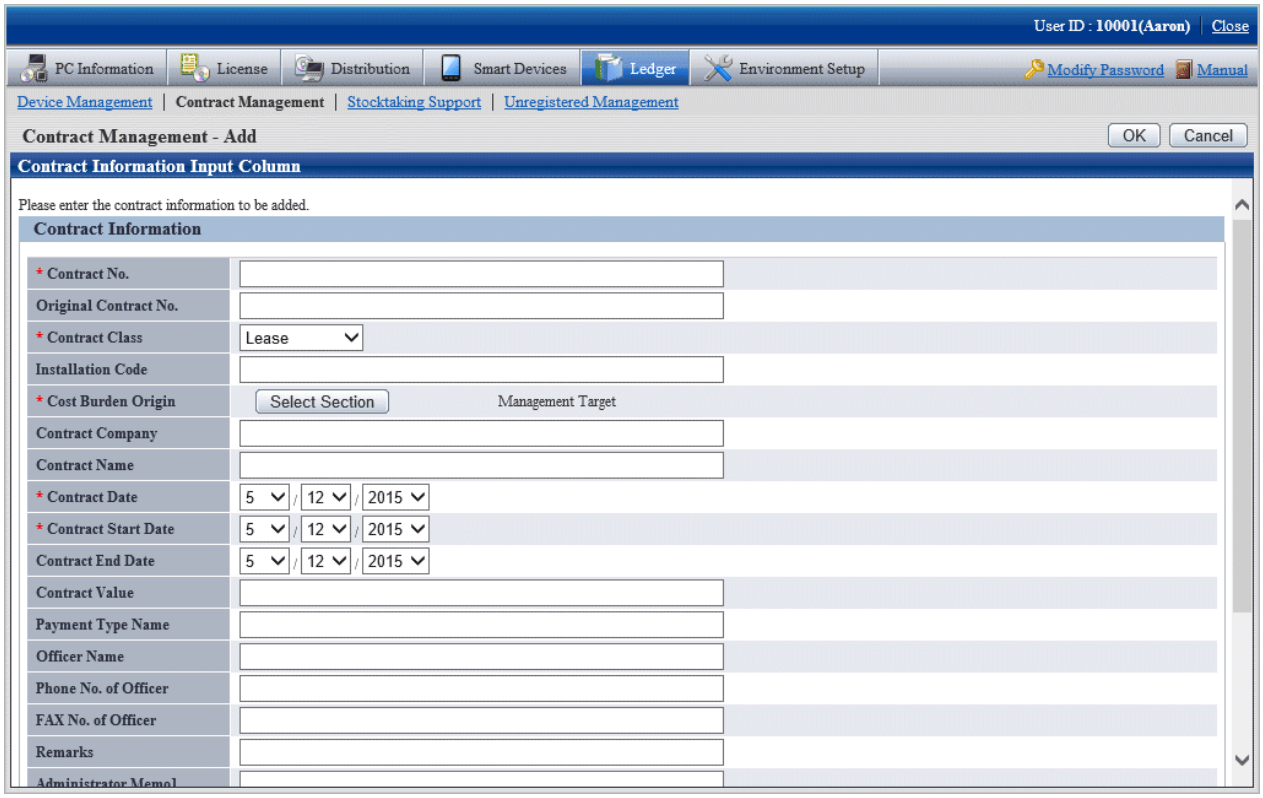
The procedure for registering or modifying the information of a contract are as follows.

Besides, by the operation of clicking the **Add** or **Modify** button in "11.4.1 Confirm Contract Information", the procedure are described.

1. Click the **Add** button or the **Modify** button.

   The following window will be displayed

Besides, the window when clicking the **Add** button will be displayed.



2. Register or modify the contract information.

   Set the following information and click the **OK** button.

Item	Descriptions
Contract No. (Required)	Set the contract number. Specify up to 20 halfwidth alphanumeric characters and the following symbol: - Besides, this item cannot be modified when modifying the contract information.
Original Contract No.	Set the contract number before contract extension. Specify up to 20 halfwidth alphanumeric characters and the following symbol: -
Contract Class (Required)	Select from the list. The list information is **Contract Class** information registered as the contract information. Besides, during modification, **Lease** can be modified as **Rent** only, or **Rent** modified as **Lease**.
Installation Code	Set the installation code. Including single-byte alphanumeric characters, single-byte symbols and multi-byte characters, 20 characters at most can be set.
Cost Burden Origin (Required)	Click the **Select Section** button, set the registered and modified section.
Contract Company	Set the name of company signing the contract.

Item	Descriptions
	Specify up to 30 fullwidth or 60 halfwidth alphanumeric characters and symbols.
Contract Name	Set the item name in the signed contract. Specify up to 64 fullwidth or 128 halfwidth alphanumeric characters and symbols.
Contract Date (Required)	Set the contract date.
Contract Start Date (Required)	Set the contract start date.
Contract End Date	Set the contract expiry date. Besides, after being omitted, it can be deleted from the contract expiration notification object.
Contract Value	Set the amount in the signed contract. Single-byte positive numbers within 9 digits can be set.
Payment Type Name	Set method of payment such as monthly payment and yearly payment. Specify up to 5 fullwidth or 10 halfwidth alphanumeric characters and symbols.
Officer Name	Set the name of contract principal. Specify up to 64 fullwidth or 128 halfwidth alphanumeric characters and symbols.
Phone No. of Officer	Set the telephone number of the contract principal. Specify up to 10 fullwidth or 20 halfwidth alphanumeric characters and symbols.
Fax No. of Officer	Set the Fax number of the contract principal. Specify up to 10 fullwidth or 20 halfwidth alphanumeric characters and symbols.
Remarks	Set the remarks information of the contract. Specify up to 30 fullwidth or 60 halfwidth alphanumeric characters and symbols.
Administrator Memo 1~6	Set the remarks information related to the contract. Specify up to 64 fullwidth or 128 halfwidth alphanumeric characters and symbols.

The set or modified information is reflected.

11.4.3 Distribute Contract Information

The following section describes how to distribute the device information to the registered contract information.

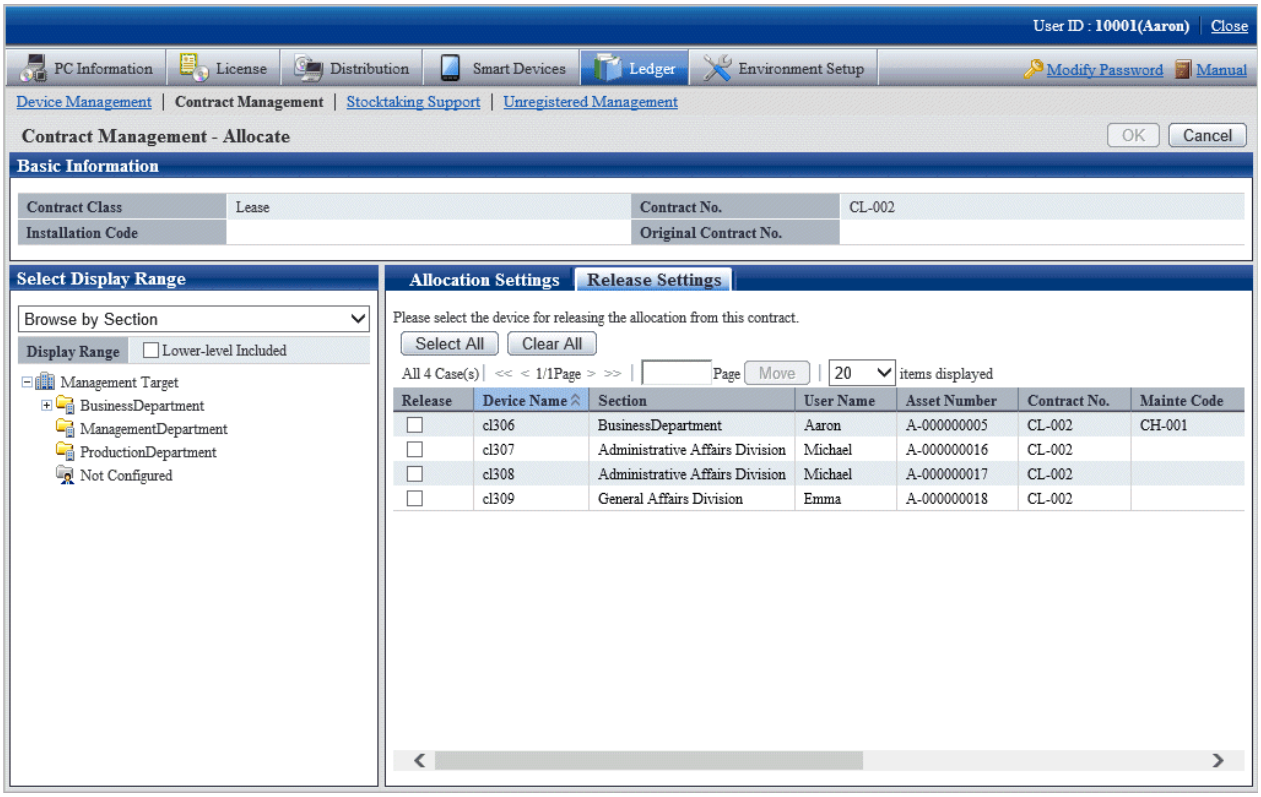
Procedures

The procedures for distributing the device information to the registered contract information are as follows.

In addition, by clicking the **Allocate** button in "11.4.1.3 Confirm Details of Contract", the procedure are described.

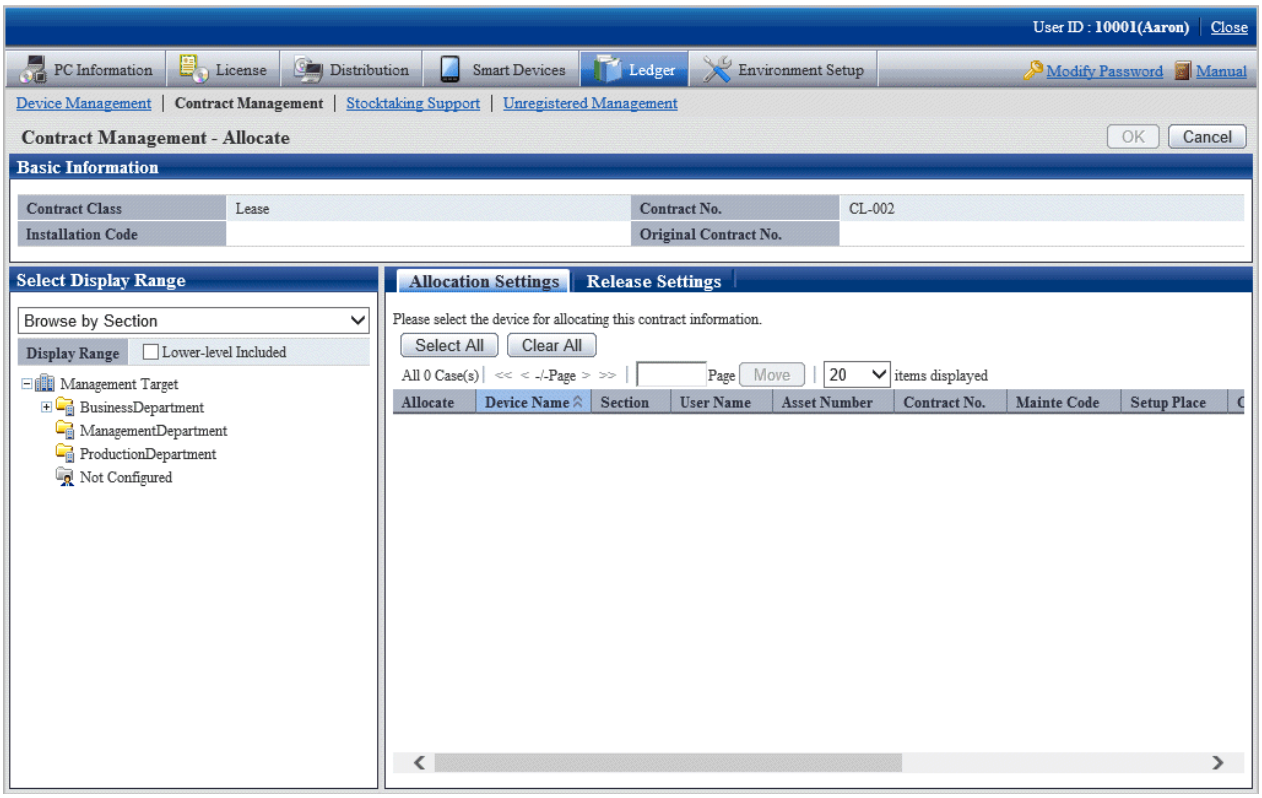
1. Click the **Allocate** button.

   The following window will be displayed

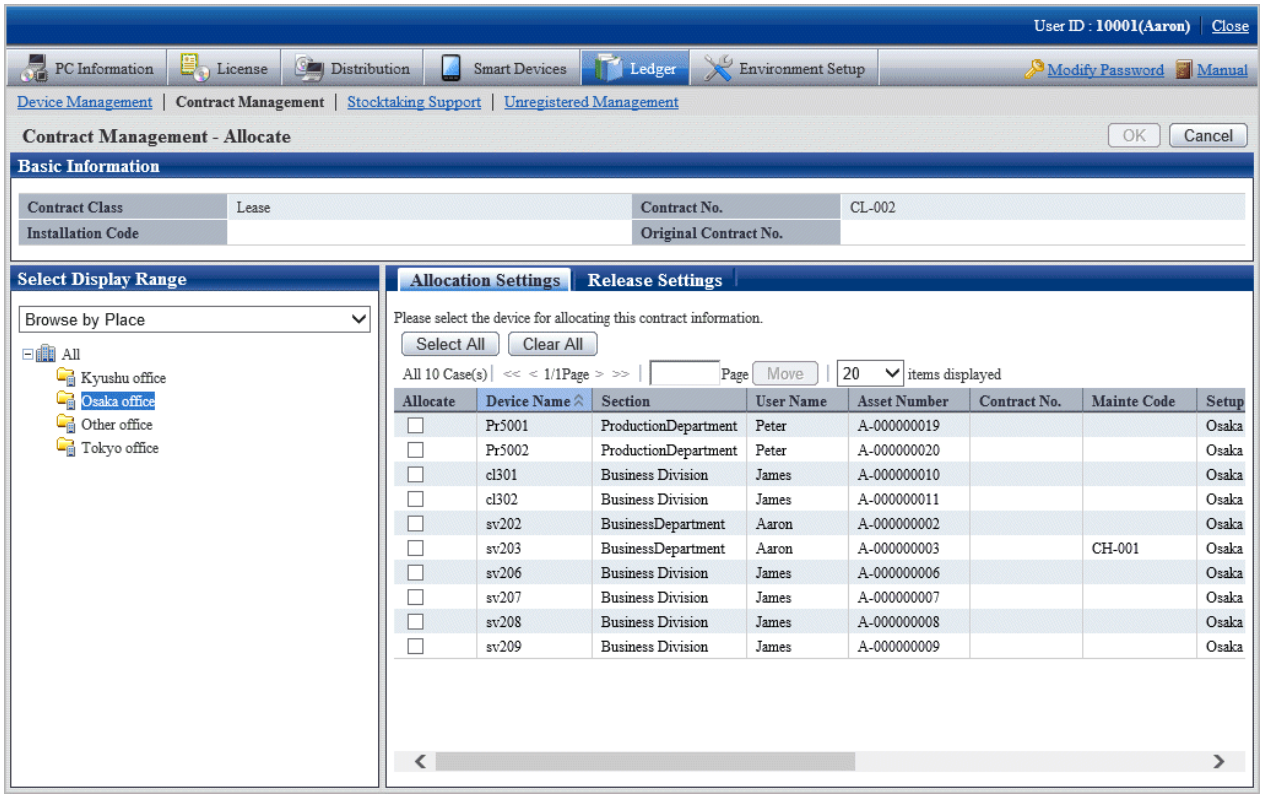


2. Click the **Allocation Settings** tab in the window.

   The following window will be displayed



3. Select the section/setting location/classification/category of the device with distributed contract information through **Select Display Range** in the window. The list of selected device is displayed on the right side.



4. Select the device with distributed contract information, and click **OK** button.

   The device is distributed to contract information.

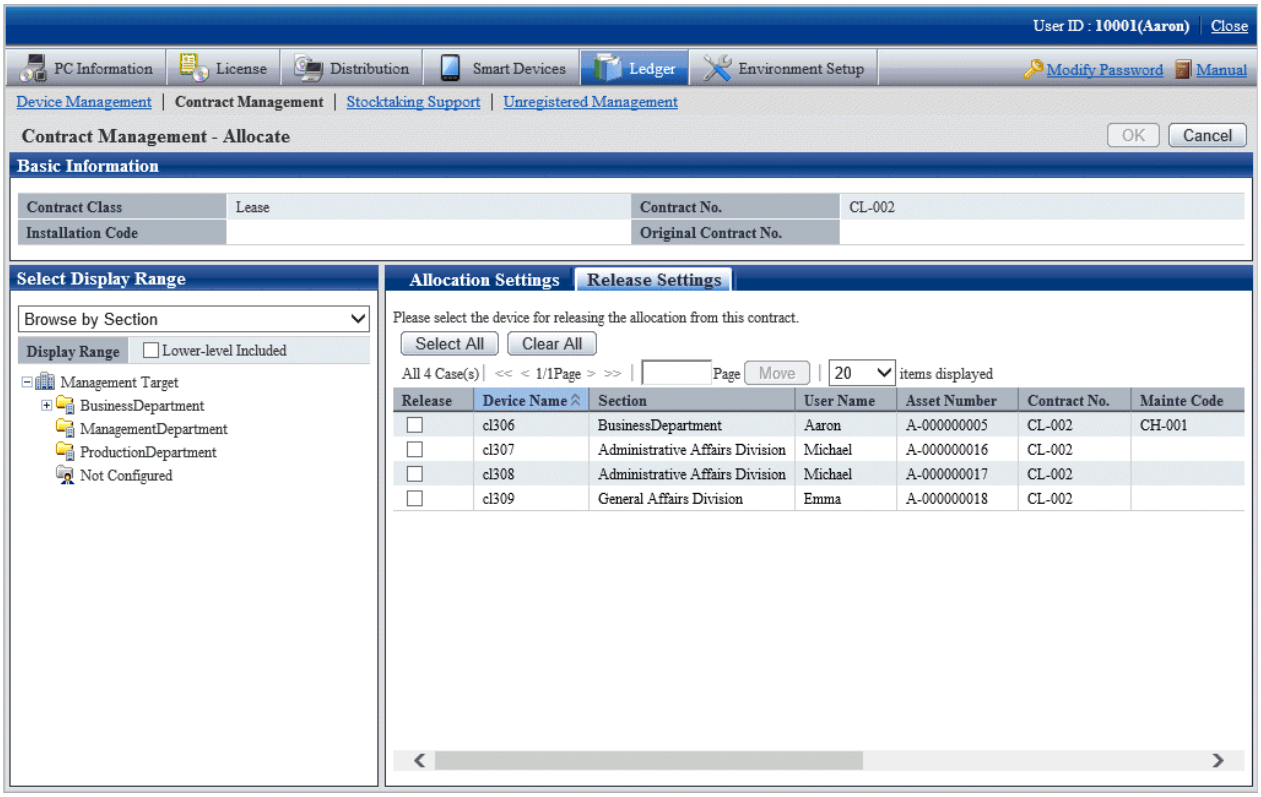
Release the distribution of contract information

The procedure for removing the device information distributed in the registered contract information are as follows.

Besides, by clicking **Allocate** button in "11.4.1.3 Confirm Details of Contract", the procedure are described.

1. Click the **Allocate** button.

   The following window will be displayed



2. Select the device to be removed contract information distribution, and click the **OK** button.

   The distribution of contract information has been removed.

11.4.4 Save Contract Information as Ledger

The following section describes how to save the contract information displayed in window as ledger.

In addition, the ledger saved in EXPORT file format can be registered through "11.2.2 Register/Modify Ledger", and the update information can be unified.

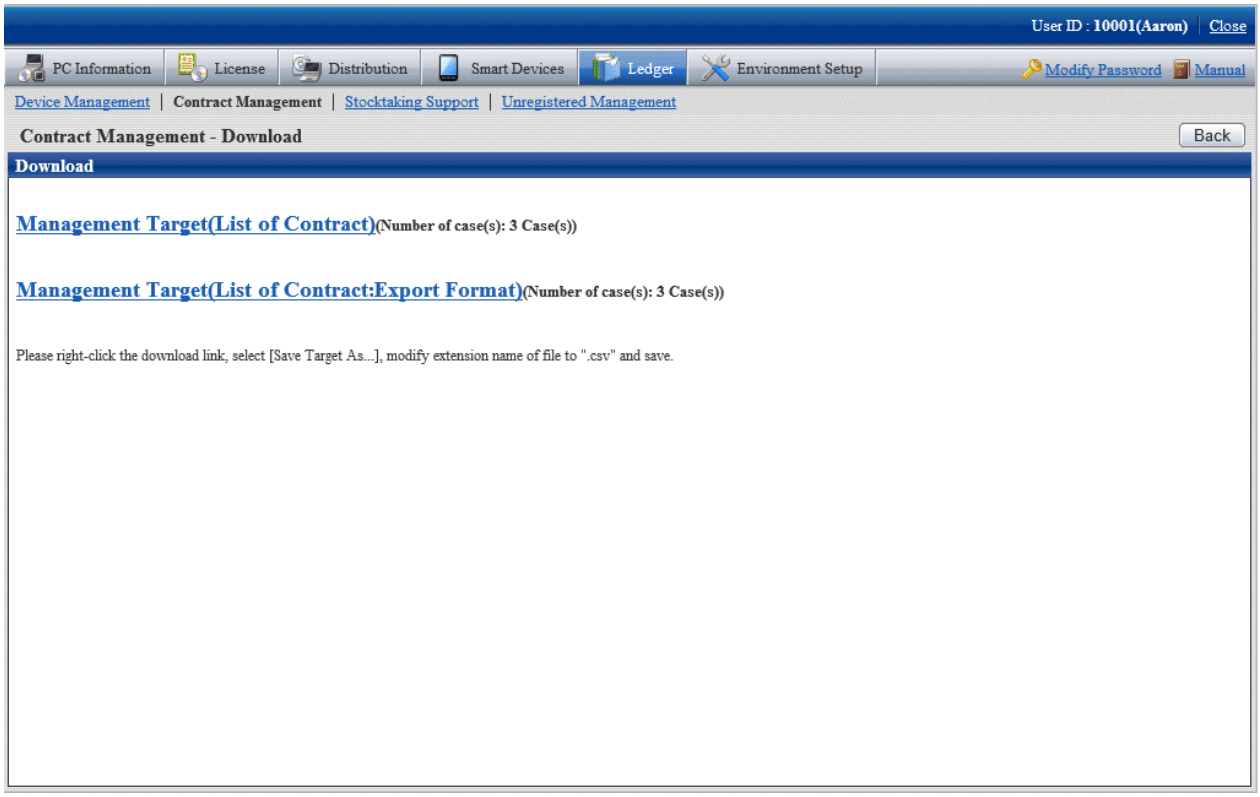
Procedures

The method for saving the contract information displayed in the window as ledger is as follows.

In addition, by clicking the **CSV Export** button in "11.4.1 Confirm Contract Information", it describes the procedure.

1. Click the **CSV Export** button.

   The following window will be displayed



2. Right click the download link, select **Save Target As...**, modify extension of file as '.csv' and save. The following file can be downloaded.

   - CSV file (*.csv)

     Saved as CSV file.

   - EXPORT file (*.csv) (The file can be downloaded in contract list window only.)

     Saved in the format registered in "11.2.2 Register/Modify Ledger".

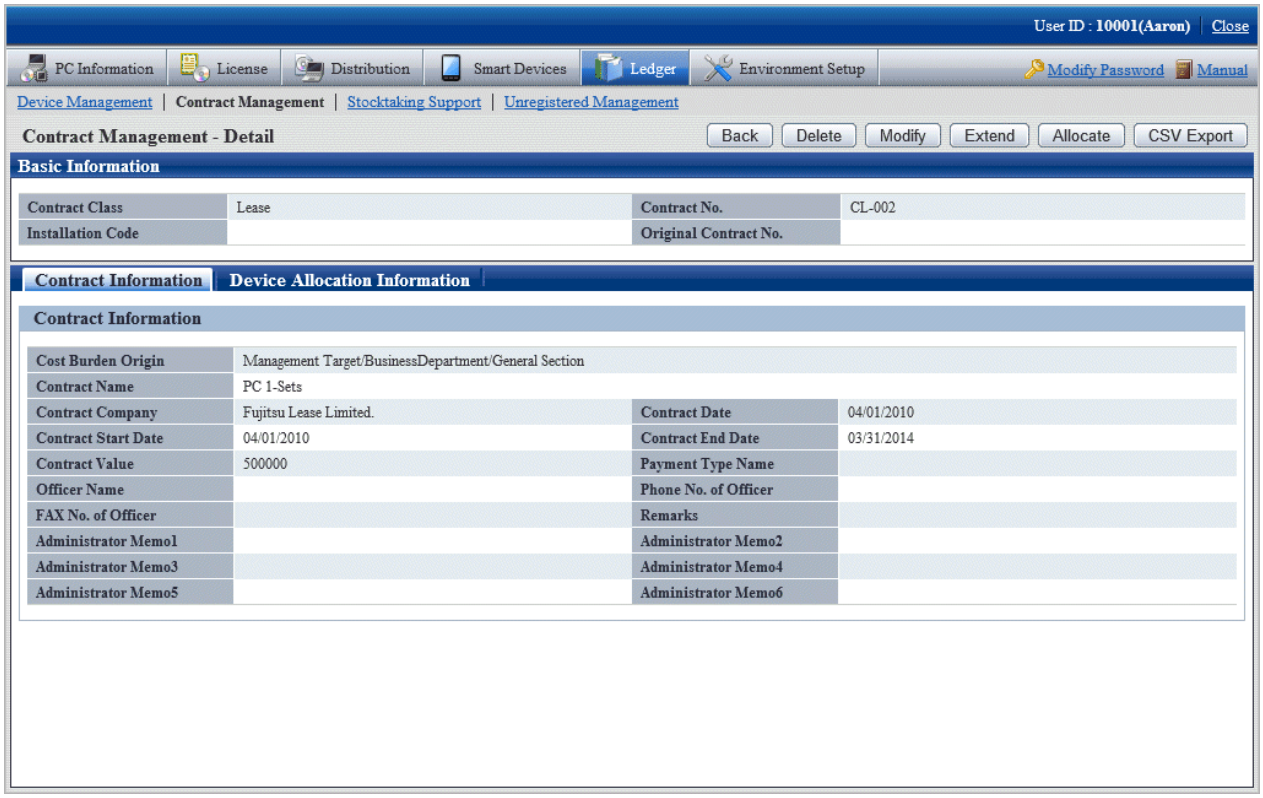
   For the details of save file, refer to "Contract Confirmation File", "Contract List File" or "Details of Contract File" of *Systemwalker Desktop Patrol Reference Manual*.

11.4.5 Extend Contract

The following section describes how to extend the contract.

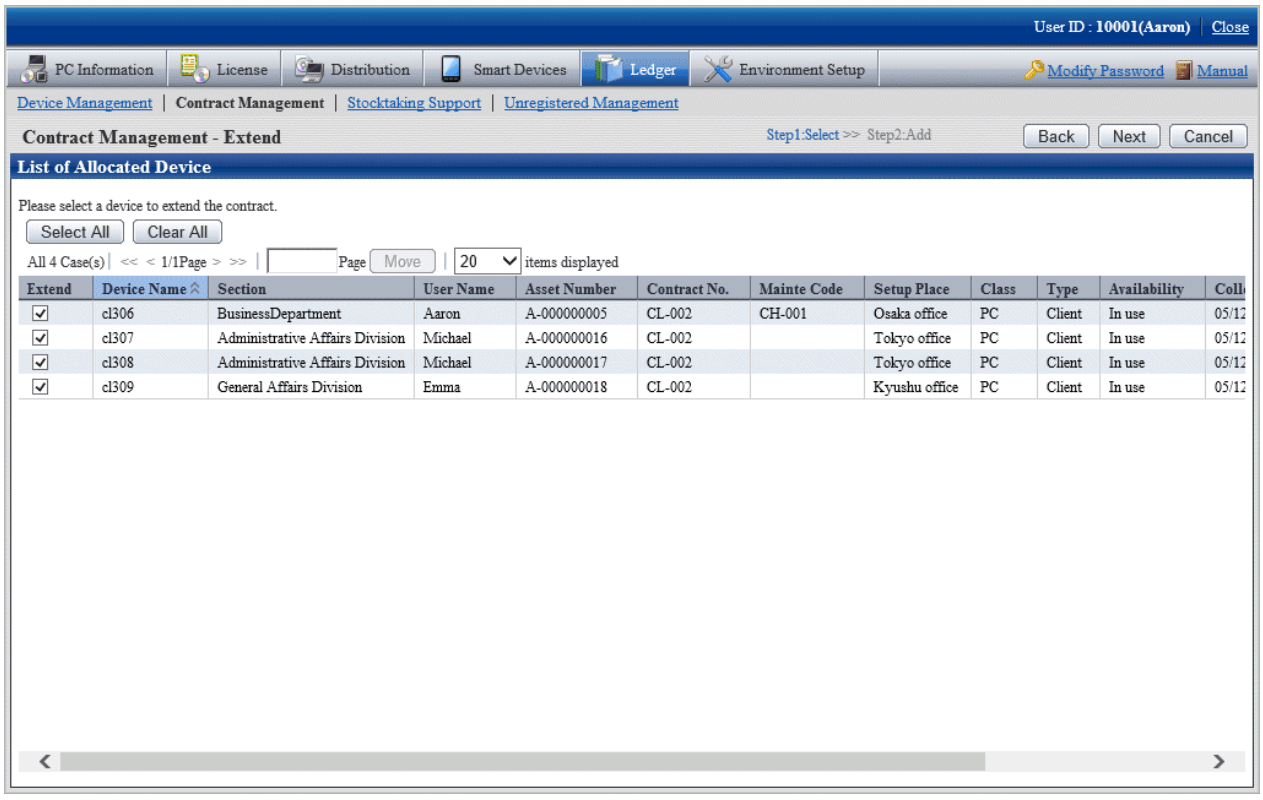
The procedure for extending the contract are as follows. Extending the contract will be the procedure after "11.3.1.3 Confirm Device Details".

1. Display the **Contract Management - Detail** window of extended contract information.



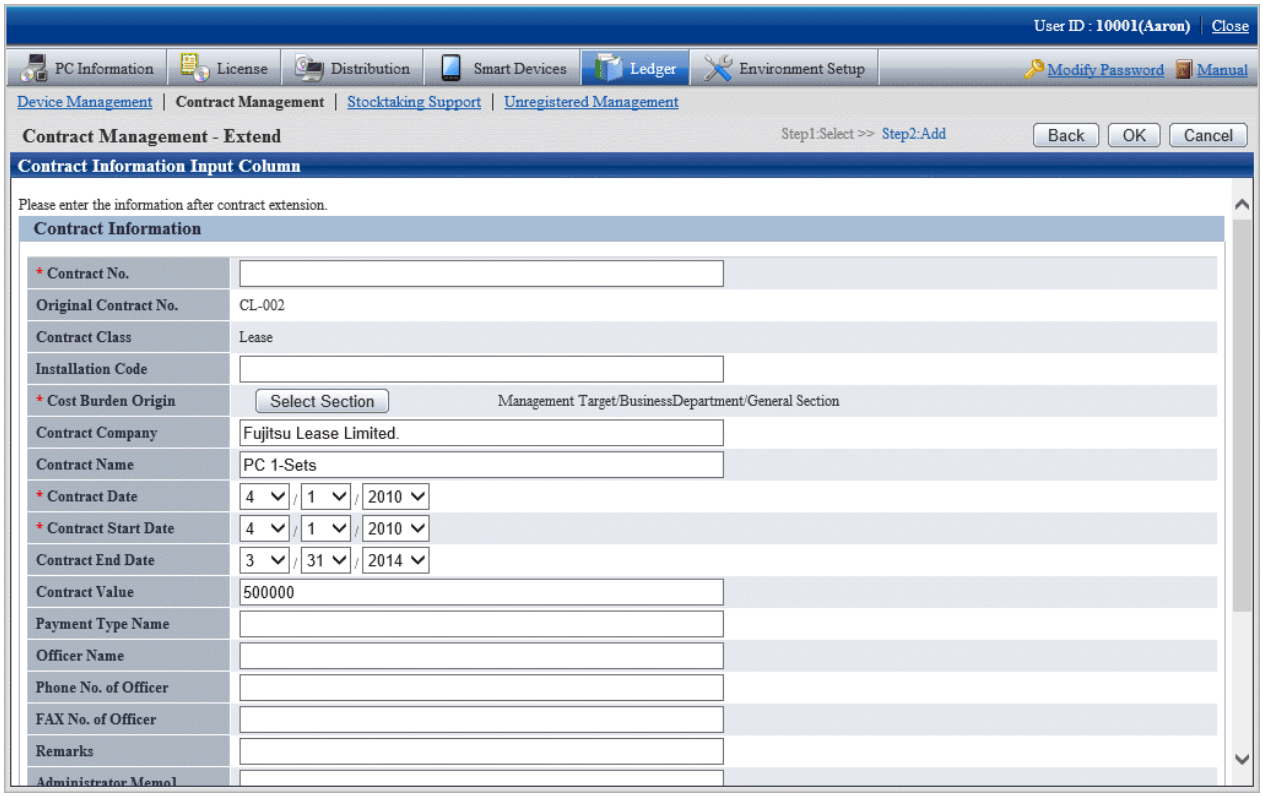
2. Click the **Extend** button.

   The following window will be displayed



3. Select the contract to be extended and click the **Next** button.

   The following window will be displayed



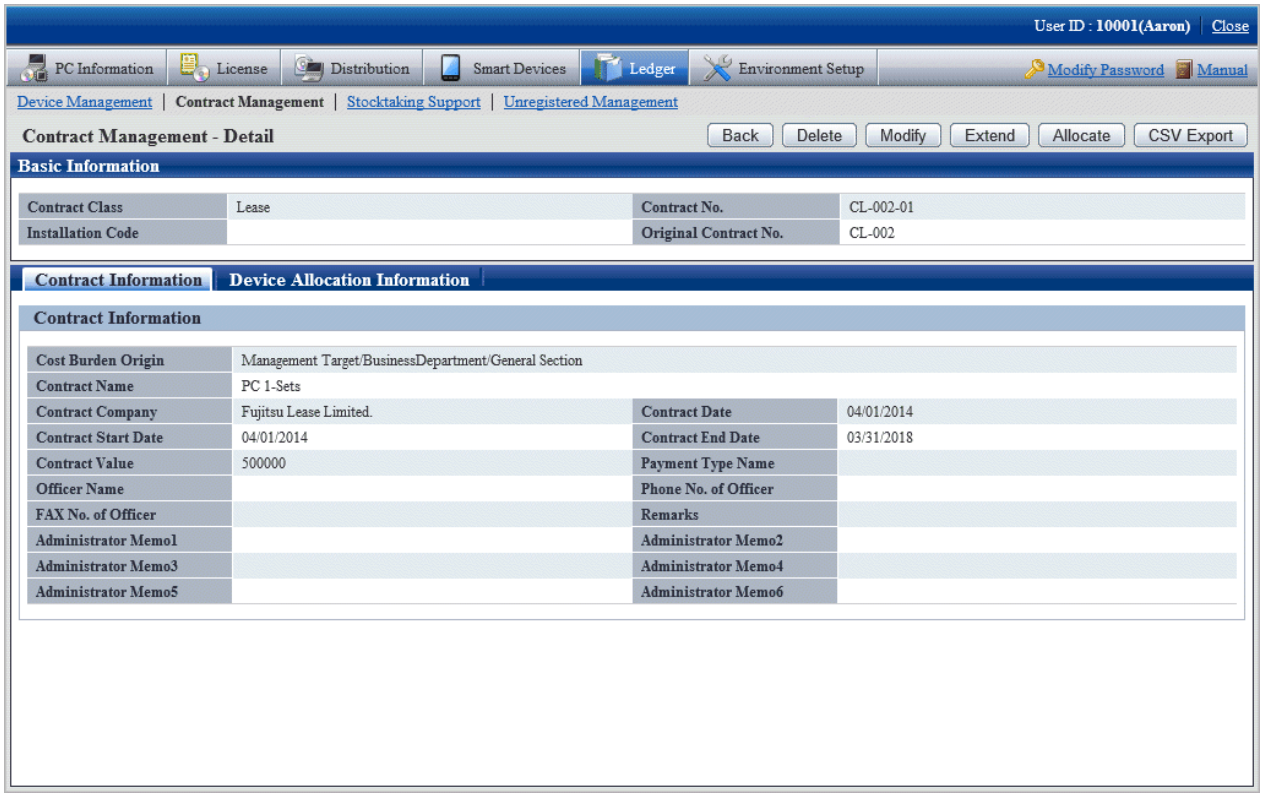
   Set the extended contract information.

   The original contract No. distributed to contract extension device will be registered after being modified as extension contract No. set in this window. The history information at this time will be commented as "Modification through Contract Extension".

4. Click the **OK** button.

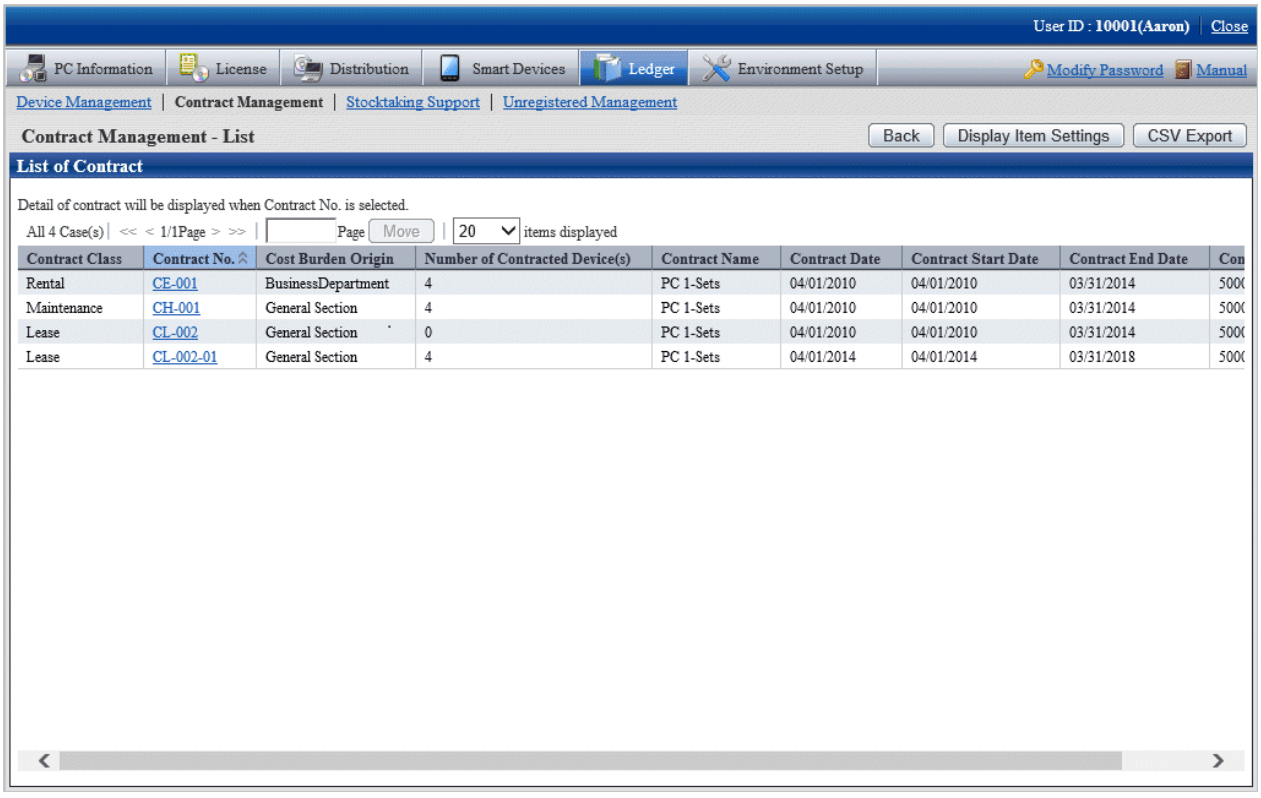
   The following window will be displayed

The contract information after extension will be displayed in the **Contract Management - Detail** window, and confirm the results after extension.



5. The **Contract List** window is displayed after clicking the **Cancel** button through the **Contract Management - Extend** window.

   The original contract information and extended contract information can be confirmed through the **Contract Management - List** window.



Point

About contract that is not extended

The original contract information can be deleted in **Details of Contract** window, and the information of device that is not extended can also be deleted at the same time.

11.5 Stocktaking Support

The following section describes how to use/register the Stocktaking Operation of device (PC and device) to be managed through management ledger.

11.5.1 Confirm Stocktaking Status

For the method for confirming the inventory status of registered device as "By Section", "By Classification" and "By Location", the following items are described in the operation procedure.

- "11.5.1.1 Confirm Various Stocktaking Status"
- "11.5.1.2 Confirm List of Stocktaking"
- "11.5.1.3 Confirm List of Excluded Stocktaking"

11.5.1.1 Confirm Various Stocktaking Status

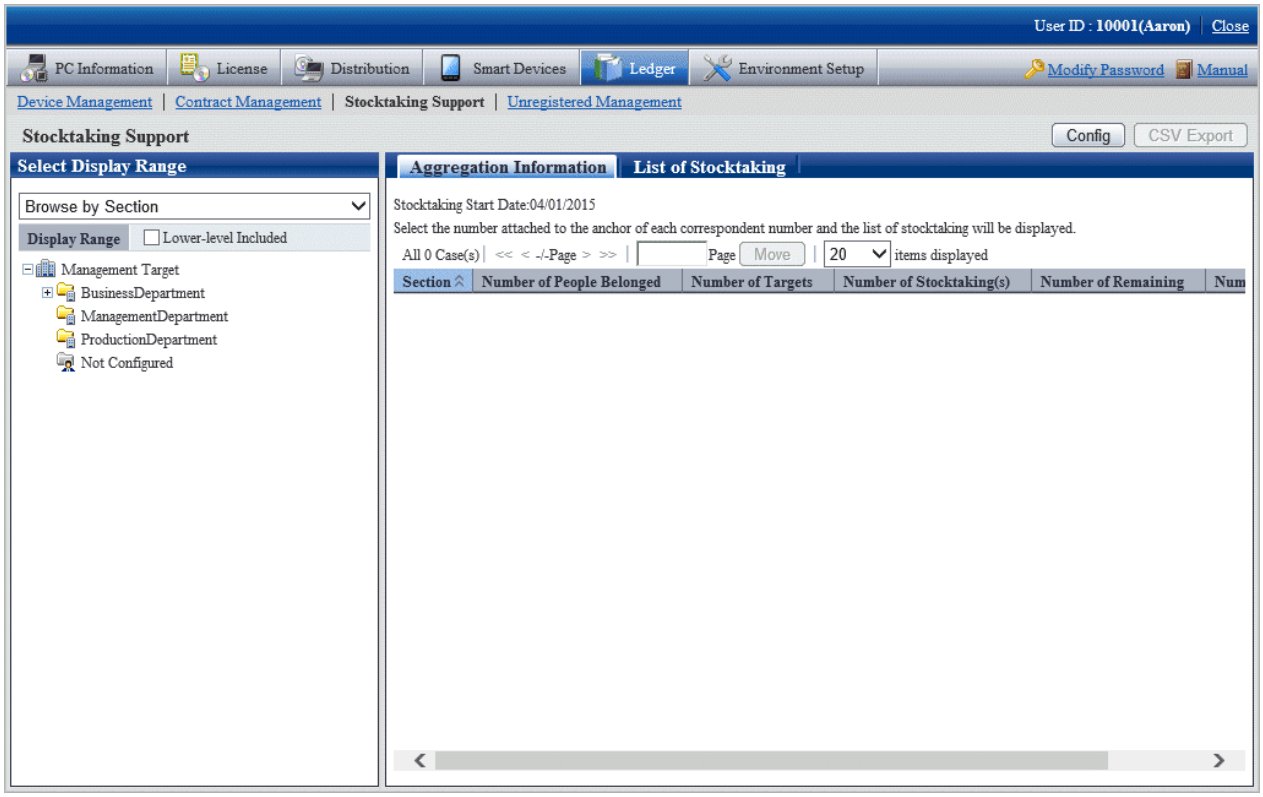
The procedure for confirming the inventory status of various device of "By Section", "By Classification" and "By Location" are as follows:

1. Log onto the main menu, and click **Ledger**.

   The **Ledger** window will be displayed

2. Click **Stocktaking Support**.

   The following window will be displayed



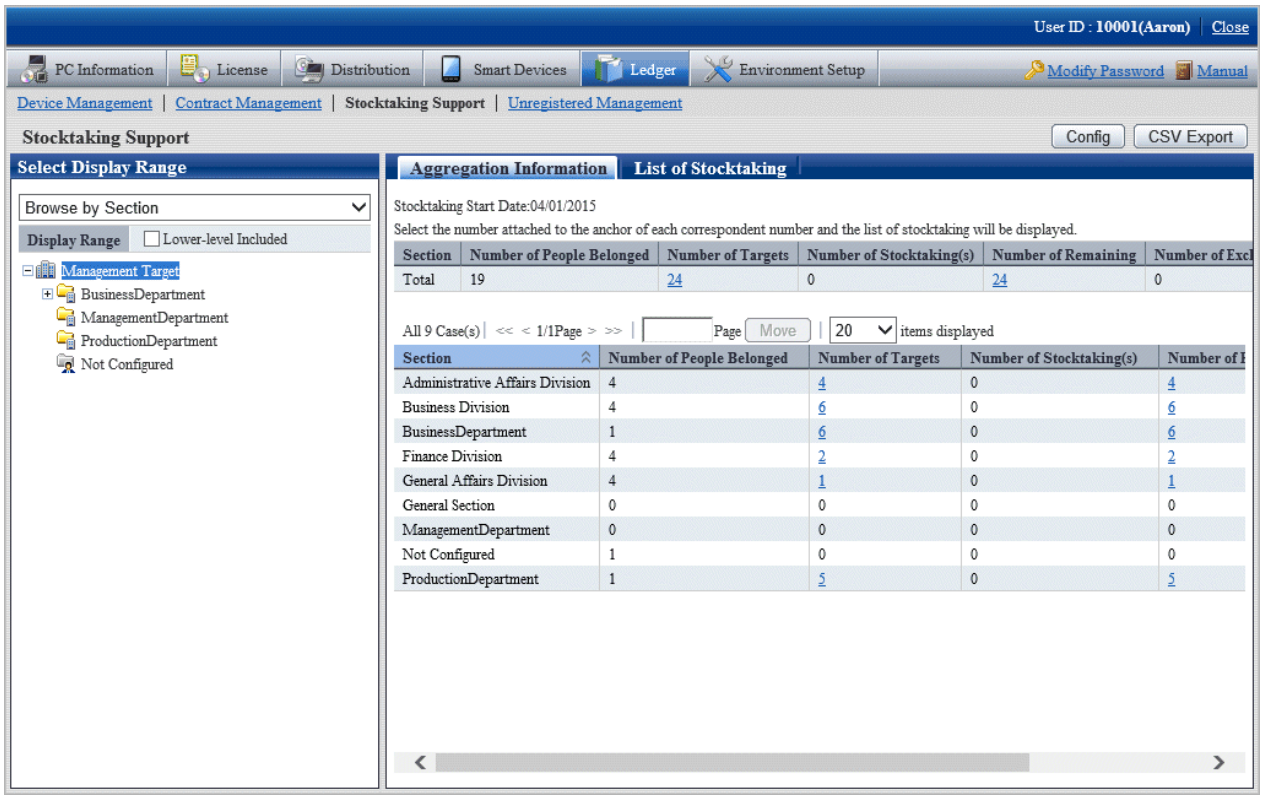
   When it is the first time to perform the inventory support, the message window prompting to set inventory start date will be displayed before the status confirmation window.

   For setting, refer to "11.5.3 Stocktaking Operation".

3. Confirm the inventory status by section.

   According to the drop-down menu on the left side of the window, select **Browse by Section** from the list.

The following window will be displayed



The meaning of each item is as follows:

In addition, it describes the situation of all display item(s).

Item	Descriptions
Section	Section information
Number of People Belonged	Number of users subordinate to the section
Number of Targets	Total number of inventory object device in the section
Number of Stocktaking(s)	Total number of checked device in the section
Number of Remaining	Total number of device that are not checked in the section
Number of Excluded	Total number of non-inventory object device in the section

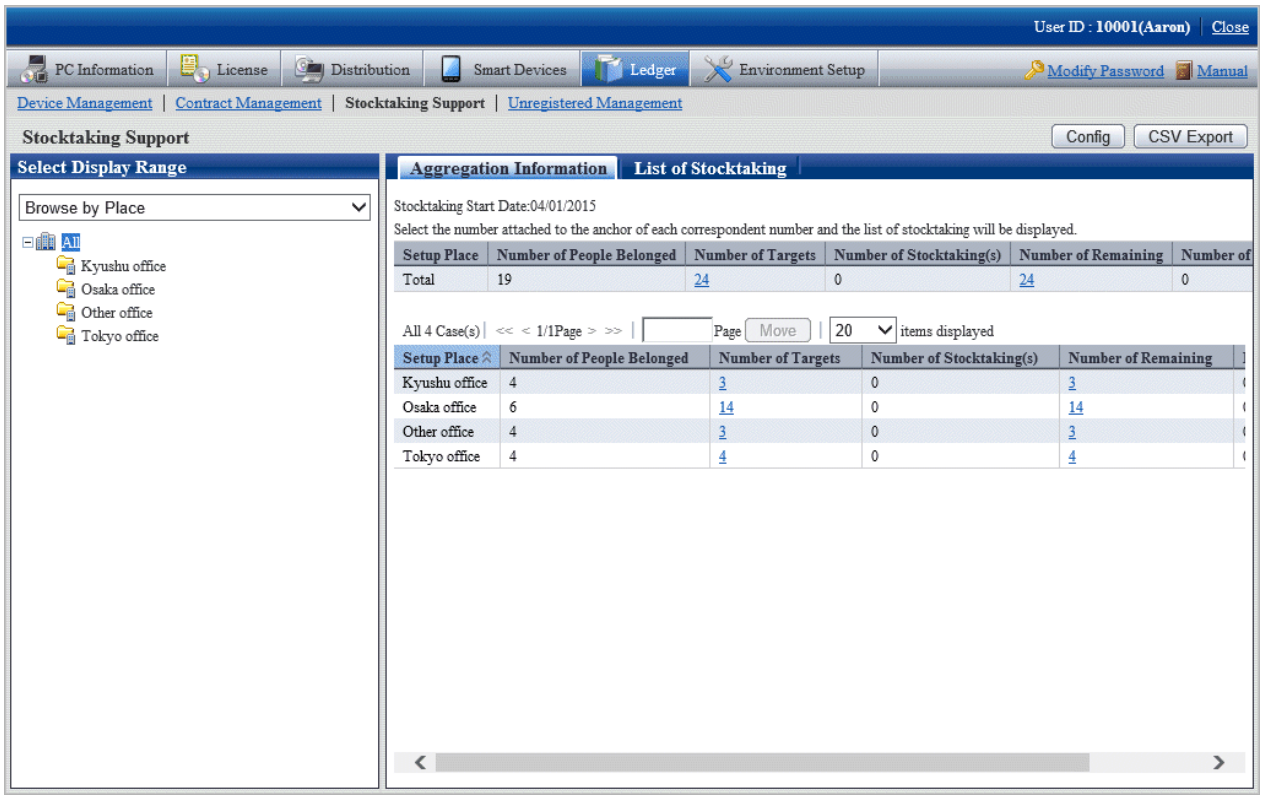
In addition, the action of each button is as follows:

Item	Descriptions
Config	Set the use method of inventory. Refer to "11.5.3 Stocktaking Operation" for details.
CSV Export	Save the information displayed in window as ledger. Refer to "11.5.2 Save Stocktaking Status as Ledger" for details.

4. Confirm the inventory status by location

According to the drop-down menu on the left side of the window, select **Browse by Place** from the list.

The following window will be displayed



The meaning of each item is as follows:

In addition, it describes all display item(s). And the action of button is the same as the above-mentioned inventory confirmation window by section.

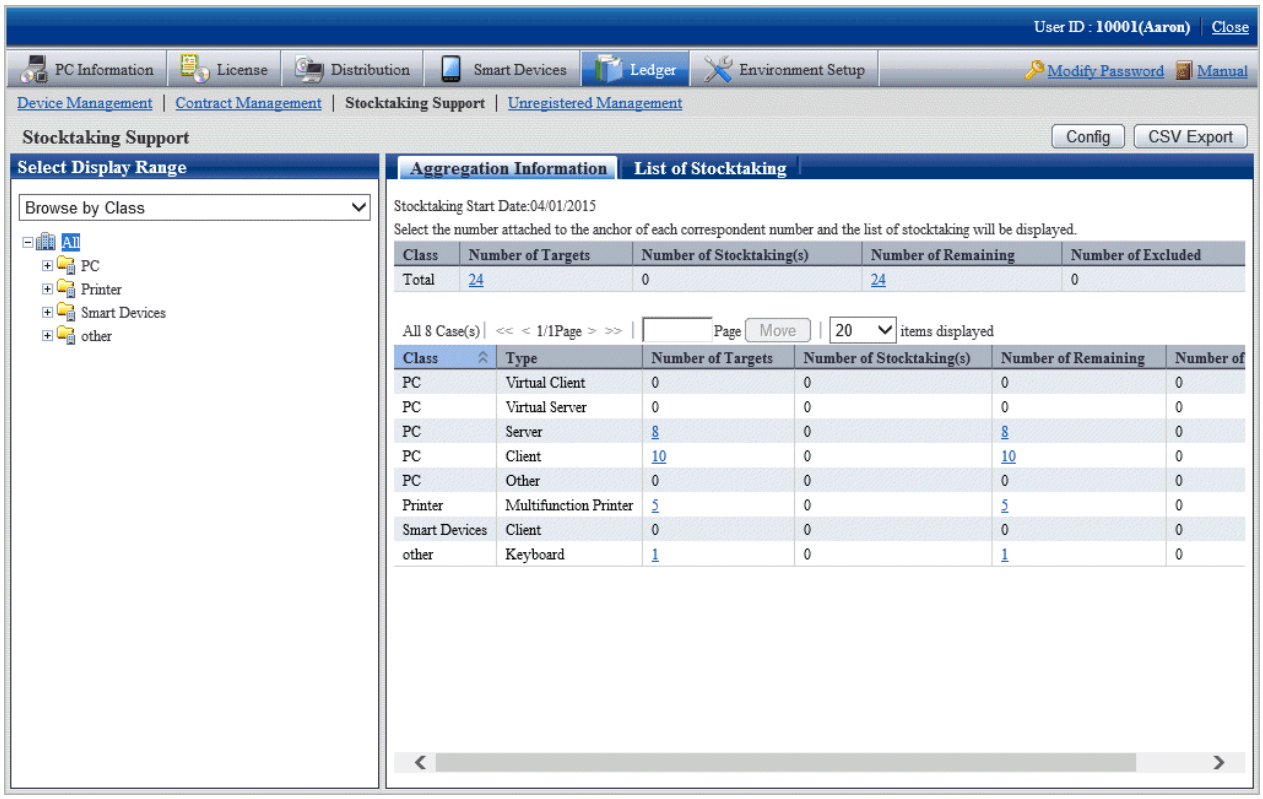
Item	Descriptions
Setup Place	Device setting location.
Number of People Belonged	Number of users subordinate to the setting location,
Number of Targets	Total number of inventory object device in the setting location.
Number of Stocktaking(s)	Total number of checked device in the setting location.
Number of Remaining	Total number of device that are not checked in the setting location.
Number of Excluded	Total number of non-inventory object device in the setting location.

Remarks: When selecting the whole company, the number of the device without setting location will be aggregated in total.

5. Confirm the inventory status by classification.

According to the drop-down menu on the left side of the window, select **Browse by Class** from the list.

The following window will be displayed



The meaning of each item is as follows:

In addition, it describes the situation of all display item(s). And the action of button is the same as above mentioned inventory confirmation window by section.

Item	Descriptions
Class	Device classification information. **Class** information registered as the device information.
Type	Category information of device . **Type** information registered as the device information.
Number of Targets	Total number of inventory object device in classification and category unit.
Number of Stocktaking(s)	Total number of checked device in classification and category unit,
Number of Remaining	Total number of the device that are not checked in classification and category unit.
Number of Excluded	Total number of non-inventory object device in classification and category unit.

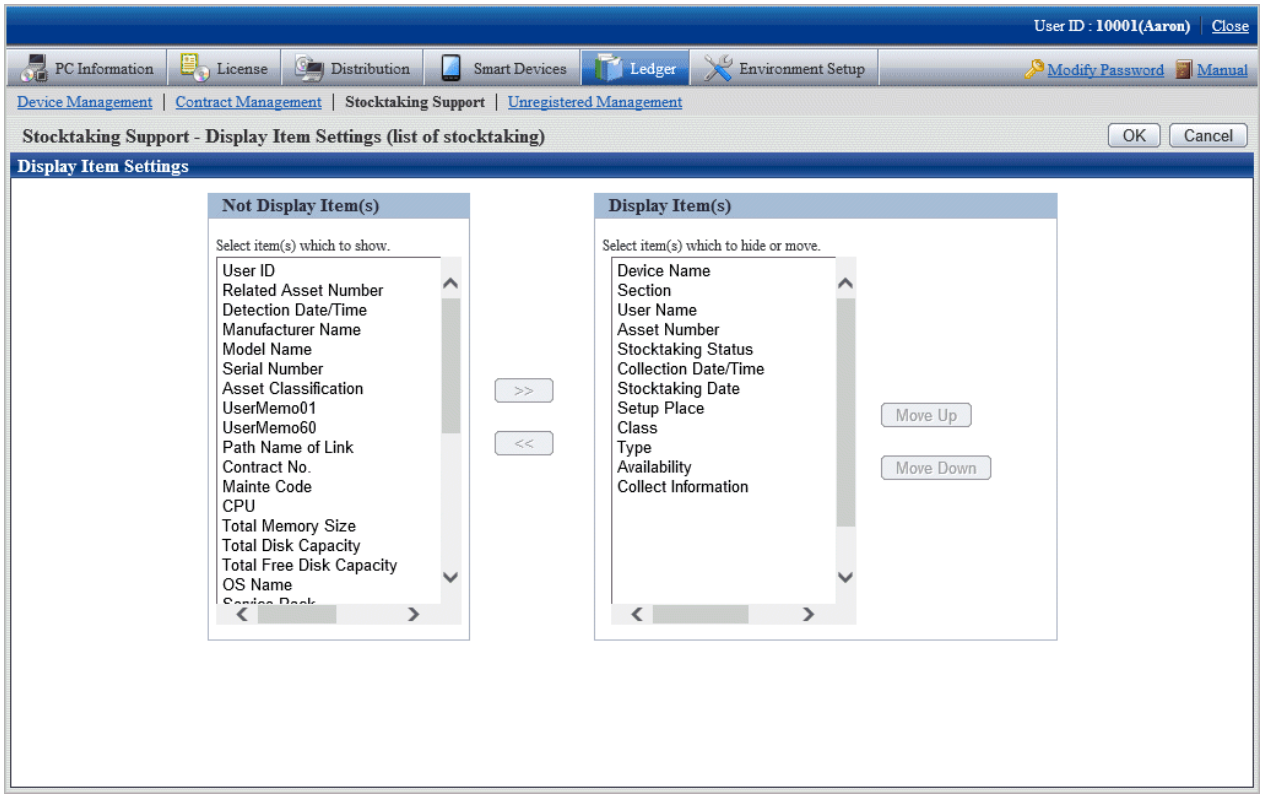
Set display item(s)

The following section describes how to set the items displayed in the window.

1. Click the **Display Item Settings** button.

   The following window will be displayed

In addition, the window when clicking the **Display Item Settings** button in the window for inventory confirmation by section will be displayed.



2. Set displayed item according to the following procedure.

   a. Select items displayed in the inventory list from the **Not Display Item(s)** list on the left side of the window, and click the >> button in the center of the window. Multiple items can be selected.

      The selected item is added to **Display Item(s)** on the right side of the window.

   b. Select items that are not displayed in the inventory list from **Display Item(s)** list on the right side of the window, and click the >> button in the center of the window. Multiple items can be selected.

      The selected item is deleted from **Display Item(s)** on the right side of the window.

   c. When modifying the sequence of **Display Item(s)**, select items from **Display Item(s)** list on the right side of the window, and click the **Move Up** or **Move Down** button.

3. After the setup of displayed item is completed, click the **OK** button.

   The display item(s) of inventory list are added to the set items.

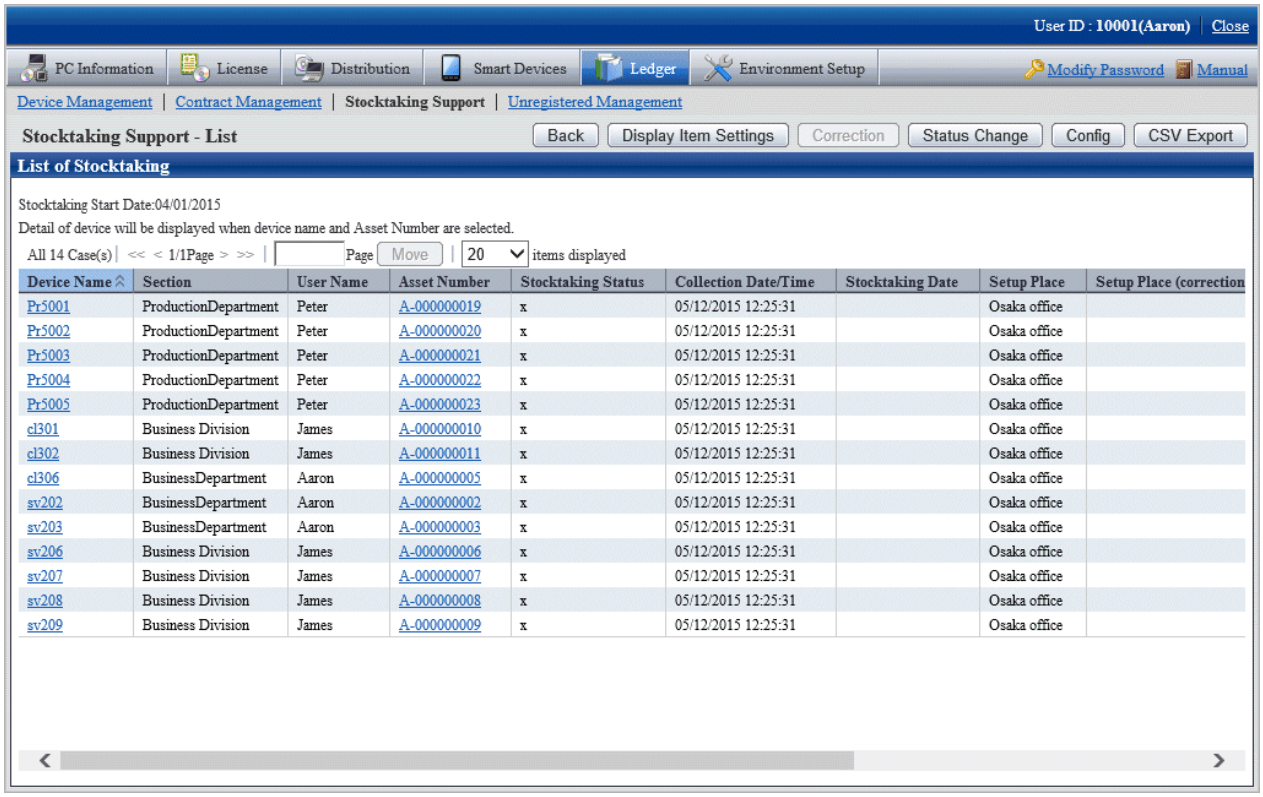
11.5.1.2 Confirm List of Stocktaking

The procedure for confirming each inventory list of "In Section", "In Classification" and "In Location" are as follows:

In addition, it will be the procedure after "11.5.1.1 Confirm Various Stocktaking Status". In addition, the procedure will be described according to the "In Section" window. The sequences of items respectively displayed in "In Classification" and "In Location" are different, but can be confirmed through the same procedure.

1. Click the numeral value of items (**Number of Targets**, **Number of Stocktaking(s)**, **Number of Remaining**) to be confirmed.

   The following window will be displayed



2. Confirm the contract list of selected items.

   Confirm the following information.

   It describes the situation of all display item(s).

Item	Descriptions
Section	Section information
User ID	ID of user that uses the machine **User ID** information registered as the device information.
User Name	Name of user that uses the machine
Asset Number	Asset management number of device **Asset Number** information registered as the device information.
Related Asset Number	Asset management number related to the machine **Related Asset Number** information registered as the device information.
Stocktaking Status	Device inventory status **o** indicates a device whose inventory is completed, and **x** indicates a device whose inventory is not completed.
Collection Date/ Time	Date and time for collecting information
Detection Date/ Time	Date and time for detecting the device through ADT
Stocktaking Date	Date and time for completing inventory
Setup Place	Device setting location information

Item	Descriptions
Setup Place (correction value)	Setting location information gotten from the device network segment information. The displayed contents are as follows: - **Display Exists** (Display Setting Location Name Confirmed through IP Address) When there is difference between network segment information and setting location - **No Display** When the network segment information matches set location, or there is no network segment information - ***Network segment information is not set** Though it is the detected network segment, but when the set location of network segment information is not set * This item will be displayed when **Display Rectification Result of Set Location in Inventory List Window** is selected in **Set Inventory Use** only.
Class	Device classification information **Class** information registered as the device information.
Type	Device category information **Type** information registered as the device information.
Availability	Device operating status **Usage Status** information is registered as the device information.
Device Name	Name of the machine **Device Name** information registered as the device information.
Manufacturer Name	Device manufacturer name **Manufacturer Name** information registered as the device information.
Model Name	Device Model Name **Model Name** information registered as the device information.
Serial Number	Device serial number **Serial Number** information registered as the device information.
Asset Classification	Asset classification of device **Asset Classification** information is registered as the device information.
User Memo from 1 to 60	Inherent information of device **User Memo from 1 to 60** information registered as the device information.
Path Name of Link	Data related to the device (for example, device image) or these input directories and URL. **Path Name of Link Target** information registered as the device information.
Contract No.	Contract number information **Contract No.** information registered as the device information.
Maintenance Code	Maintenance code of device **Maintenance Code** information registered as the device information.
CPU	CPU Clock Speed of PC

Item	Descriptions
Total Disk Capacity	Total disk capacity of PC
Total Free Disk Capacity	Available disk capacity of PC
Total Memory Size	Total memory capacity of PC
OS Name	OS name of PC
Service Pack	Service Pack applied in PC
IP Address 1	IP address set in PC - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/). - IPv6 addresses are separated with a semicolon (;).
IP Address 2	IP address set in PC - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/). - IPv6 addresses are separated with a semicolon (;).
MAC Address 1	MAC address set in PC
MAC Address 2	MAC address set in PC
Date of Manufacture	Device date of manufacture
Date of Registration	Date for registering to the device asset ledger
Collect Information	Indicate whether PC Inventory information exists. **o** indicates PC Inventory information exists, and **x** indicates PC Inventory information does not exist. Inventory information is deleted manually, it will also be displayed as **x**.
Inherent Item of User Definition	As Inventory information, user sets the inherent information arbitrarily. The user will be displayed as set item and inherent information. For example, after user has set **Property Number**, it will be displayed as **Property Number**.

In addition, the action of each button is as follows:

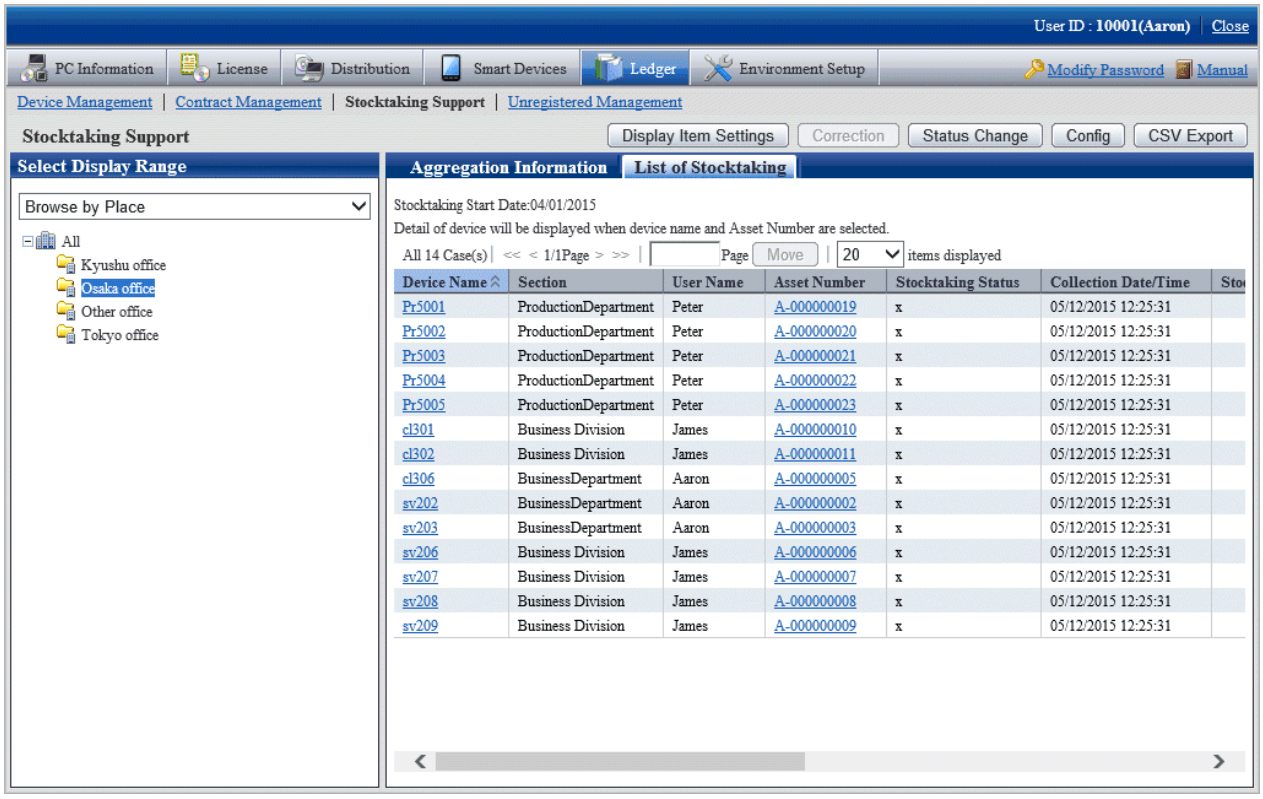
Item	Descriptions
Back	Display the previous window.
Display Item Settings	Set the items displayed in the window. Refer to "Set display item(s)" for details.
Correction	Rectify the setting location. If **Display** is selected for **Correction Result of Setup Place** is not selected in **Stocktaking Support** - **Config**, this button is invalid. Refer to "11.5.3 Stocktaking Operation" for details.
Status Change	Modify the inventory status of device . Refer to "11.5.3 Stocktaking Operation" for details.
Config	Set the method for using the inventory.

Item	Descriptions
	Refer to "11.5.3 Stocktaking Operation" for details.
CSV Export	Save the information displayed in window as ledger. Refer to "11.5.2 Save Stocktaking Status as Ledger" for details.

In addition, the inventory list can be confirmed according to the following procedure. Operate when confirming by section.

1. Click the **List of Stocktaking** tab.

   The following window will be displayed



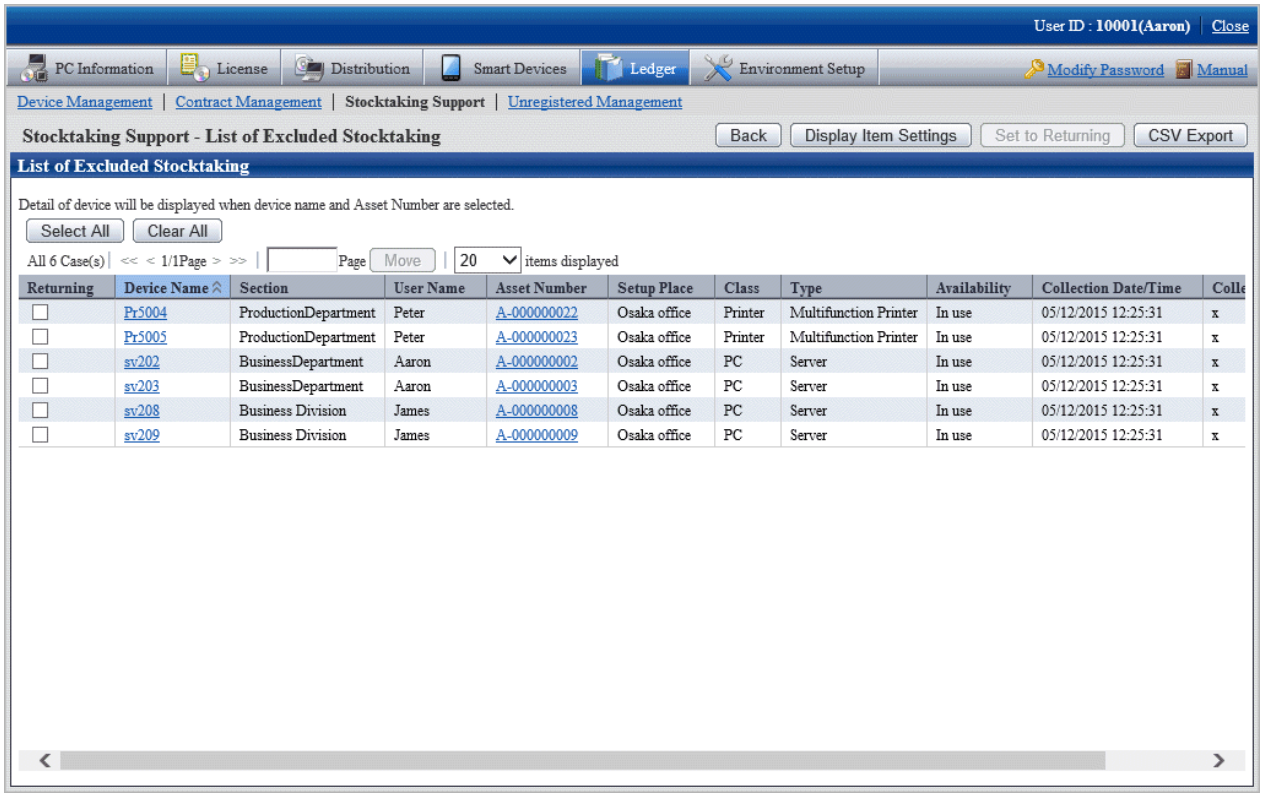
11.5.1.3 Confirm List of Excluded Stocktaking

The procedure to confirm the non-inventory object list are as follows.

In addition, it will be the procedure after "11.5.1.1 Confirm Various Stocktaking Status".

1. Click the numeral value of **Number of Non-inventory Object**.

   The following window will be displayed



2. Confirm the non-inventory object list.

   For the descriptions of each item, refer to "11.5.1.2 Confirm List of Stocktaking".

   In addition, the action of each button is as follows:

Item	Descriptions
Back	Display the previous window.
Display Item Settings	Set the items displayed in the window. Refer to "Set display item(s)" for details.
Set to Returning	Set the selected device as inventory object. Refer to "11.5.3 Stocktaking Operation" for details.
CSV Export	Save the information displayed in the window as ledger. Refer to "11.5.2 Save Stocktaking Status as Ledger" for details.

11.5.2 Save Stocktaking Status as Ledger

The following section describes how to save the inventory status displayed in window as ledger.

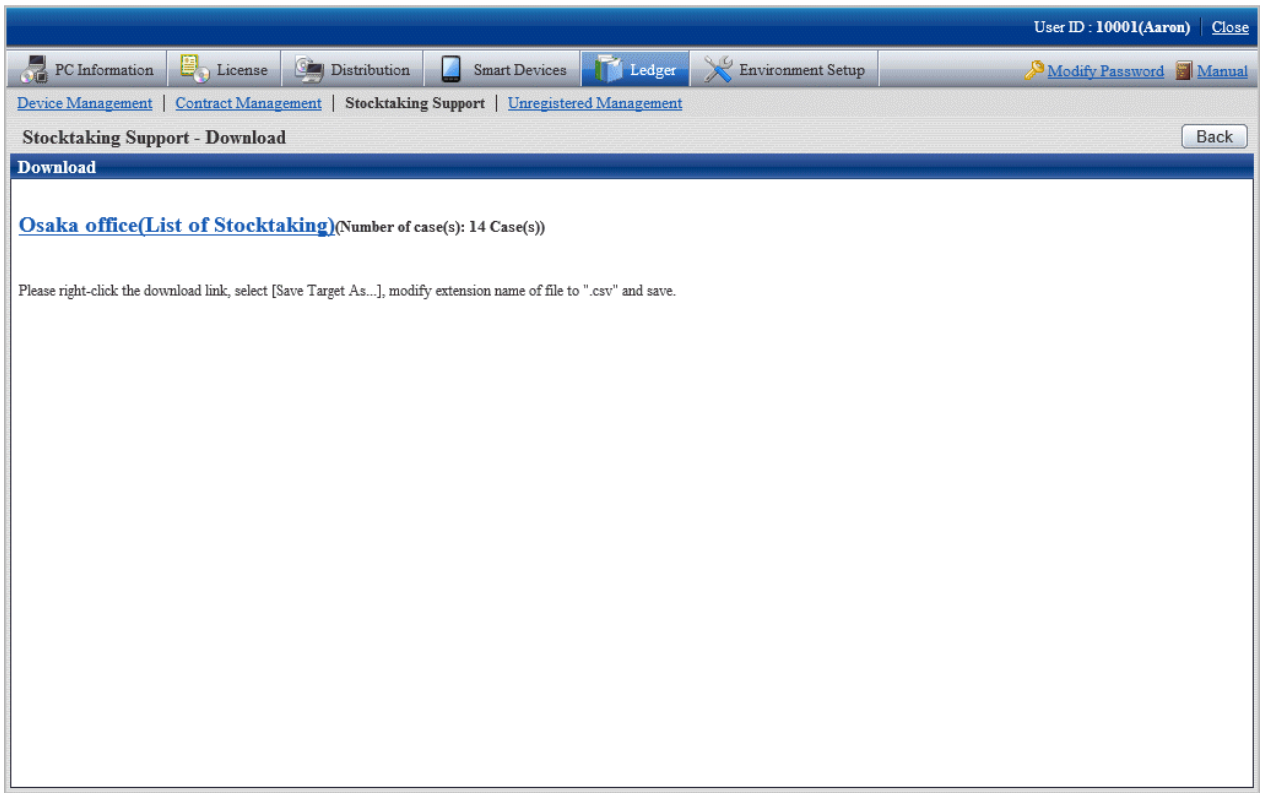
Procedures

The procedures to save the inventory status as ledger are as follows.

In addition, by clicking **CSV Export** button in "11.5.1 Confirm Stocktaking Status", the procedures are described.

1. Click the **CSV Export** button.

   The following window will be displayed



2. Right click the download link, select **Save Target As...**, modify extension of file as '.csv' and save. The following file can be downloaded.

   - CSV file (*.csv)

     Saved as CSV file.

   For the details of saved files, refer to "Inventory Confirmation File", "Inventory Object List" or "Non-inventory Object List" of *Systemwalker Desktop Patrol Reference Manual*.

11.5.3 Stocktaking Operation

The following section describes the Stocktaking Operation of management device in management ledger.

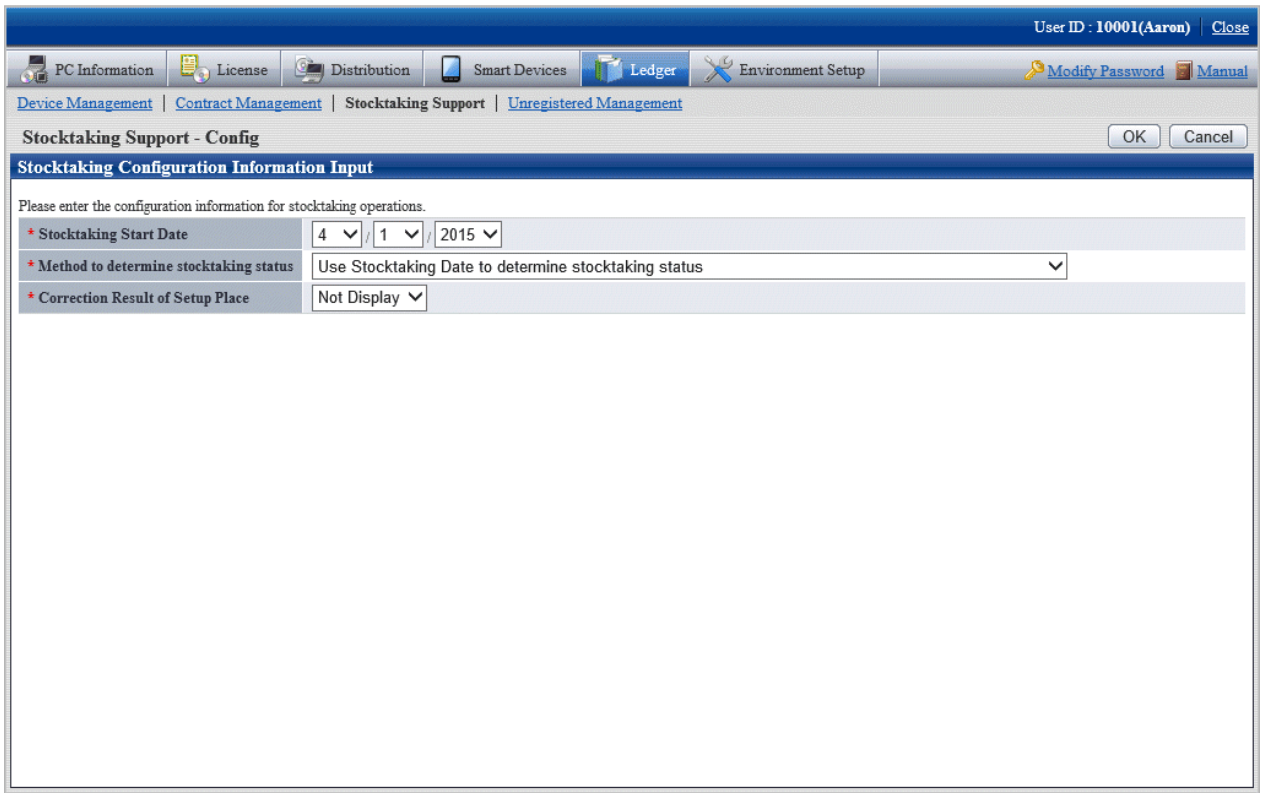
Procedures

The procedures for Stocktaking Operation are as follows.

In addition, by clicking the **Config** button, the procedures are described.

1. Click the **Config** button.

   The following window will be displayed



2. Set the use method of inventory.

   Set the following information and click the **OK** button.

Item	Descriptions
Stocktaking Start Date	Set Inventory start date. It can be set between 180 days earlier than current date and the current date. The Stocktaking Operation between start date and current date has been checked. In addition, the configuration value will be used as initial value of report output inventory status. Refer to "13.3 Output Stocktaking Status" for details.
Method to determine stocktaking status	Set the method for judging the inventory status. - **Use Stocktaking Date to determine stocktaking status** Judge the inventory status only based on stocktaking end date (**o**, **x**). After the inventory start date, when the inventory is completed in stocktaking end date and time, the inventory status will be o (completed). - **Use Stocktaking Date and Collection Date/Time to determine stocktaking status** After selecting this item, including the date and time to pass automatic collection of CT, the item will be used when checking the inventory existence. Judge the inventory status based on date and time of inventory completion and collection (**o**, **x**). After the specified inventory start date,

Item	Descriptions
	when the inventory is completed at certain date and time, the inventory status will be **o** (completed) when the inventory has been made. - **Use Stocktaking Date, Collection Date/Time and Detection Date/ Time to determine stocktaking status** After selecting this item, including the date and time to pass automatic collection of CT, the item will be used when checking the inventory existence. Based on the same priority of stocktaking end date and time, collection date and time and detection date and time, judge the inventory status (**o**, **x**). After the specified inventory start date, when the inventory is completed at certain date and time, the inventory status will be **o** (completed) when the inventory has been made.
Correction Result of Setup Place	When the rectification results of setting location has been displayed in inventory list window, select **Display**, and when it is not displayed, select **Not Display**. After selecting **Display**, in the setting location item of each inventory list window, the rectified setting location will be displayed.

After modifying **Method to determine stocktaking status**, the **Stocktaking Status** (inventory is completed or not completed) of device executing the Stocktaking Operation automatically will be modified.

But the **Stocktaking Status** of device executing the Stocktaking Operation through the following operations cannot be modified.

- Stocktaking Operation executed manually

The start date of facility will be set.

3. Perform inventory task.

   Operate according to the following situations.

   - "Inventory task performed manually"

     It is the inventory task performed through window operations.

     When performing the inventory task manually, it should be set as **Use Stocktaking Date to determine stocktaking status** in **Method to determine stocktaking status** through the **Stocktaking Support - Config** window.

   - "Inventory task performed automatically"

     It is the inventory task performed automatically.

     When performing the inventory task automatically, excluding **Use Stocktaking Date to determine stocktaking status** should be set in **Method to determine stocktaking status** through the **Stocktaking Support - Config** window.

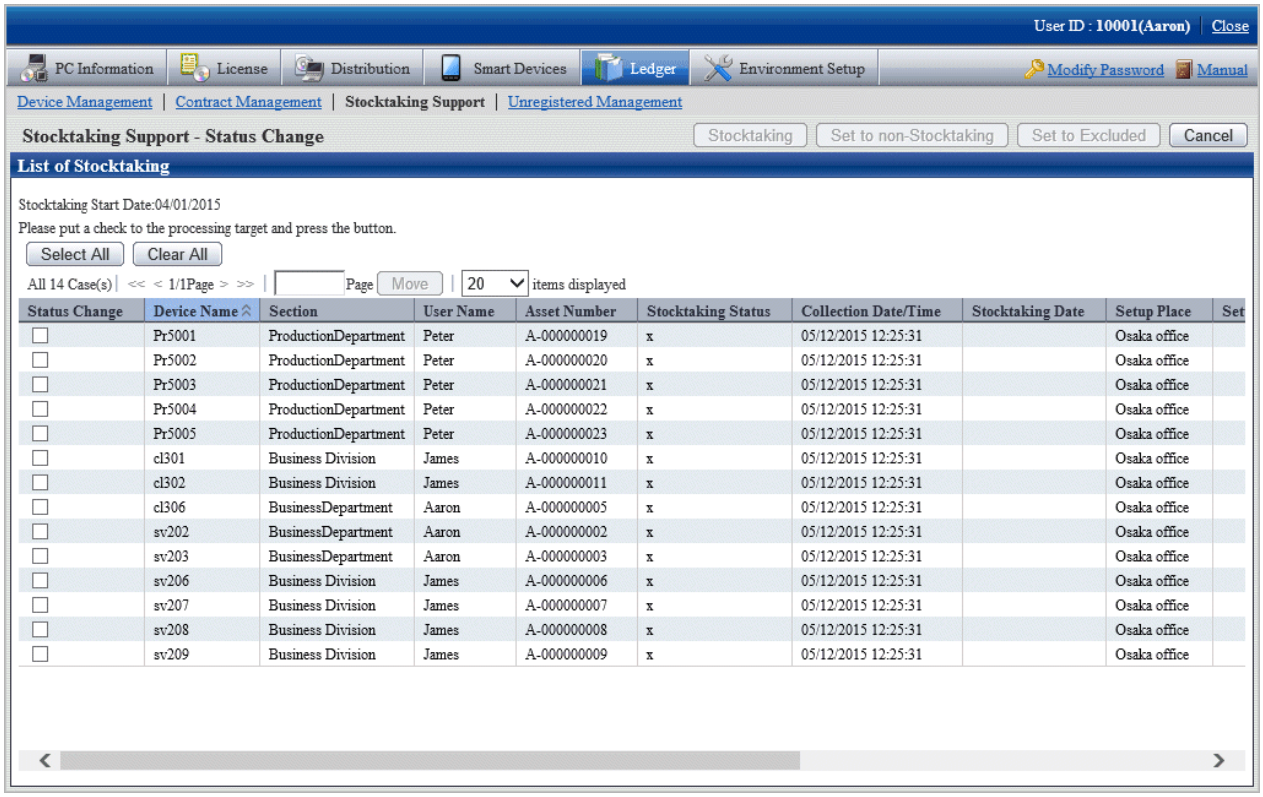
     Besides, "Inventory task performed manually" can also be performed at this time.

Inventory task performed manually

It is described by displaying the operations in the window in "11.5.1.2 Confirm List of Stocktaking".

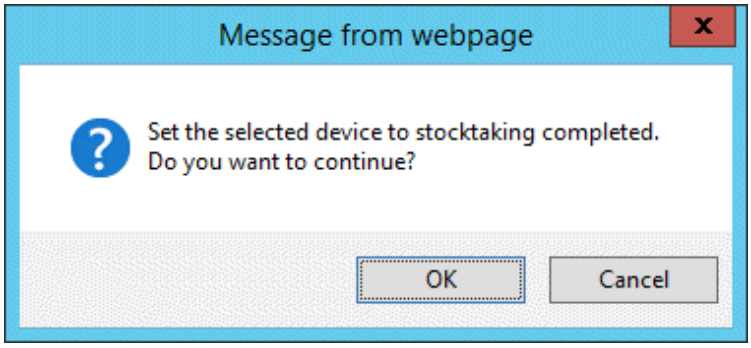
1. Click the **Status Change** button.

   The following window will be displayed



2. Select the device which has been made an inventory and click the **Stocktaking** button.

   The following window will be displayed



3. Set the device as inventory made.

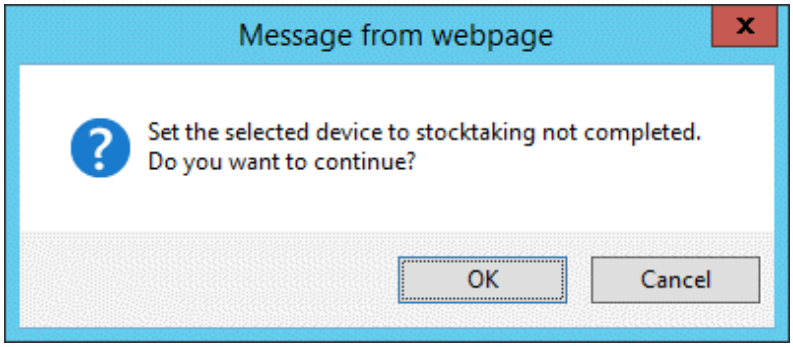
   Click the **OK** button.

   Stocktaking Status is changed from **x** to **o**.

   Besides, the date and time when clicking **OK** in **Stocktaking Date** is set.

4. Select the device which has not completed inventory, click the **Set to non Stocktaking** button.

   The following window will be displayed



5. Set the device as inventory not completed.

   Click the **OK** button.

   Stocktaking Status is changed from **o** to **x**.

6. Delete the device from the inventory object.

   Select the device deleted from the inventory object and click the **Set to Excluded** button.

   It is deleted from the list of inventory object.

   The deleted device is moved to the **List of Excluded Stocktaking** window.

7. Take the device deleted from the inventory object as inventory object.

   This part is described by displaying the operations in the window in "11.5.1.3 Confirm List of Excluded Stocktaking".

   Select the device deleted from the inventory object and click the **Set to Returning** button.

   It is deleted from the list of non inventory object.

   The deleted device is moved to the **List of Stocktaking** window.

Inventory task performed automatically

Take Inventory information collected in Systemwalker Desktop Patrol as the asset information (device information) managed by management ledger to register or modify it.

PC registered or modified after **Stocktaking Start Date** set in the **Stocktaking Support - Config** window will be set as inventory made.

For how to confirm the inventory status, refer to "11.5.1 Confirm Stocktaking Status".

The result of the inventory task performed automatically will be displayed in **List of Stocktaking**.

When **Display** is selected for **Correction Result of Setup Place**, the setting location (rectified value) will be displayed following the item of the setting location. The content displayed in the setting location (rectified value) is as follows:

Get the setting location information from the network segment information of the machine. The displayed content is as follows:

- **Displayed** (Setting Location Name Confirmed by IP Address is Displayed)

  When the network segment information and the setting location do not match

- **Not Displayed**

  When the network segment information matches the setting location or the network segment information does not exist

- ***Network Segment Information is not Set**

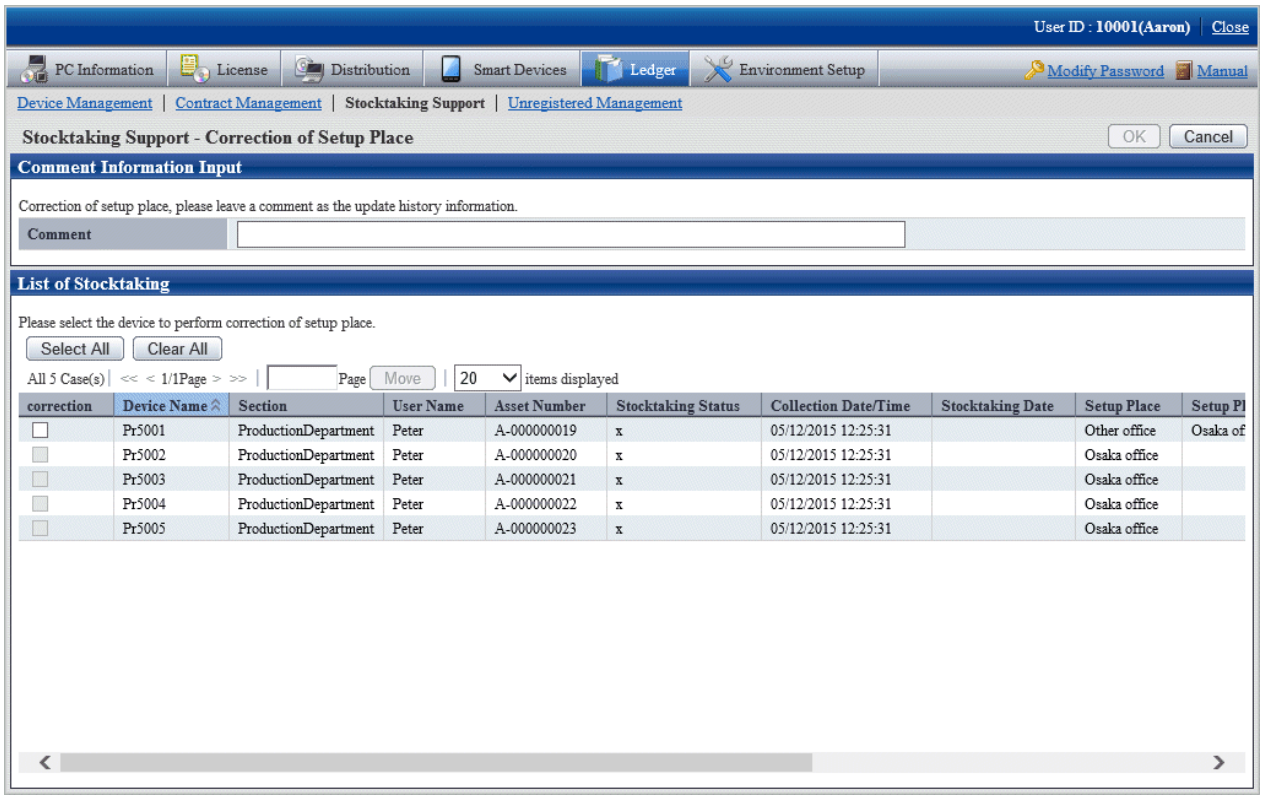
  When the setting location of network segment information has not been set though the network segment has been detected

Determine whether to rectify and rectify the setting location as required.

1. Confirm device to be rectified the setting location in the **List of Stocktaking** window.

   If necessary, click the **Correction** button.

   The following window will be displayed



   Even if the rectified value is displayed in the setting location (rectified value), the setting location might be moved temporarily. Determine whether to rectify the setting location and select the device after the administrator has confirmed the actual situation.

   After ranking according to the setting location (rectified value), the setting location where difference exists can be confirmed side by side merely.

2. Select annotation and device to be rectified in the setting location in the **Correction of Setup Place** window.

   *After setting **Comment**, it will also be reflected to **Comment** of **History Information**.
   If omitted, as annotation, it will be set as **Modification by Rectifying Setting Location**.

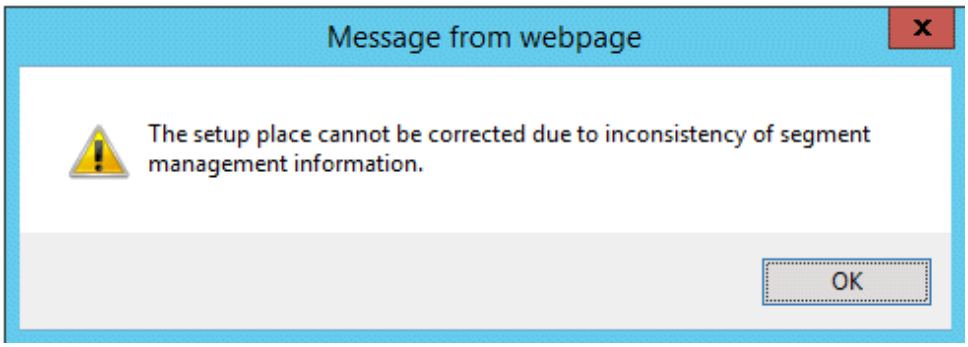
3. Click the **OK** button.

   Start to rectify the setting location.

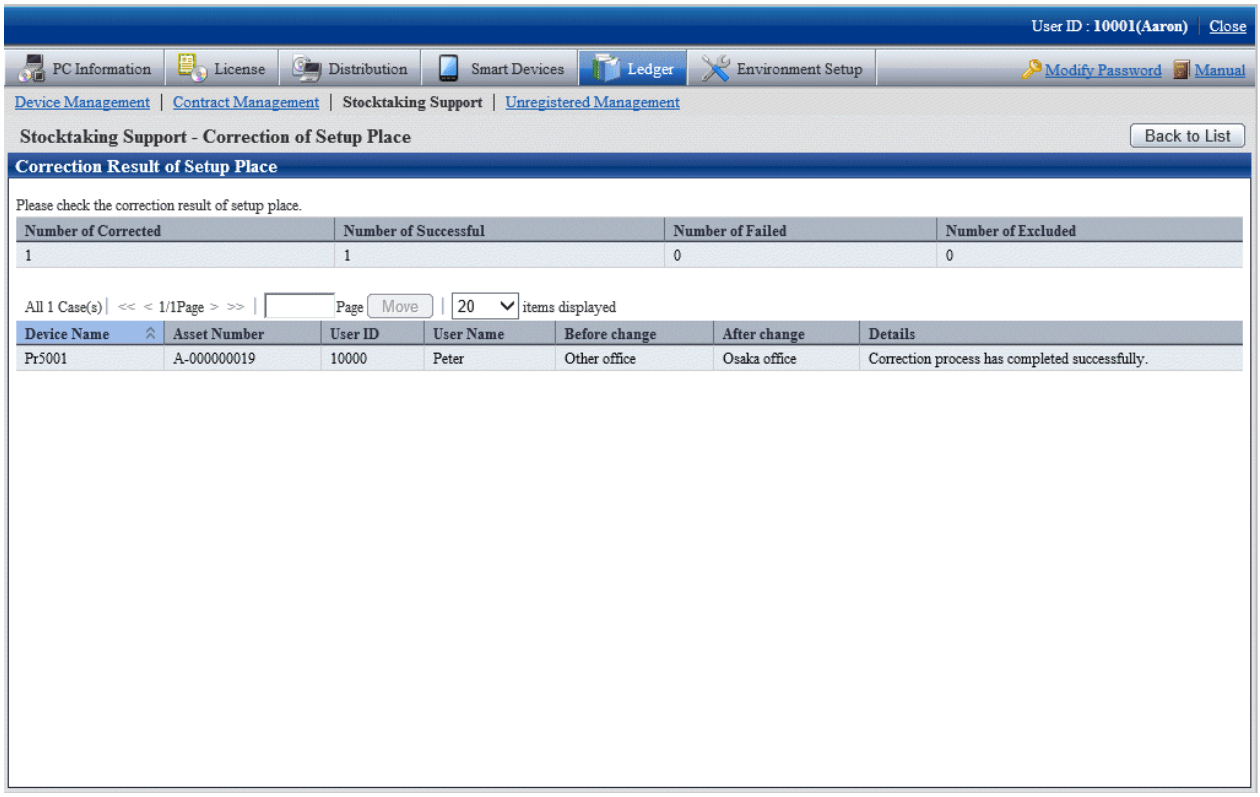
   The result of rectification will also be saved as history information.

   Due to organization modification, etc., modifications exist in building management information, and when network segment where setting location name has not been set for the network segment exists, the following message will appear.

At this time, click the **Correction** button by rectifying the Segment Management Information in the **Segment Management** window.

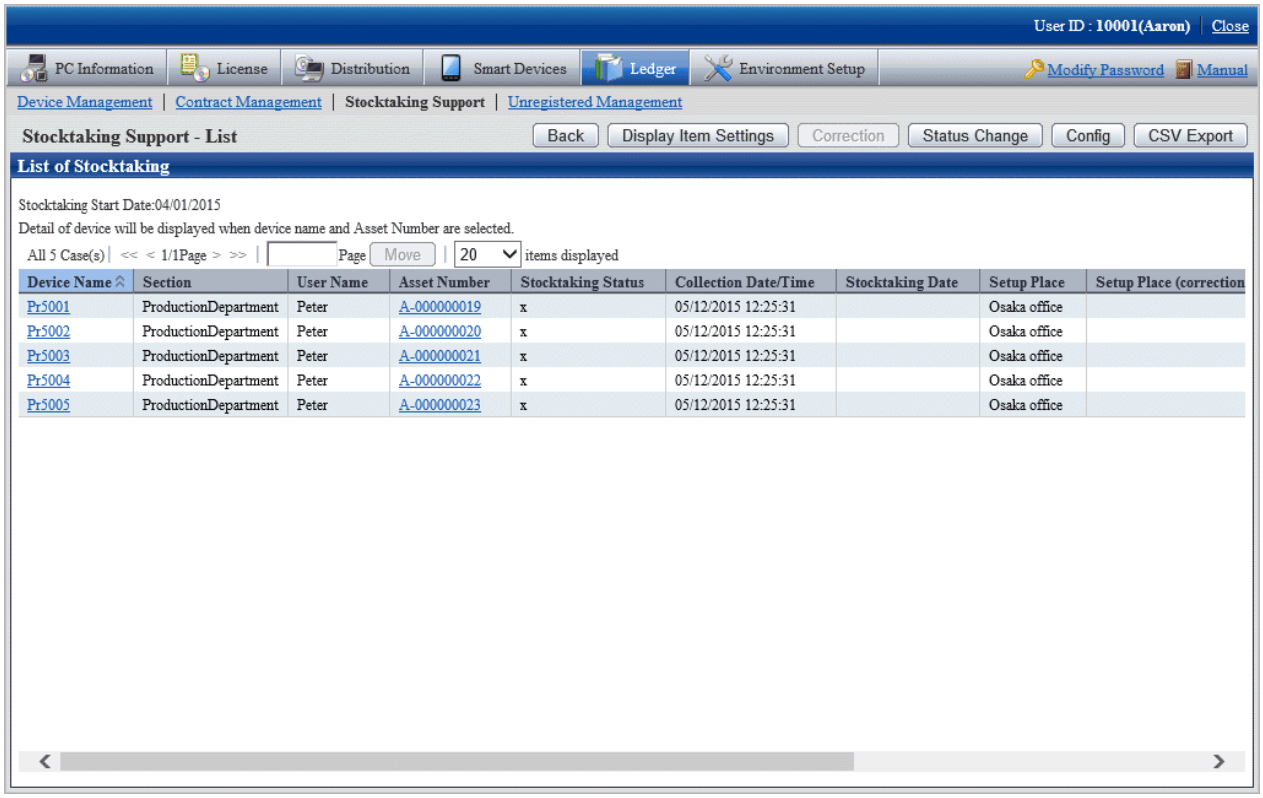


The **Correction Result of Setup Place** window is displayed after the rectification of setting location has been completed.



4. Confirm the content and click the **Back to List** button.

   The **List of Stocktaking** window is displayed again.



5. Confirm the setting location has been modified.

   Besides, confirm the inventory result (**o** or **x** will be displayed in **Stocktaking Status**).

   When confirming the setting locations before and after modification, select **Update History Information** in the **Device Management** window.

Chapter 12 Manage Machine by Layout Diagram

This chapter describes how to manage machines by layout diagram (location map function).

12.1 Preparation

Before performing the setting of location map function, the following preparation is required.

Settings of security level of Microsoft(R) Visio(R)

When using Microsoft(R) Office Visio(R) 2003, select **Macro** from the **Tool** menu of Microsoft(R) Visio(R) to modify the security level to **Medium**.

When the **Security Warning** window of Microsoft(R) Visio(R) is displayed, make sure to select **Enable Macro**. If **Disable Macro** is selected in the **Security Warning** window of Microsoft(R) Visio(R), the location map function will be unable to be operated.

Note

How to operate location map

The operation method of location map function varies depending on the version of Microsoft(R) Office Visio(R) being used.

When using Microsoft(R) Office Visio(R) 2003 or 2007, operating by using the **Desktop Patrol** from the menu bar of Microsoft(R) Visio(R). When using Microsoft(R) Office Visio(R) 2010 or 2013, operation by using the menu of **Desktop Patrol** in **Add-in** of the menu bar of Microsoft(R) Visio(R).

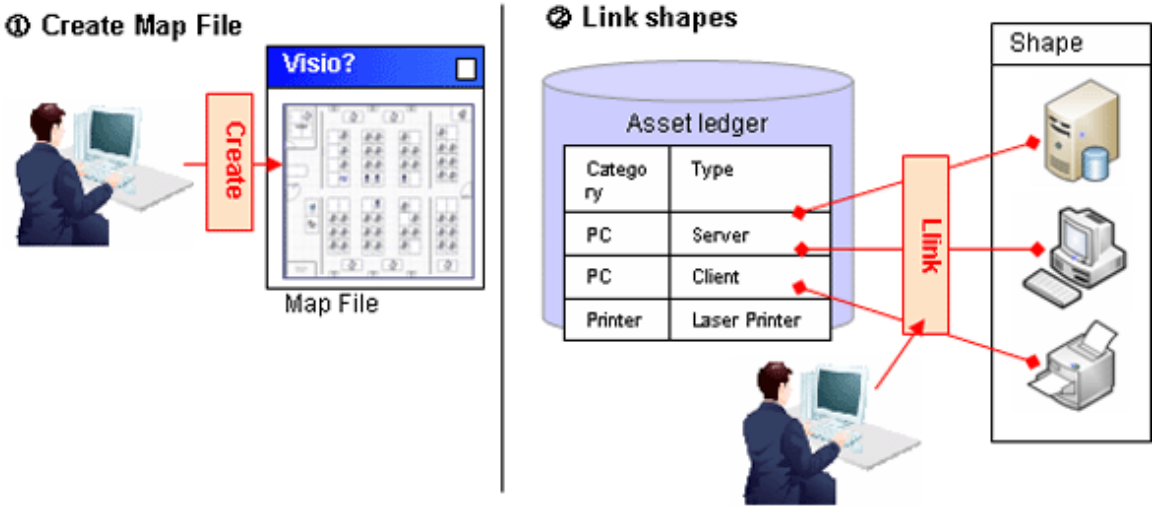
In addition, this manual records the operation method of Microsoft(R) Office Visio(R) 2003, 2007. When using Microsoft(R) Office Visio(R) 2010 or 2013, replace "From the menu bar of Microsoft(R) Visio(R),..." with "From the **Add-in** tab, ..." in the following description paragraph.

12.2 Perform Installation Settings of Location Map Function

In the location map, the machine in the map file is displayed as the shape of Microsoft(R) Visio(R). When using shape, allocate shape according to the category/type of machine. For example, if **Category/Type** is **PC/Server**, then use the shape of PC. If it is **Printer/Laser Printer**, then use the shape of printer, and so on. **Category/Type** of machine can be identified from shape.

*Perform the installation settings of the location map function shown in the following on a certain PC with location map function installed when it is used by multiple administrators. In addition, the installation setting requires the authority of system administrator account.

As the installation method of location map function, it is necessary to prepare for creating the map file to be used in this function, as well as the association of **Category/Type** and shape. The procedure is shown as follows.



About glossary of Microsoft(R) Visio(R)

Shape

It is the images for showing the shapes such as PC and printer to be configured in the map file.

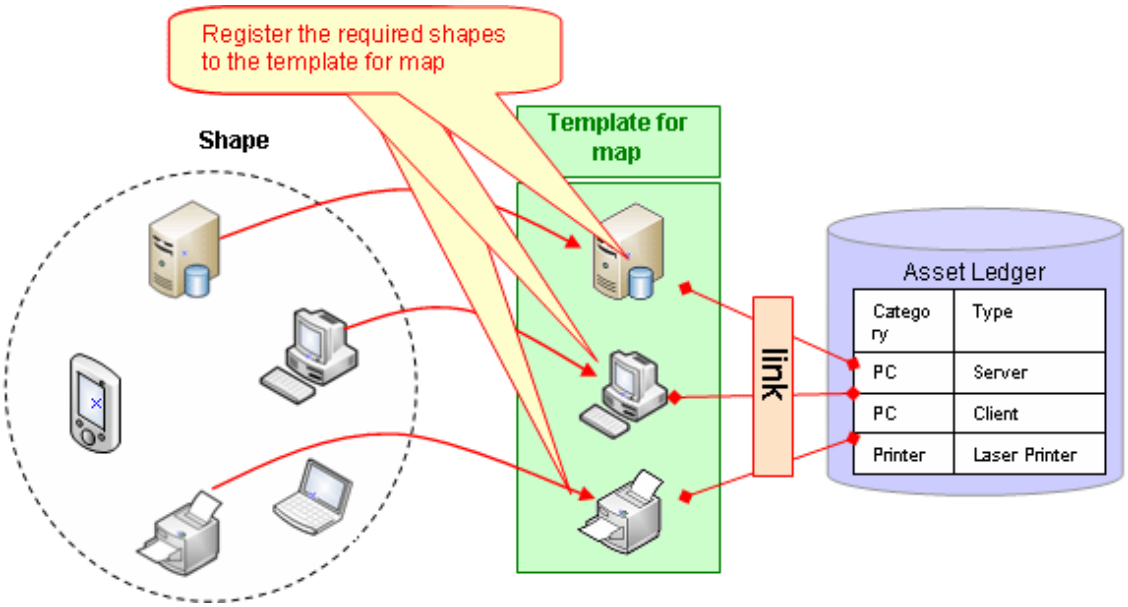
Stencil

It is the collection of shapes mentioned above.

Stencil can be created according to purpose and the type of shape and shapes can be classified.

About how to associate category/type with shapes

In the location map function, the shapes associating with the category/type of machine are registered as stencil (stencil for map) in advance. When the category/type of machine is associated with shapes, associate the shapes registered to stencil for this map with category/type.



About automatic configuration of machine

When newly configuring a machine through setting the user name at each position on the map file in advance, the position of correspondent machine will be configured automatically. Consequently, the burden on administrator during installation can be reduced.

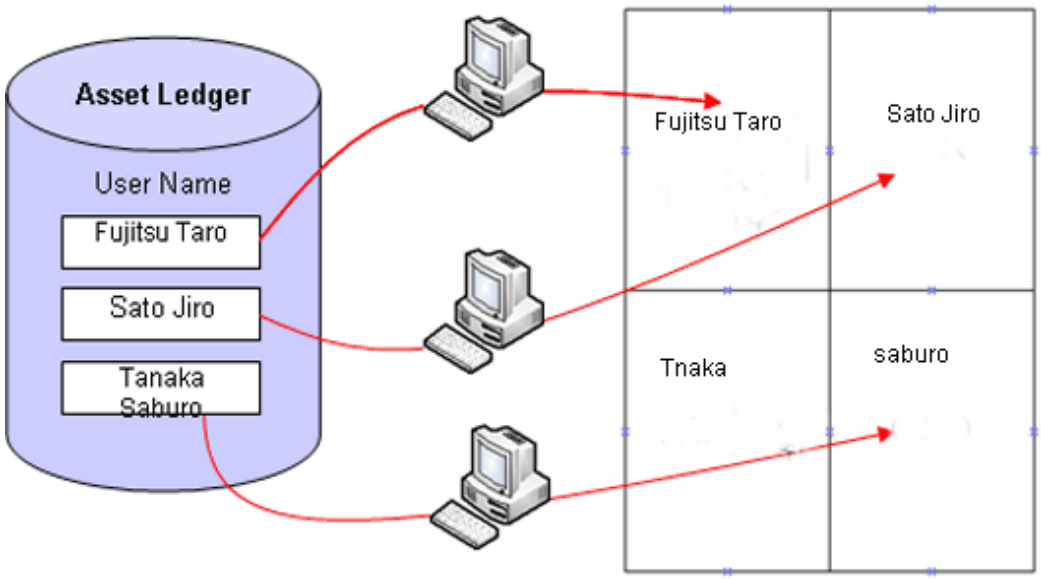
[About Configuration Method at Automatic Configuration]

- In automatic configuration, compare text set for the position on user name of machine and map file with the text excluding the following to determine the configuration location.
  - Single-byte blank
  - Multi-byte blank
  - Single-byte bracket
  - Multi-byte bracket
  - The keywords set by the user (refer to "12.2.7 Perform Automatic Configuration Settings of Machine" for setting method)
- When multiple correspondent configuration locations exist, the priority of configuration locations is as follows.
  1. Text that completely matches with the position

2. Text that mostly matches from the beginning

- When "Line feed" exists in the text set in position, the part before and after line feed will be processed as other statement. At this time, the machine of user name that matches with the separated text will be configured.
- Multiple machines cannot be configured at one position in automatic configuration.

* The following shows the example of automatic configuration.



The following shows the installation procedure of the location map function.

1. Create the target for saving the map file (required)

Prepare the folder for saving the map file.

2. Create and register the map file (required)

Create layout diagram using Microsoft(R) Visio(R) and register the map file.

3. Set the target for saving the map file (required)

Set the target for saving the map file.

4. Associate the map file (required)

Associate map file and setting location.

5. Create the stencil for map (required)

Create a collection of shapes as the stencil for map.

6. Association of shapes (required)

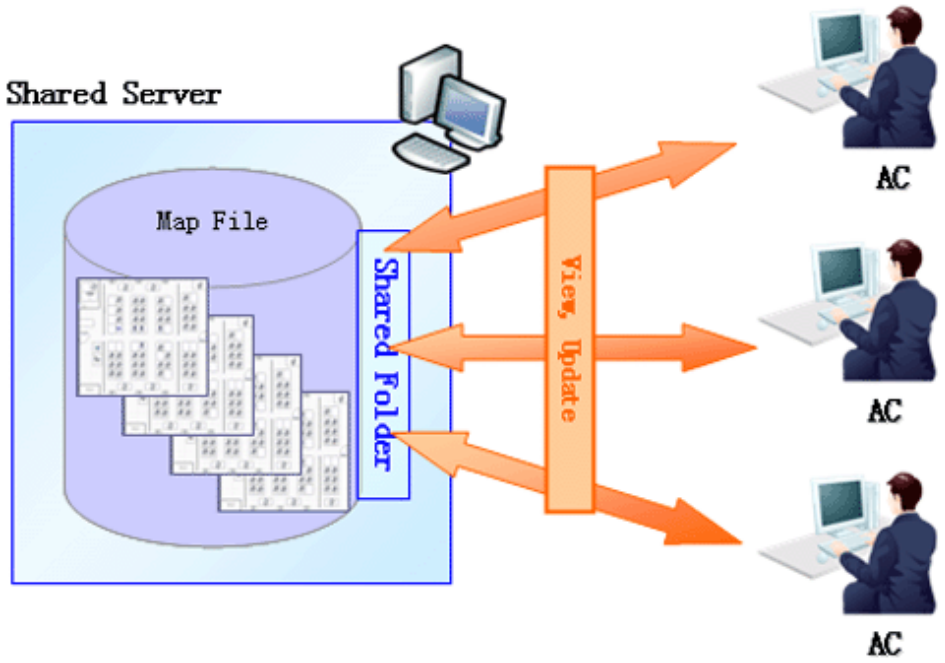
Associate shapes in category/type of machine.

7. Set automatic configuration of machine (optional)

Set the existence of automatic configuration and information relating to automatic configuration.

12.2.1 Create the Target for Saving Map File

Create the target for saving map file. To enable the viewing of map file from multiple PCs of Desktop Patrol AC, it is required to save onto the shared folder that can be viewed from the PC of Desktop Patrol AC.



*For shared folder, the authority of reading/writing from the PC of each Desktop Patrol AC is required.

12.2.2 Create Map File

Create map file using Microsoft(R) Visio(R) according to setting location.

Register the sample of map file to the following location. Create the map file by referring to this file.

Registration destination of sample file

AC installation directory\Sample\sample.vsd

- Drawing size of map file and file name are based on Microsoft(R) Visio(R).
- Set the number of drawing pages of map file to 1 page.
- Set the drawing scale of map file map to equal.

  *The drawing scale can be set according to the following procedure.

  1. Select **File** > **Page Settings** from the menu bar of Microsoft(R) Visio.
  2. Select **Equal (1:1) (N)** from the **Drawing Scale** tab of the **Page Settings** window.
  3. Click the **OK** button of the **Page Settings** window to reflect settings.
- When performing automatic configuration of machine, set the user name in the text of each position of the map file. Configure the machine by referring to the set text.

  *images such as bitmap and JPEG, as well as layout such as Excel files exist, they can be used directly without creating the layout again. However, when using the images and Excel file, the automatic configuration of machine cannot be performed.

  a. When images such as BMP and JPEG exist

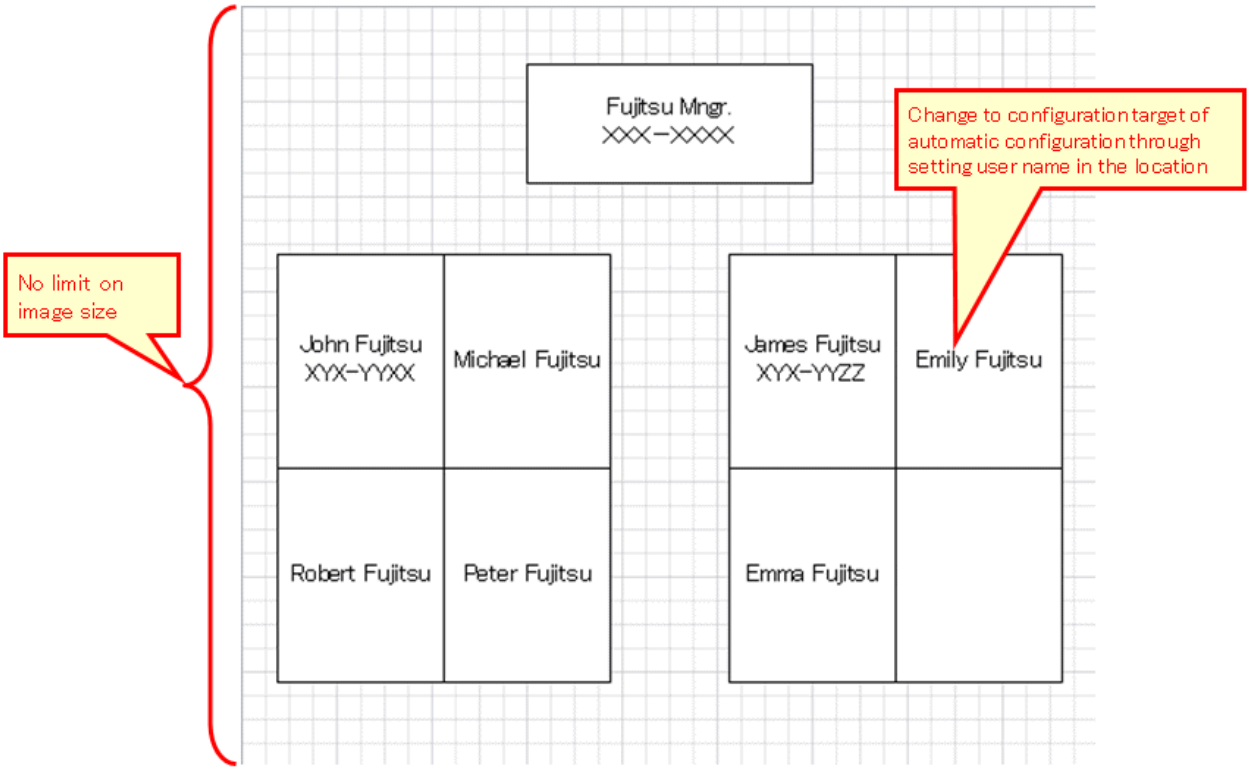
     Images can be imported to Microsoft(R) Visio(R).

     Attach the image files to the drawing of Microsoft(R) Visio(R).

  b. When Excel file exists

     Capture layout diagram of Excel as image file with the same procedure as "a" mentioned above and attach to the drawing file of Microsoft(R) Visio(R).

Save the created map file to the target for saving the map file set in "12.2.1 Create the Target for Saving Map File".



12.2.3 Set the Target for Saving Map File

Set the path of target for saving the map file prepared in "12.2.1 Create the Target for Saving Map File" for the location map function.

1. Log on to the AC Menu with the account of system administrator.

   The AC menu will be displayed.

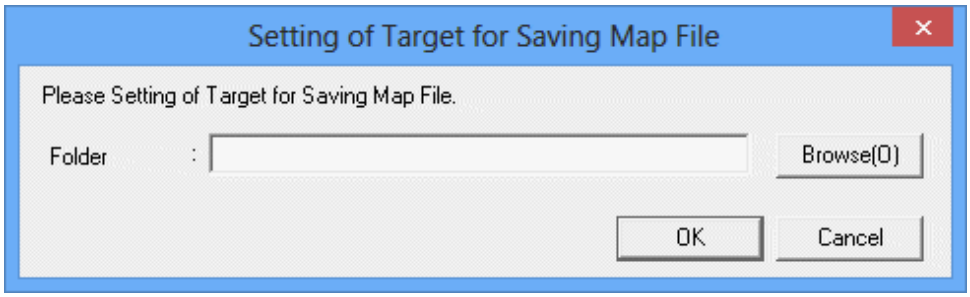
2. Click **Location Map**.

   Microsoft(R) Visio(R) will be started.

   *Before logon, when Microsoft(R) Visio(R) is starting, start a new Microsoft(R) Visio(R). The started Microsoft(R) Visio(R) will become active.

3. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Setup of the Storage Location of Map-File**

   The **Setting of Target for Saving Map-File** window will be displayed.



4. Set the path for saving map file in the saving target folder, and click the **OK** button.

   * When specifying the network folder from the **Browse** button, re-allocate the network drive.

Note

When access error occurred in Windows Vista(R), Windows(R) 7 or Windows(R) 8

When specifying a network folder that requires user name and password for the saving target folder, it is likely that the saving target of map file with access error cannot be set.

In the above condition, it is required to enter the user name and password corresponding to the network folder from Microsoft(R) Visio(R). From the menu bar of Microsoft(R) Visio(R), select **File** > **Open** to open the specified network folder and the user name and password can be entered.

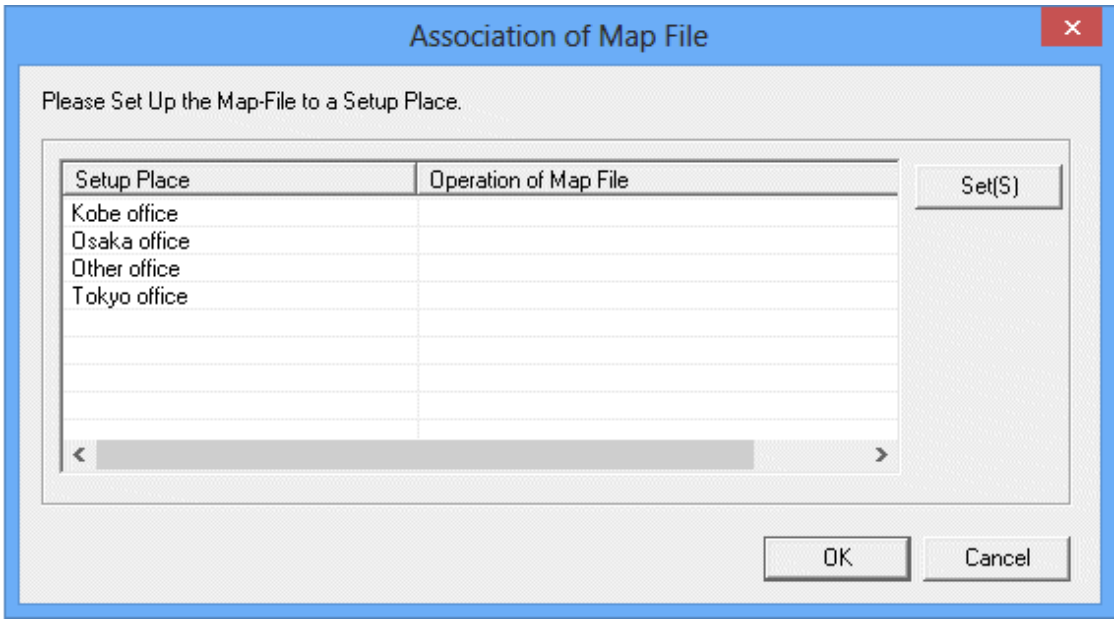
The operation of entering user name and password as mentioned above is required every time when the OS is restarted. To specify the network folder for the saving target folder, it is recommended to use the environment that does not require user name and password.

12.2.4 Associate Map File

Associate the map file and setting location registered in "12.2.2 Create Map File".

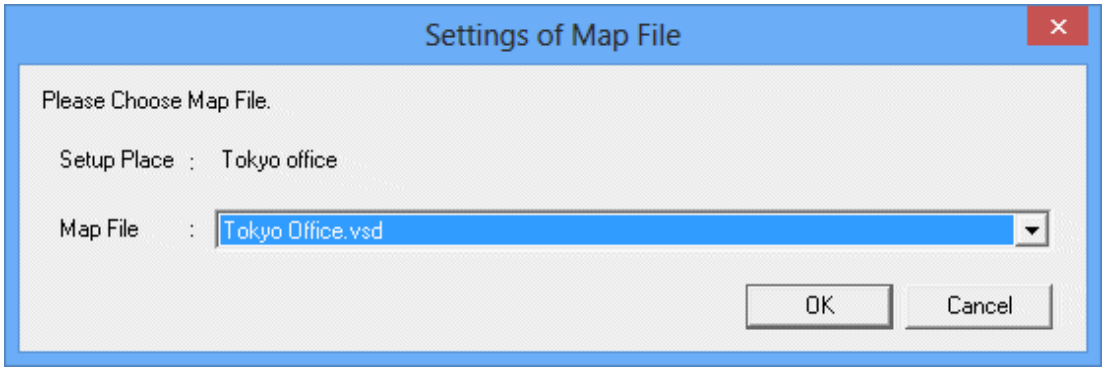
1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Correlation of Map-File**.

   The **Association of Map-File** window will be displayed.



2. From the **Association of Map-File** window, select the setting location to set map file and click the **Set(S)** button.

   The **Settings of Map File** window will be displayed.



3. Select the map file from the **Settings of Map File** window, and click the **OK** button.

   * In the combo box of map files, the map files exist in the saving target of map file set in "Create 12.2.1 Create the Target for Saving Map File Target of Map File" will be displayed.

4. Repeat the above "2." and "3." to set the map file for the setting location managed in the location map function.

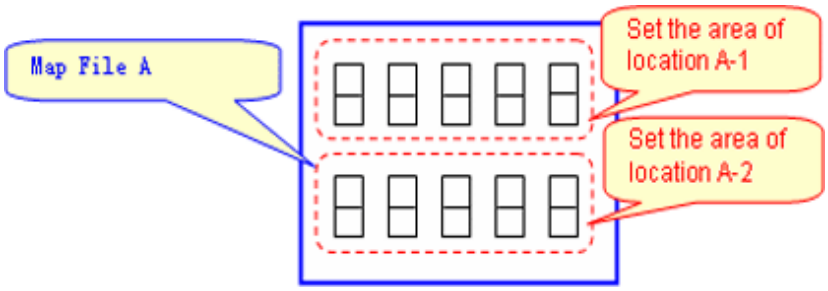
   Then, click the **OK** button in the **Association of Map-File** window and register the set content.

Point

Association of setting location and map file

The case of association that is not 1 to 1 between setting location and map file is shown as follows.

When multiple setting locations exist for one map file

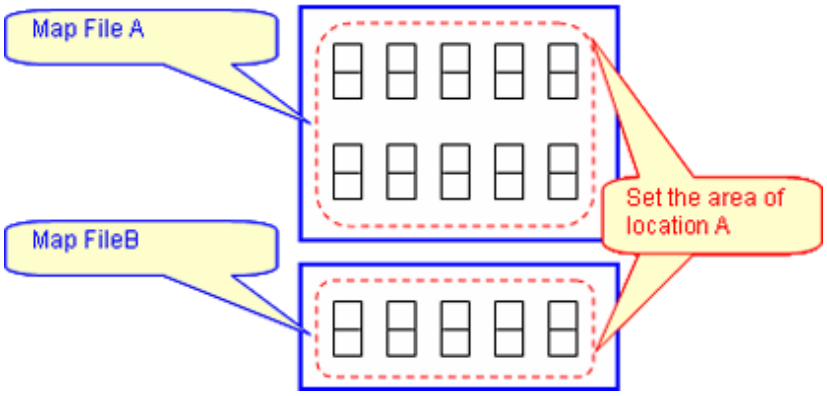


Associate the map file A in the above image as follows.

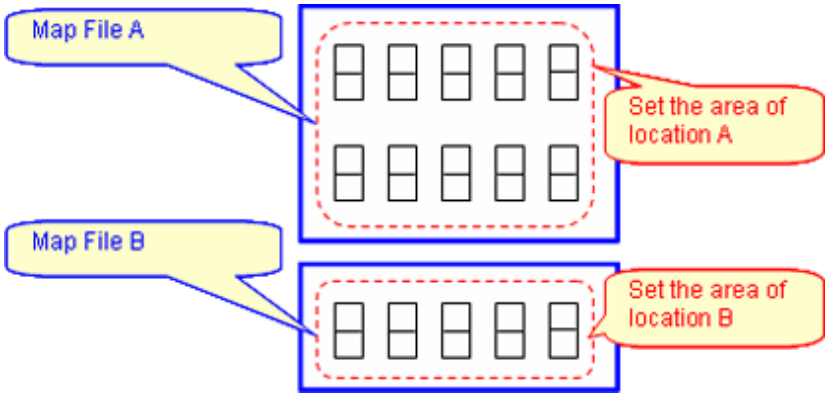
Set the area of location A-1: Map File A

Set the area of location A-2: Map File A

When one setting location exists in multiple layout diagrams



In the above diagram, it is unable to manage in the location map function. Divide the setting location information (building management information of DTP side), manage map file A and B in other setting locations. (Refer to the following diagram).



Set the area of location A: Map File A

Set the area of location B: Map File B

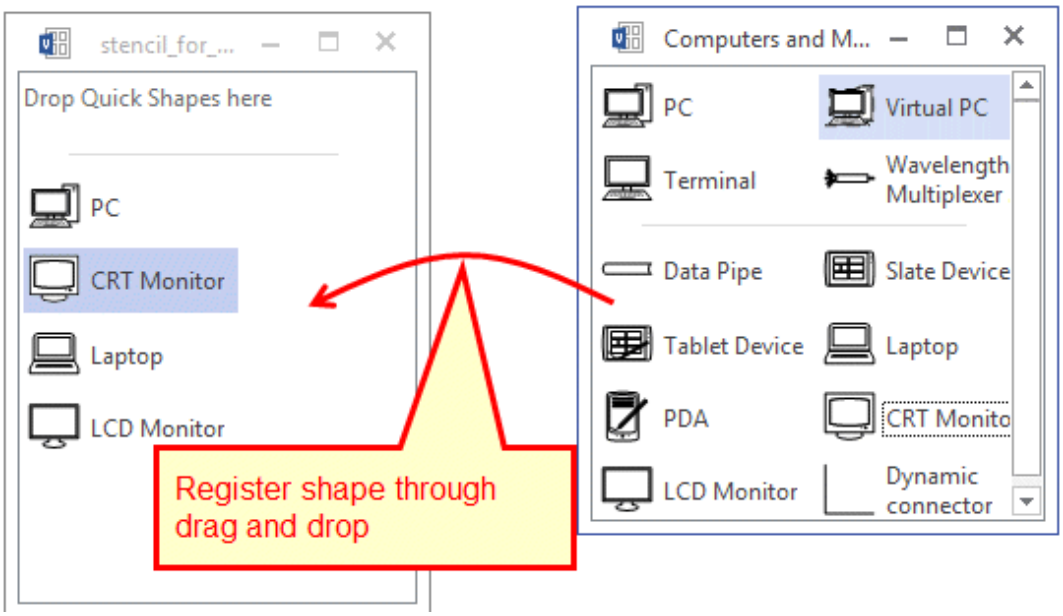
12.2.5 Create Stencil for Map

Create a collection of shape associated in category/type of machine as the stencil used by map.

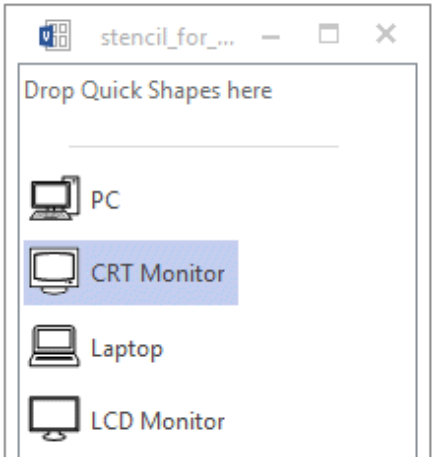
1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Edit Stencil for Map**.

   The stencil for map will be displayed.

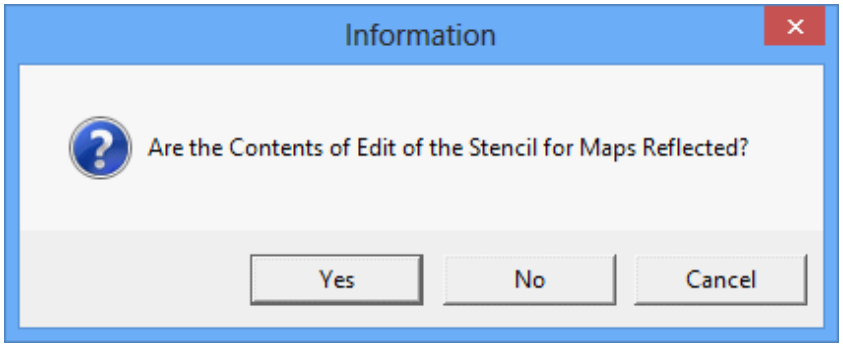
2. Open the stencil in which the shapes to be used exist (open the correspondent stencil from **File** > **Shape (E)** from the menu bar of Microsoft(R) Visio(R)), and drag&drop the shape to be used to the stencil for map.



3. After the registration operation to the stencil for map has completed, click the **x** button of window of the stencil for map to exit.



The reflection confirmation message of stencil for map will be displayed.



4. Click the **Yes** button of the reflection confirmation message of the stencil for map to reflect the content edited to the stencil for map.

Point

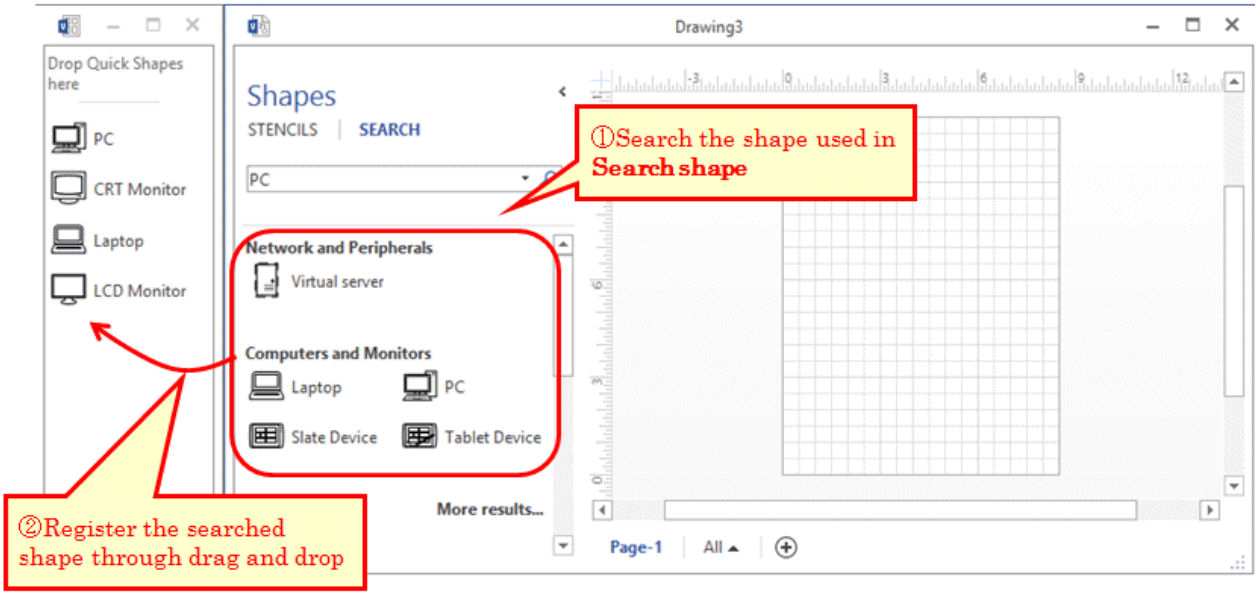
Shape can be registered to stencil for map through searching

In the step of the above "2.", when drag&drop shapes, the shape to be used can be searched from **Search Shapes**.

[Search Method]

1. Select **File** > **New** > **New Drawing** of the menu bar of Microsoft(R) Visio(R).

2. Select **View** > **Drawing Window** of the menu bar, and the shape searched using **Search Shapes** can still be registered to the stencil for map through drag&drop.



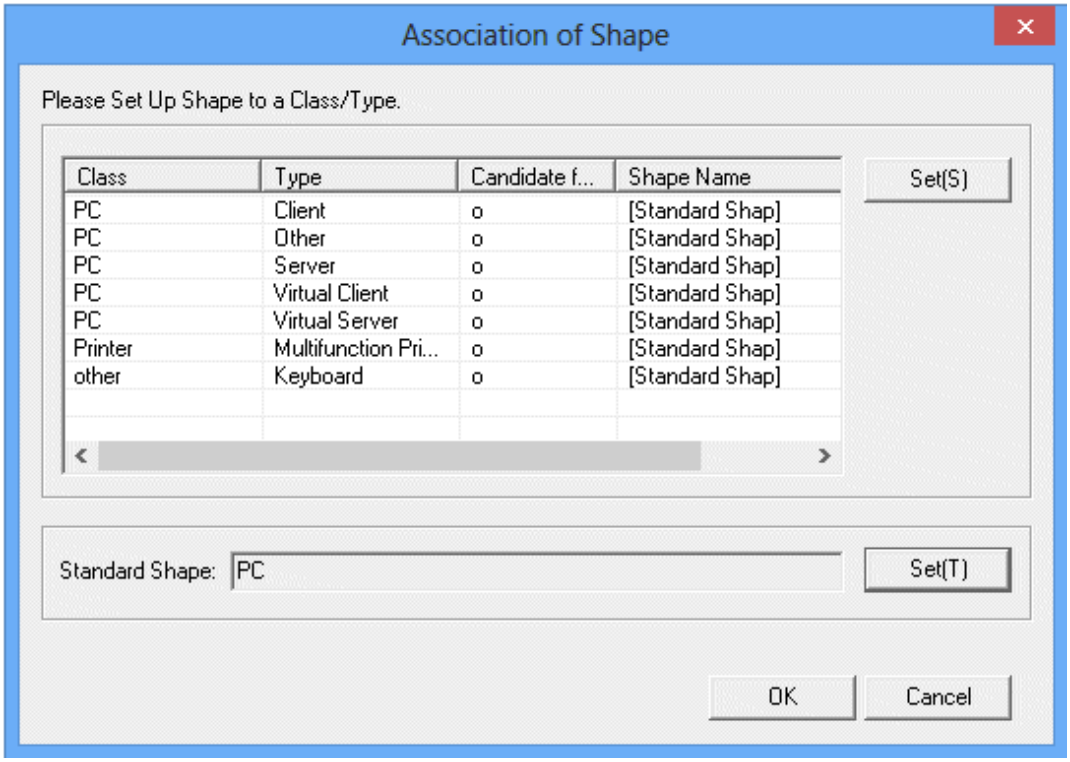
12.2.6 Association of Shape

Associate the category/type of machine with shapes.

In addition, set the category/type that is not targeted as the map file here. For example, when monitor and keyboard are not managed in map file, it is possible to exclude these settings from the target.

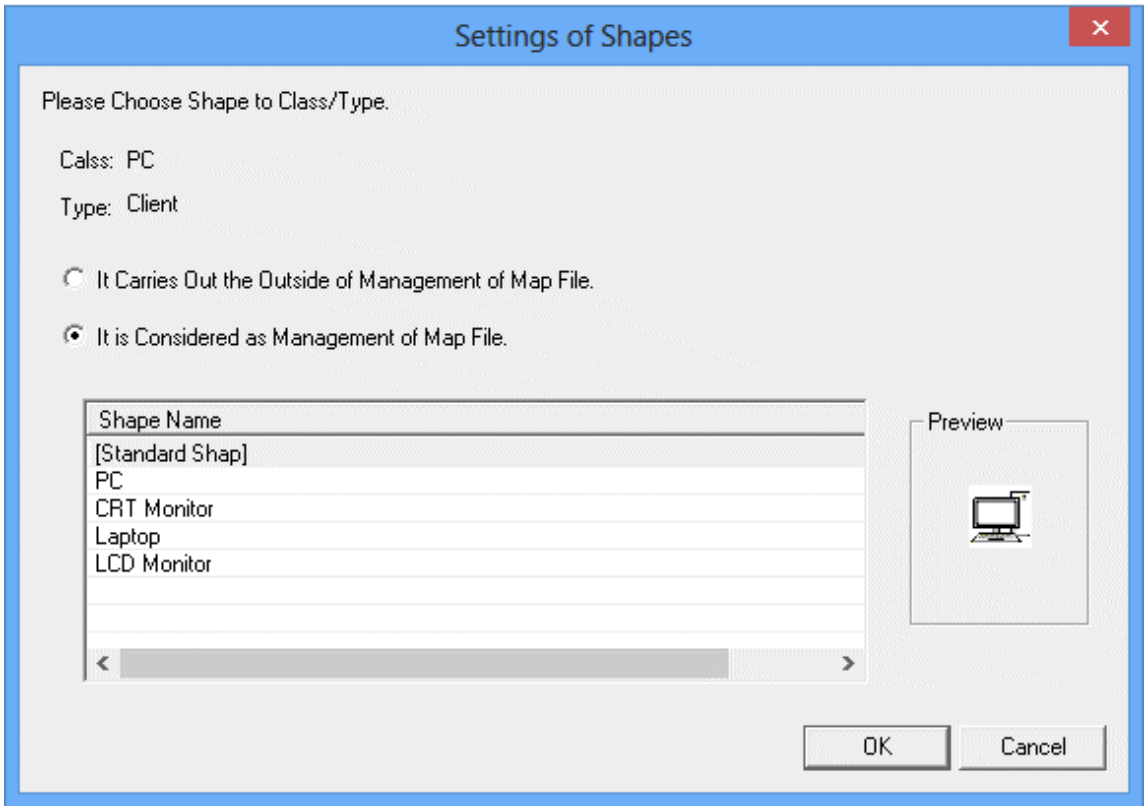
1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Correlation of Shape**

   The **Association of Shape** window will be displayed.



2. From the **Association of Shape** window, select the category/type of shape, and click the **Set(S)** button.

   The **Settings of Shapes** window will be displayed.



3. Select to associate shape name as the configuration target of map file, and click the **OK** button.
4. Repeat the above "2." and "3." And set the shape name for category/type.

   Then, click the **OK** button of the **Association of Shape** window to reflect the set content.

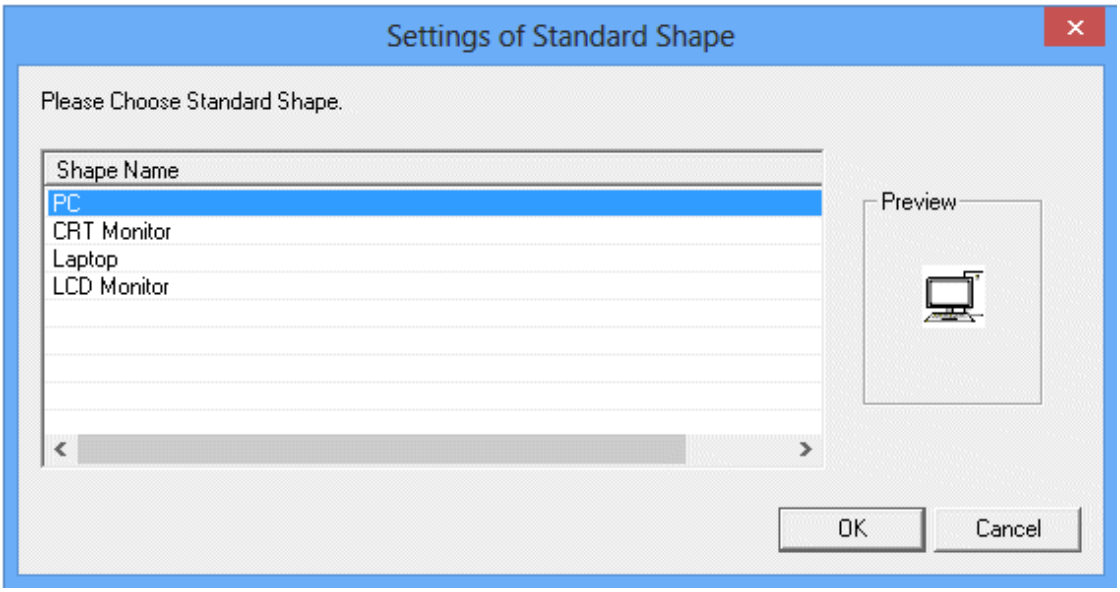
Point

Standard Shape can be set

In the location map function, when association of shape is not performed for category/type, the shape defined in **Standard Shape** for correspondent category/type will be associated. If typical shape is set for **Standard Shape**, it is not necessary to associate shapes for all categories/types (the category/type with omitted settings will also be associated with the same shape).

The shape of **Standard Shape** can be set through clicking the **Set(T)** button of **Standard Shape** of the **Association of Shape** window.

Settings of Standard Shape window



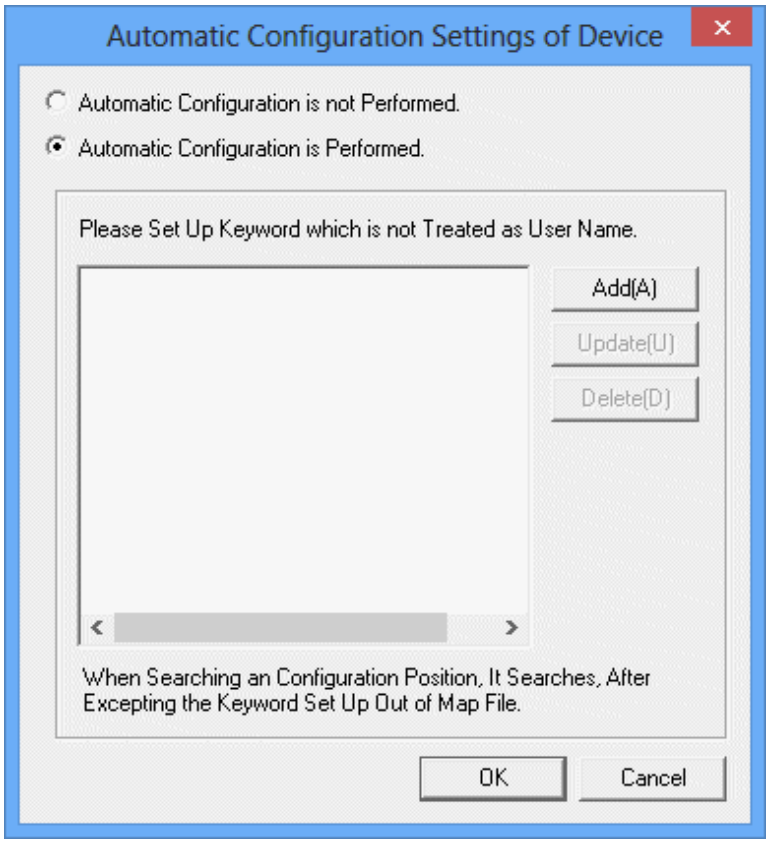
12.2.7 Perform Automatic Configuration Settings of Machine

Set whether to configure the created shape of machine automatically in map file.

In addition, when searching the automatic configuration location, set the keyword to be excluded from the map file.

1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Automatic Arrangement Setup**.

   The **Automatic Configuration Setting of Device** window will be displayed.

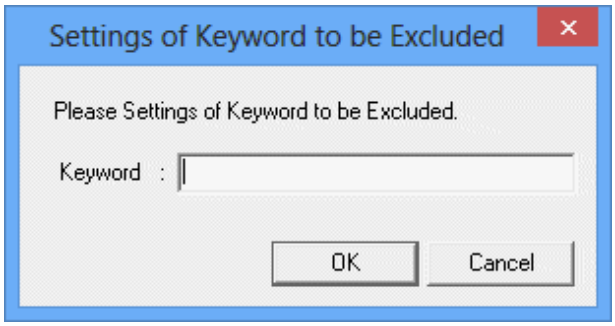


2. Select perform/not to perform automatic configuration from the **Automatic Configuration Setting of Device** window.
3. When performing automatic configuration, set the keyword that will not be processed as user name on the map file. There are following two methods to set keywords.

   - Add keyword

     1. Click the **Add** button.

        The **Setting of Keyword to Excluded** window will be displayed.



        Up to 16 fullwidth or 32 halfwidth characters can be set for the **Keyword**.

     2. Set the keyword to be excluded, and click the **OK** button.

   - Update keyword

     1. Select the keyword to be modified.
     2. Click the **Update** button. (The window same as **Add** will be displayed.)

3. Set the keyword to be excluded and click the **OK** button.

- Delete keyword

1. Select the keyword to be deleted.
2. Click the **Delete** button.

4. Repeat **Add**, **Update**, and **Delete** of "3.", and set keyword.

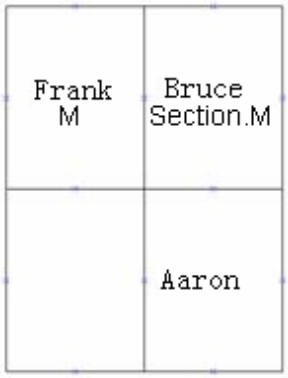
   Then, click the **OK** button of the **Automatic Configuration Setting of Device** window to register the set content.

Point

Set role name .etc for the keyword not to be processed as user name

The "Role Name" .etc is corresponded as the keyword not to be processed as user name on the map file.

In the following example, set the keyword not included in user name of machine as "Section.M", "M" of role name.



* For entered keyword, single-byte and multi-byte characters are seen as different characters.

12.3 Operate Location Map

This section describes how to operate the location map function.

- Create map file
- Confirm machine information
- Confirm the difference with asset ledger
- Confirm the status of machine

About user authority

To use this function, the authority of "system administrator" and "section administrator" is required.

- System Administrator

  It is allowed to operate all machines.

- Section Administrator

  It is allowed to operate machines under its own section, subordinate section or not configured.

Notes

- About the use of multiple administrators at the same time

  The location map function cannot be used by multiple administrators at the same time. The map file being edited by another administrator cannot be viewed/edited.

- About the machine not to be configured to map file

  The following machines are out of the configuration target of map file.

  - The machine for which the setting location is not defined
  - The machine of category/type set to out of configuration target

12.3.1 Create Map File

In the location map function, for map files, machine can be configured, the configuration for the configured machine can be cancelled and machine can be moved to other map file. Use these functions to create map file.

Configuration of machine

Open the map file, and the operation procedure from configuration of machine to the saving of map file is shown below.

1. Log on to the AC menu with the account of system administrator or section administrator.

   The AC menu will be displayed.

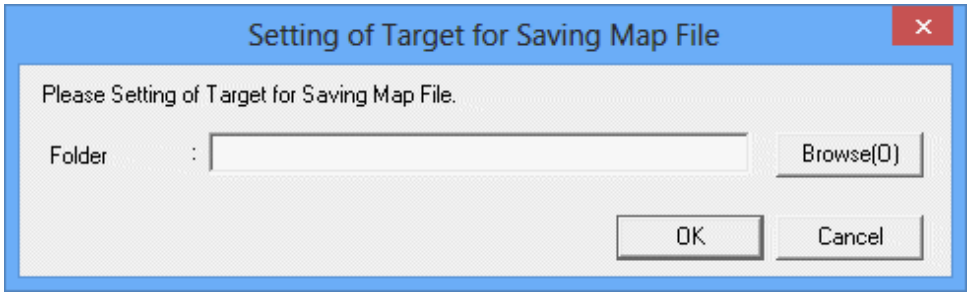
2. Click **Location Map**.

   Microsoft(R) Visio(R) will be started.

3. Set the target folder for saving map file. Perform during the installation of the following settings and when the target folder for saving is modified.

   From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Environment Construction** > **Setup of the Storage Location of Map-File**, set the patch for saving map file in the displayed **Setting of Target for Saving Map-File** window.

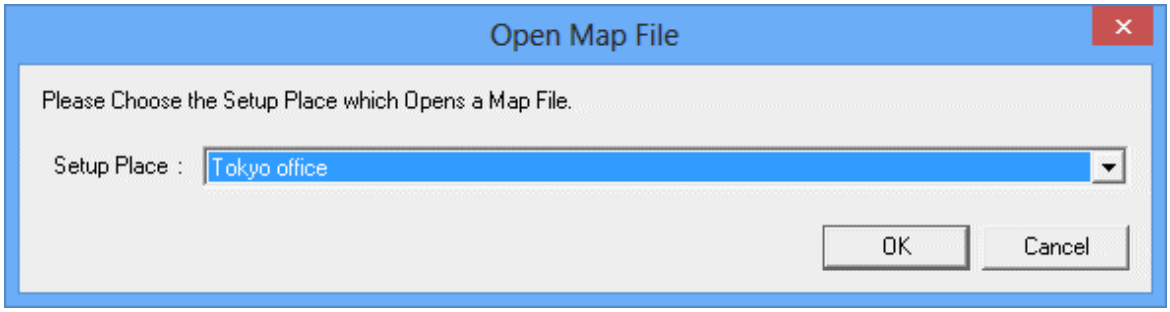
   The **Setting of Target for Saving Map-File** window will be displayed.



   *Perform the allocation to the network drive again for the saving target of map file. Set a path of network drive as saving target folder.

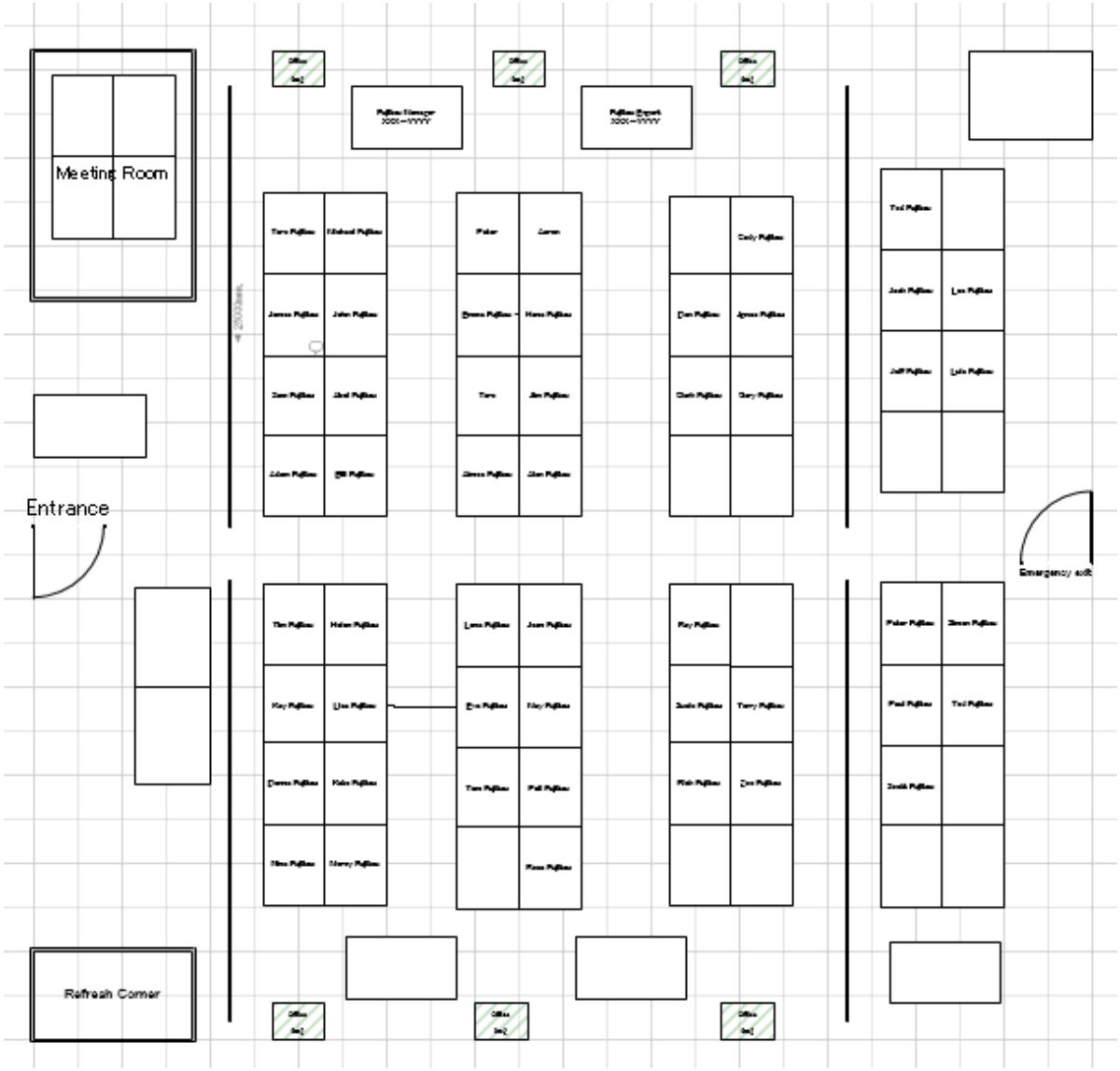
4. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Operation of Map File** > **Open**.

   The **Open Map File** window will be displayed.



5. After selecting the setting location from the **Open Map File** window, click the **OK** button.

   The map file of the selected setting location will be displayed.

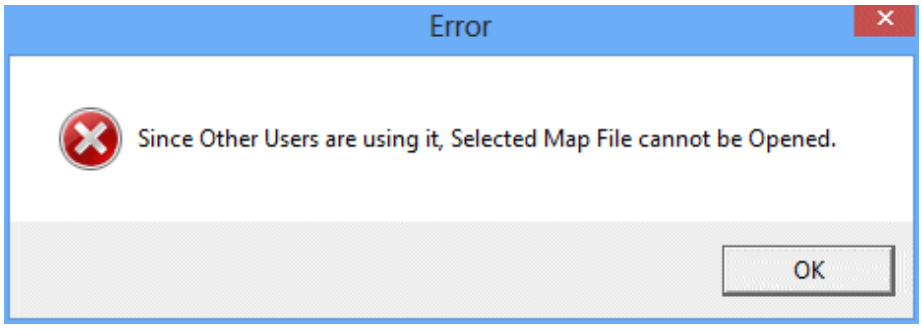


Note

Error occurred when the map file that is being edited by another administrator is selected

When the setting location that is being edited by another administrator is selected, the following message will be displayed.

Execute again after the other use has finished editing.



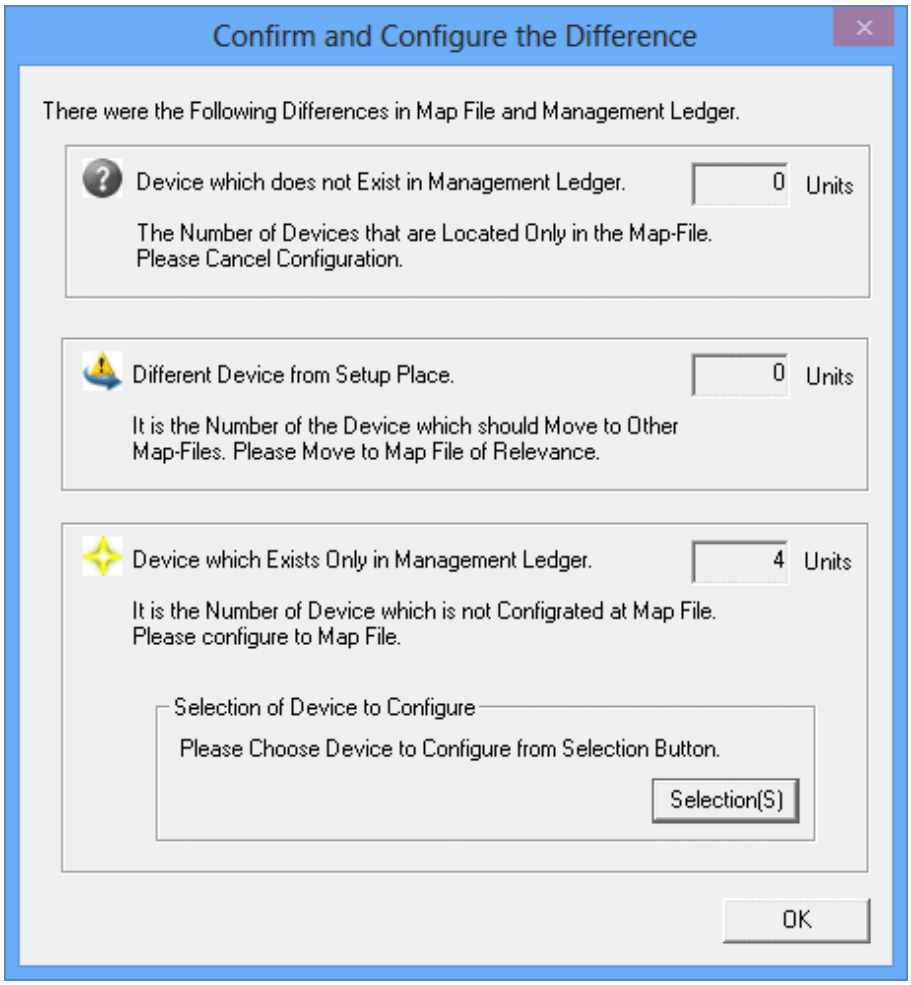
* On the map file, when the machine has been configured, the asset management number under the shape of machine will be displayed.

* In the following cases, machine will not be displayed.

- When the user that uses the location map function is the section administrator, the machine of other sections will not be displayed.
- When multiple setting locates are associated on the map file, the machine with different setting locations will not be displayed.

6. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Confirm and Configure the Difference with Asset Ledger**.

   The **Confirm and Configure the Difference** window will be displayed.

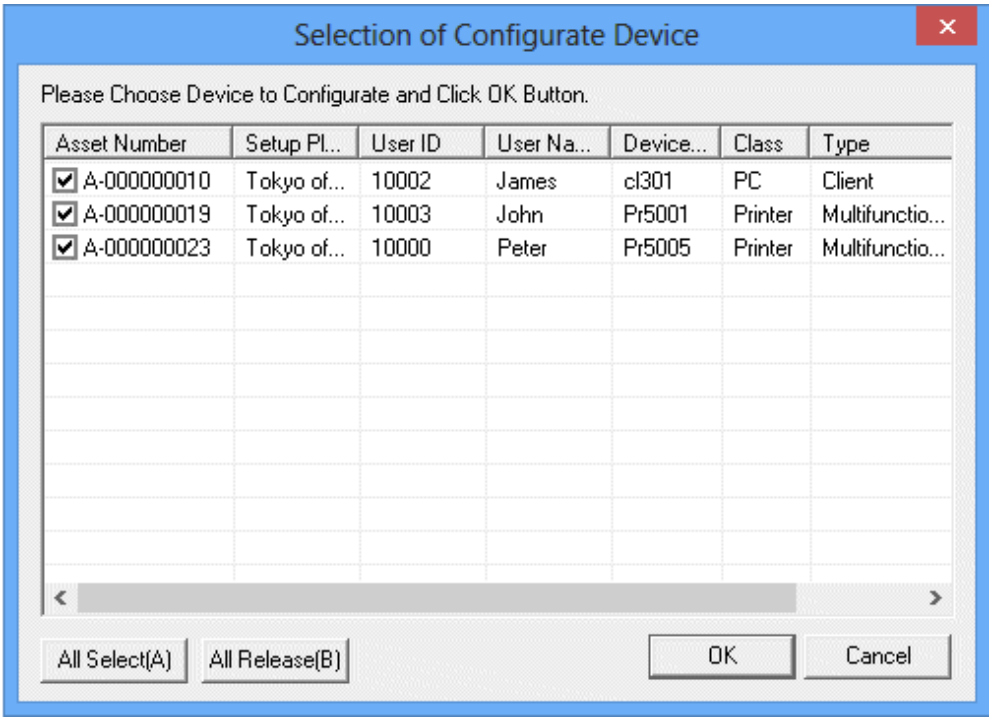


7. Click the **Selection** button of the **Confirm and Configure the Difference** window.

   The list of machine without configuration will be displayed in the displayed map file.

   - The machine that has completed the configuration of map file will not be displayed in the list.

- For machine without associated shapes, the shape name will be displayed as **Standard Shape**.



8. Select the checkbox of machine to be configured, and click the **OK** button.
9. Click the **OK** button of the **Confirm and Configure the Difference** window.

   The selected machine will be configured virtually on the map file.

When the setting of automatic configuration is performed, machine will be configured automatically. When the setting of automatic configuration is not performed, it will be configured to the location at top left of the map file.

10. Configure the machine that has been configured virtually to the machine physically exists on the map file.

Point

The information of machine can be configured after confirmation

Double-shape the shape of the configured machine and the information of machine can be confirmed. Use it as the reference data at the time of moving to the formal configuration location.

Shape Data - PC.24	
Assets Management No.	A-000000144
Setup Place	Tokyo office
Section	DTP-Foreign
User ID	PeterFujitsu
User Name	Peter Fujitsu
Device Name	CT144
Class	PC
Type	Client

11. Repeat the above "10.", and create the map file.

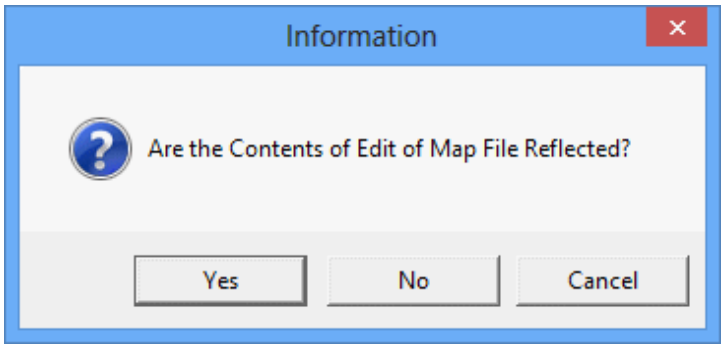
12. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Operation of Map File** > **Save** to save the map file.

Note

Save the map file from the location map function

The result of editing such as file saving inside the Microsoft(R) Visio(R) menu will not be reflected to the map file. While saving, make sure to save the above operation.

If the **x** button of the map file is clicked to close the map file without saving it, the confirmation message for whether to save or not will be displayed.



Note

When map file is not matched, it is unable to save

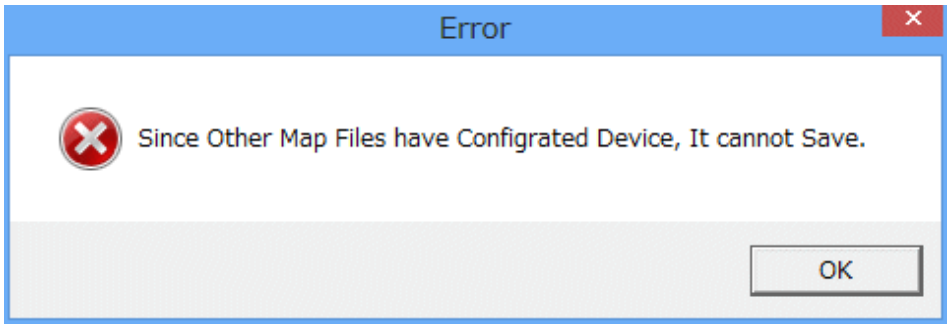
When the map file is edited by multiple administrators, the machine may not match with the map file sometimes.

Example)

a. When the Administrator A configures the **Machine A** to the map file of Setting Location A
b. Before saving the operation of the above "a)", the Administrator B configures the **Machine A** to the map file of Setting Location B

In this case, the Machine A will be configured to any one of Setting Location A and B.

If inconsistency occurred as the above example, the following message will be displayed when saving and the map file cannot be saved.



After this message has been closed, the status confirmation icon will be displayed for the correspondent machine for whether to confirm other map files. Save after performing the **Cancel Configuration** operation of the correspondent machine from this map file.

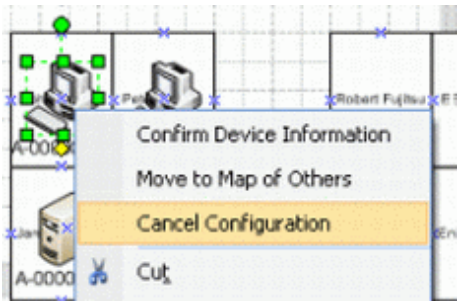
13. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Operation of Map File** > **Close** to close the map file.

Cancellation of configuration

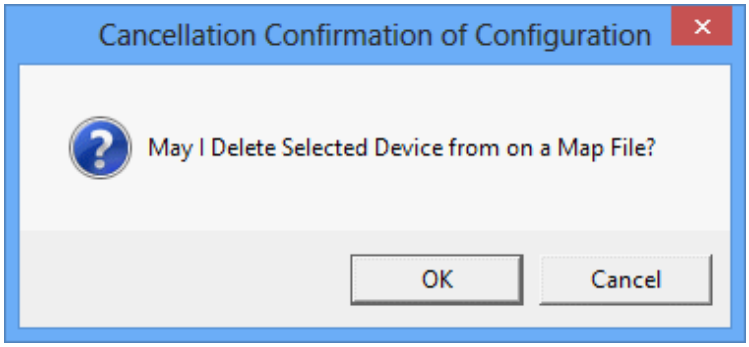
For the machine that has completed the configuration of map file, the following shows the operation procedure to cancel configuration (delete from map file).

1. Right-click the machine that has been configured, and click **Cancel Configuration** in the displayed menu.

   When performing the cancellation of the configuration of multiple machines, after selecting all machines to be cancel operation and click **Cancel Configuration**.



   The **Cancellation Confirmation of Configuration** window will be displayed.



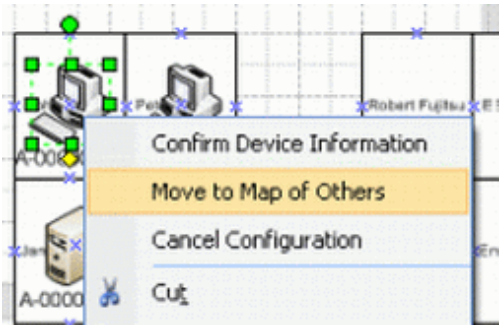
2. Click the **OK** button to cancel the configuration.

Move to other map

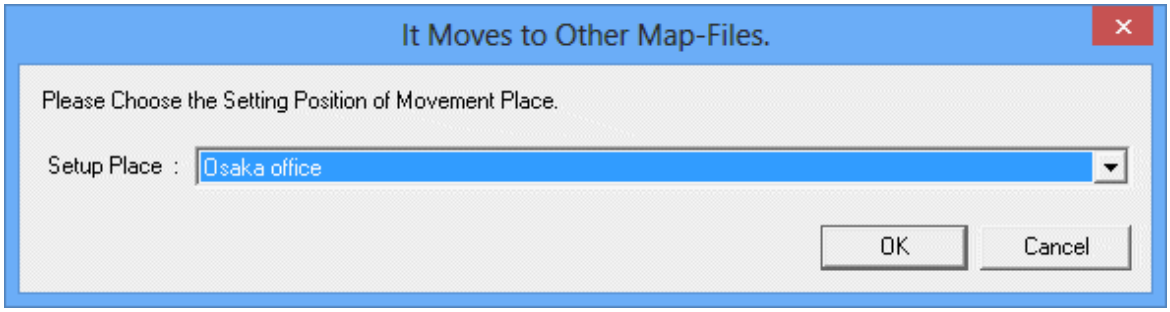
The following shows the operation procedure of moving the machine that has been configured to another map.

1. Right-click the machine that has been configured, and click **Move to Map of Others** in the displayed menu.

   To move multiple machines, after selecting all the machines to be moved, click **Move to Map of Others**.

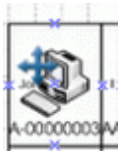


The **It Moves to Other Map-Files** window will be displayed.



2. Select the setting location to be moved, click the **OK** button.

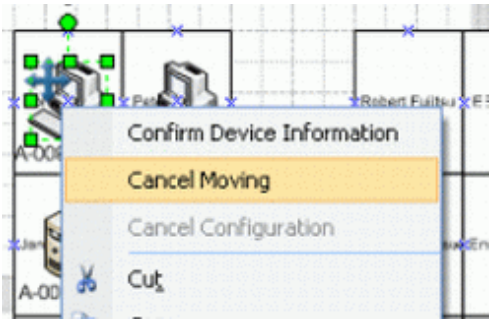
   The icon of correspondent machine to be moved will be displayed.



Point

The moving can be cancelled

Right-click the machine to be moved to here and click **Cancel Moving** in the displayed menu, the moving can be cancelled.



3. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Operation of Map File** > **Save** to save the map file.

   Once saved, the machine to be moved will be deleted from the map file.

   In addition, since the machine moved to the map file at destination of moving will be configured virtually, open the map file in the destination of moving and adjust configuration location .etc.

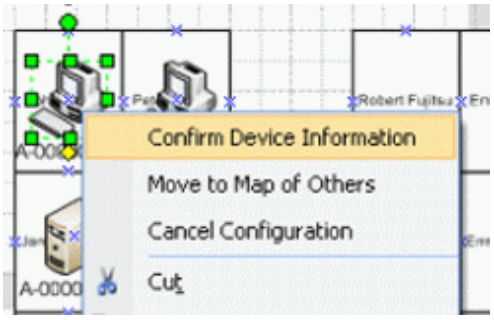
   The operation of moving to other map file is performed while saving the map file. Do not move when not to save the map file.

12.3.2 Confirm Machine Information

The operation procedure to confirm the machine information of the machine that has been configured is shown as follows.

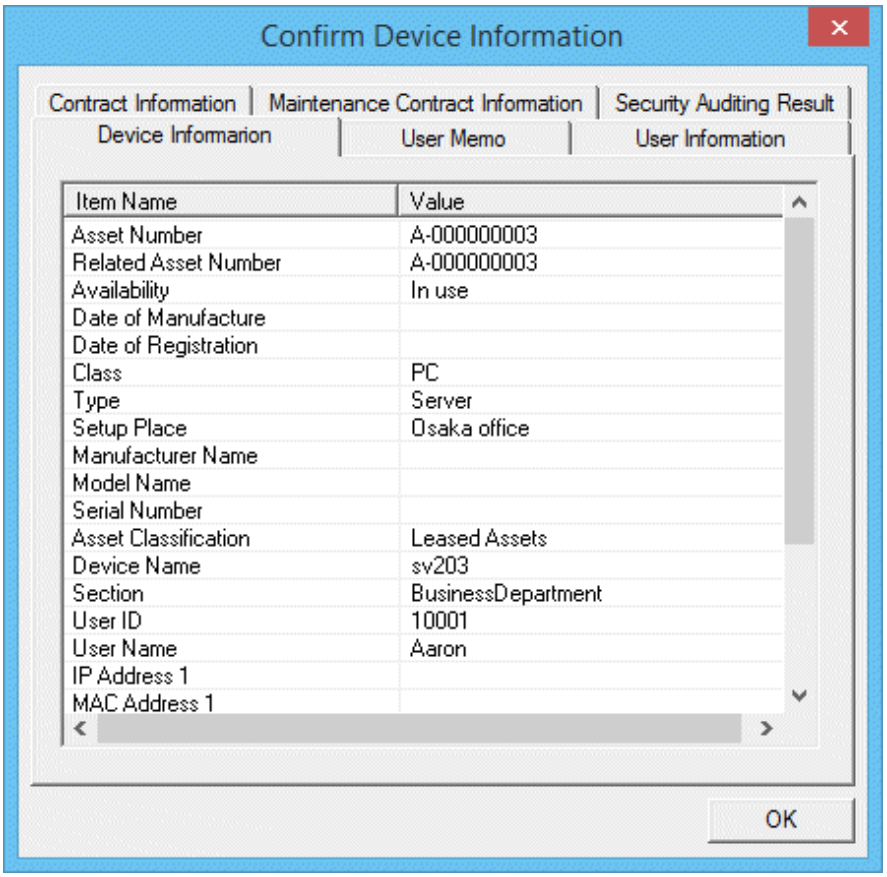
1. Right-click the machine that has been configured, and click **Confirm Device Information** in the displayed menu.

   *The confirmation of machine information in selected status for multiple machines cannot be performed.



   The **Confirm Device Information** window will be displayed.

Device Information tab

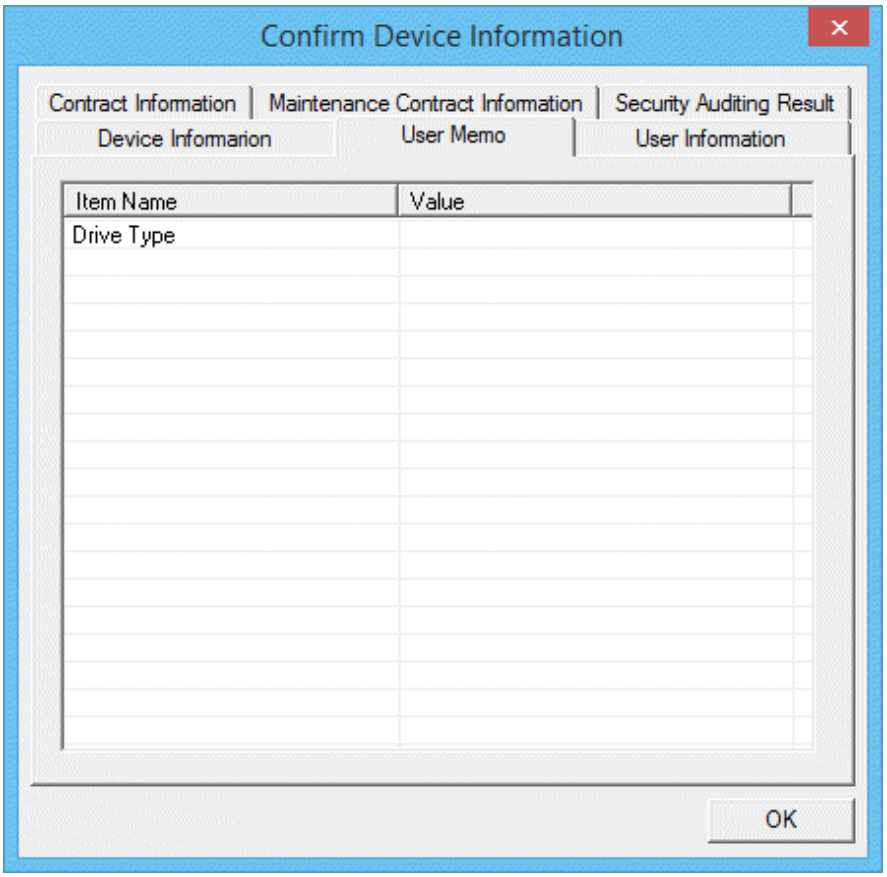


Item	Description
Assets Number	Asset number of machine.
Related Assets Number	Related asset number of machine.
Class	Category information of machine.
Type	Type information of machine.
Setup Place	Setting location information of machine.
Manufacturer Name	Manufacturer name of machine.

Item	Description
Model Name	Model name of machine.
Serial Number.	Serial number of machine.
Asset Classification	Asset classification of machine.
Availability	Availability of machine.
Device Name	The name used as machine.
Date of Manufacture	The year and month when the machine is manufactured.
Date of Registration	Year, month and date of registration to the asset ledger of machine.
Section	Information of section.
Use ID	User ID of the user that uses the machine.
User Name	User name that uses the machine.
Path Name of Link	Data related to machine (e.g. image of machine), as well as folder and URL that contains such data.
Processor Name	Processor name of the PC.
Clock Number	Clock number of CPU of the PC.
Total Memory Capacity	Total memory capacity of PC.
Total Disk Capacity	Total capacity of hard disk of PC.
Total Remaining Disk Capacity	Remaining capacity of hard disk of PC.
OS Name	OS name of PC.
Service Component	Service components applied to PC.
IP Address 1	IP address set for PC. - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/). - IPv6 addresses are separated with a semicolon (;).
IP Address 2	IP address set for PC. - In dual stack environments, separate IPv4 and IPv6 addresses with a forward slash (/). - IPv6 addresses are separated with a semicolon (;).
MAC Address 1	MAC address set for PC.
MAC Address 2	MAC address set for PC.
Collection Information	It shows the existence as PC inventory information on the database of DTP. When existing as PC inventory information, "o" is displayed, and when not existing as PC inventory information, "x" is displayed.
Collection Date/Time	Date and time when information is registered.
Detection Date/Time	Date and time when machine is detected in ADT.
Completion Date of Stocktaking	Date and time when stocktaking has completed.

User Memo tab

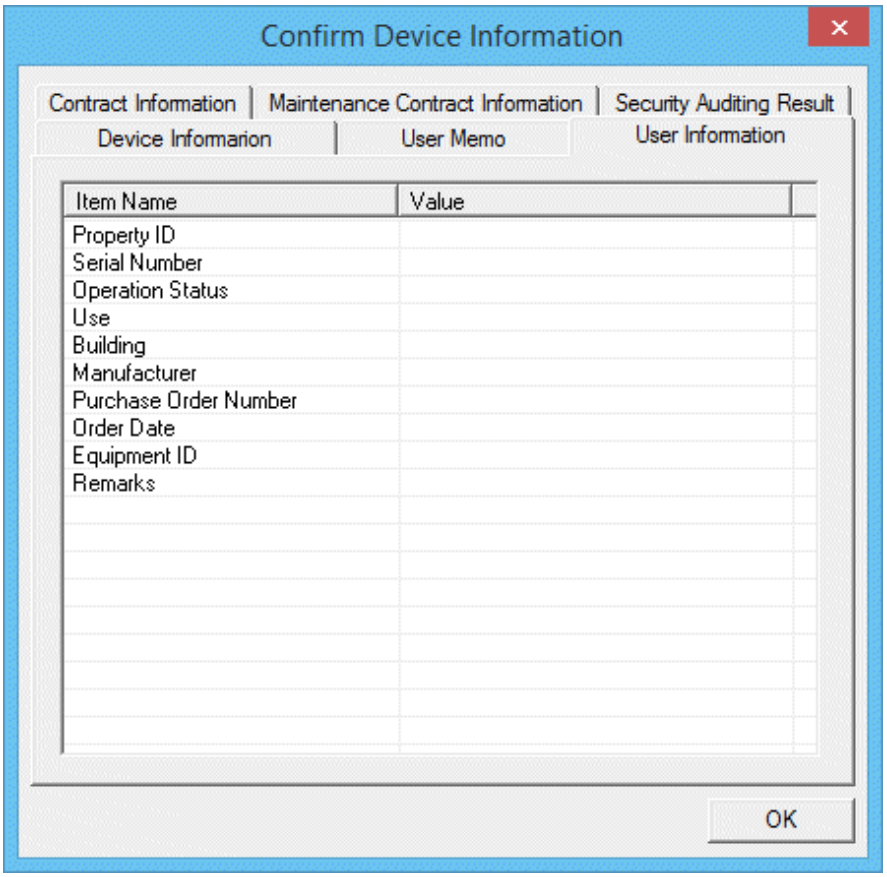
*It is not displayed when all the item names of user memo are "Unused".



Item	Description
User Memo 1~60	User memo of machine.

User Information tab

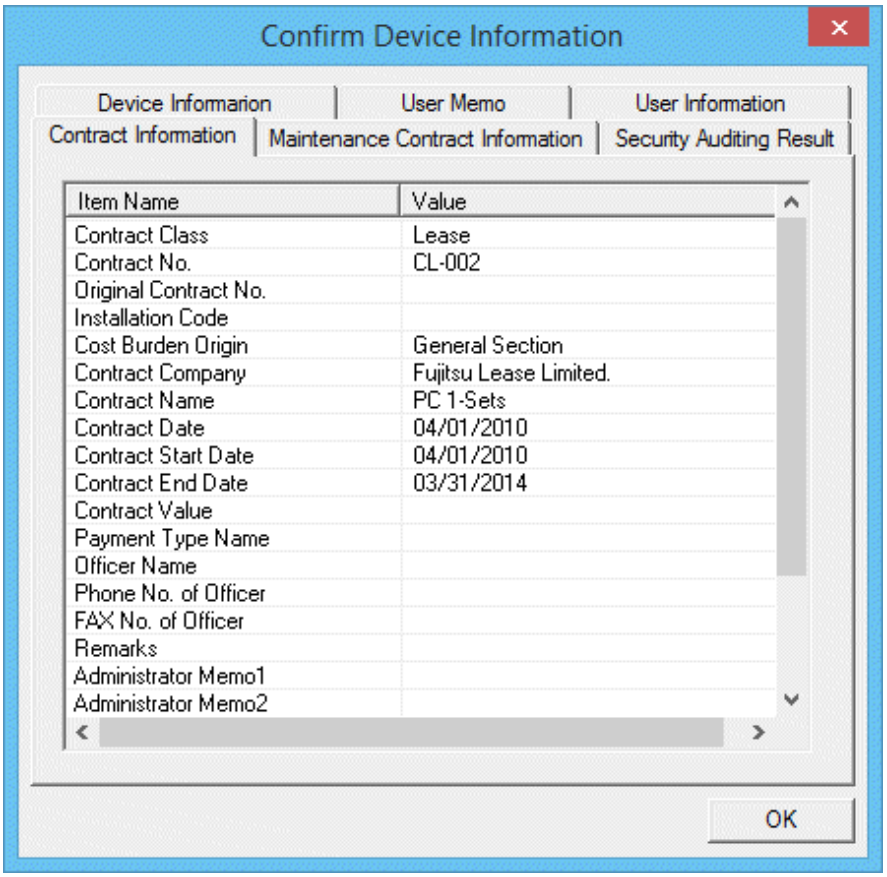
* It is not displayed when all the item names of user information are not defined.



Item	Description
Inherent Item of User Information	The user memo that is set freely as the inventory information of DTP. The item name and user memo set by user will be displayed. For example, when "Property ID" has been set by user, "Property ID" will be displayed.

Contract Information tab

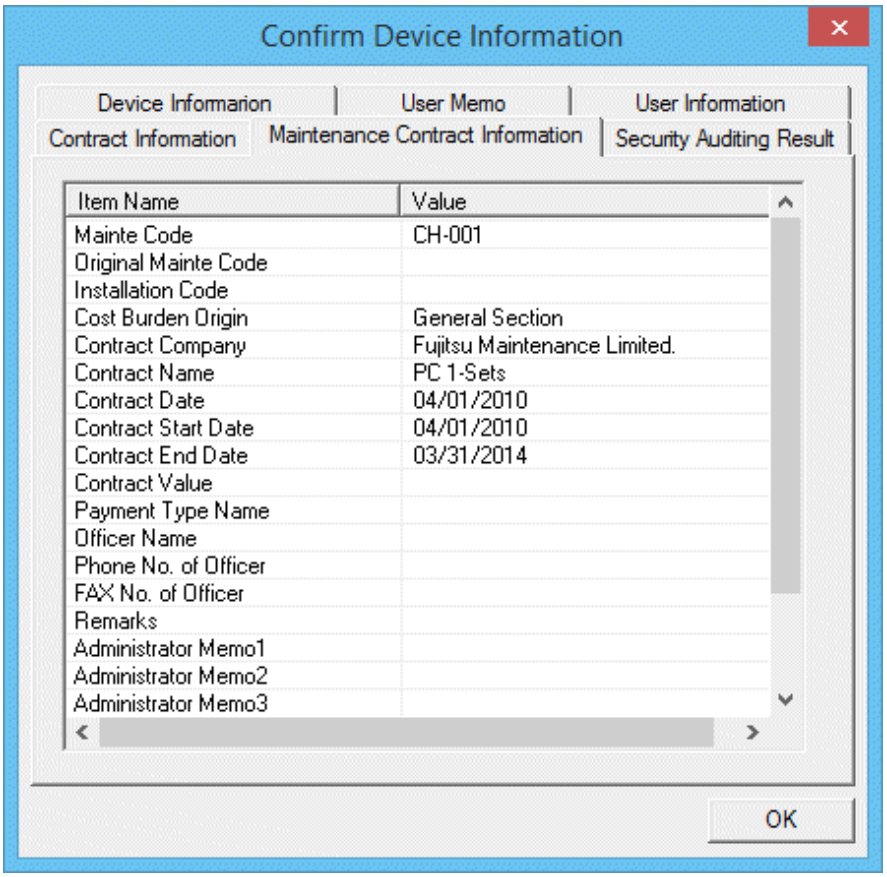
*It is not displayed when the machine has no lease/rental contract.



Item	Description
Contract Class	Category information of contract.
Contract No.	Information of contract number.
Original Contract No.	Information of contract number before contract extension.
Installation Code	Contract No. when the contract is managed by contract company.
Cost Burden Origin	Information of the cost bearing party of contract.
Contract Company	Contracted company name.
Contract Name	Contracted article name.
Contract Date	Contracted date of the contract.
Contract Start Date	Contracted start date of contract.
Contract End Date	Contracted termination date of contract.
Contract Value	Contracted price of contract.
Payment Type Name	Payment method such as monthly payment or yearly payment .etc.
Officer Name	Contract officer name.
Phone No. of Officer	Telephone number of contract officer.
Fax No. of Officer	Fax number of contract officer.
Remarks	Remarks information of contract.
Administrator Memo 1~6	Memo information of contract.

Maintenance Contract Information tab

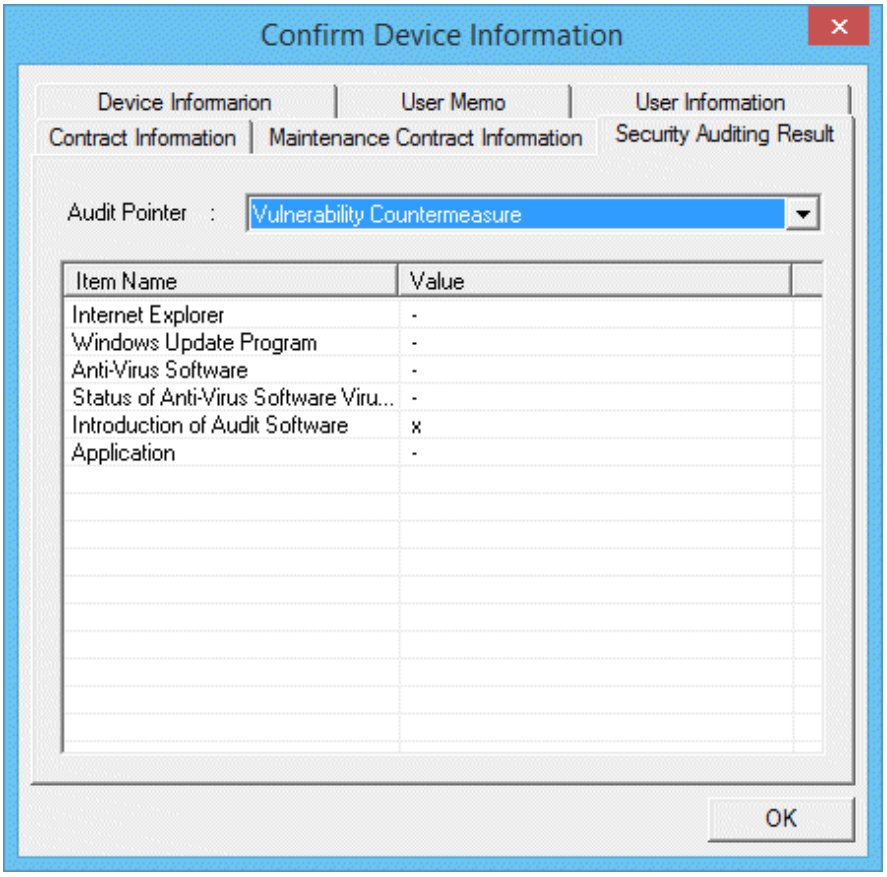
*It is not displayed when the machine is not bounded with any maintenance contract.



Item	Description
Mainte Code	Information of the number of maintenance contract.
Original Mainte Code	Information of the number of maintenance contract before contract extension.
Installation Code	Contract No. when the contract is managed by contract company.
Cost Burden Origin	Information of the cost bearing party of contract.
Contract Company	Contracted company name.
Contract Name	Contracted article name.
Contract Date	Contracted date of the contract.
Contract Start Date	Contracted start date of contract.
Contract End Date	Contracted termination date of contract.
Contract Value	Contracted price of contract.
Payment Type Name	Payment method such as monthly payment or yearly payment .etc.
Officer Name	Contract officer name.
Phone No. of Officer	Telephone number of contract officer.
Fax No. of Officer	Fax number of contract officer.
Remarks	Remarks information of contract.
Administrator Memo1~6	Memo information of contract.

Security Auditing Result tab

* It is not displayed when the category of machine is not PC.



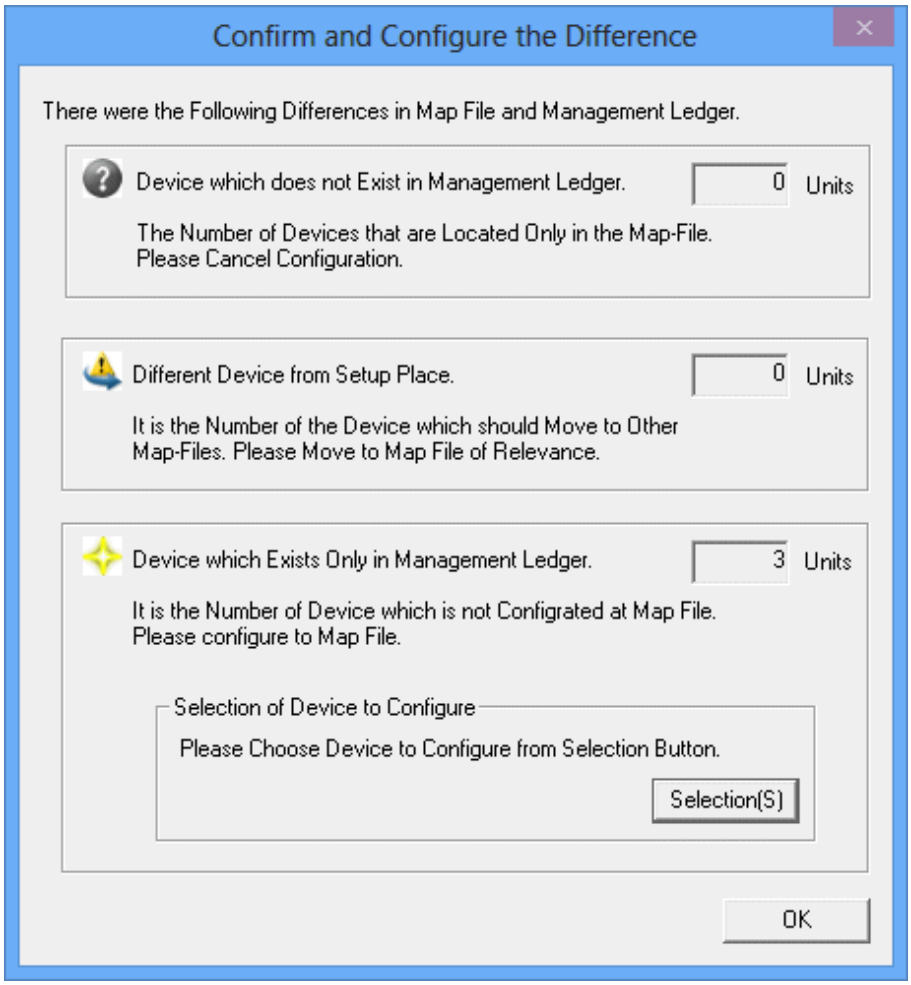
Item	Description
Audit Pointer	Select the Audit Pointer to confirm the result of security auditing. The result of selected Audit Pointer will be displayed in the Auditing Result.
Auditing Result	The result of Audit Pointer will be displayed for each auditing item. When the auditing result is OK, o will be displayed. When the auditing result is failed, **x** will be displayed.

12.3.3 Confirm the Difference with Asset Ledger

Compare the map file with the asset ledger. The operation procedure to confirm the comparison result is shown as follows.

1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Confirm and Configure the Different with Asset Ledger**.

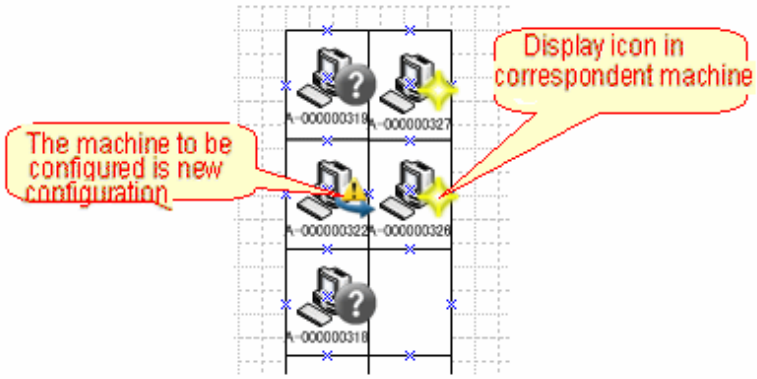
   The **Confirm and Configure the Difference** window will be displayed.



2. After confirming the comparison result, click the **OK** button of **Confirm and Configure the Difference** window.

   The confirmation result will be reflected to the map file.

   (The icon of correspondent machine will be displayed. The machine requires configuration will be newly configured. The machine to be configured can be selected from the **Selection** button of the **Confirm and Configure the Difference** window.)



*From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Hide Confirmation Icon**, each icon displayed in the machine can be hidden.

After the confirmation icon has been set to hidden, repeat the above procedure and the icon can be displayed again.

Perform the following operation according to the displayed icon.

It is the machine in which the asset ledger does not exist.

Right-click the correspondent machine and perform the operation of **Cancel Configuration**.

It is the machine ready to be configured in other map file.

Confirm the setting location of machine. When it is needed to be moved to other map file, right-click the correspondent machine to perform the operation of **Move to Map of Others**.

It is the machine that is newly configured virtually.

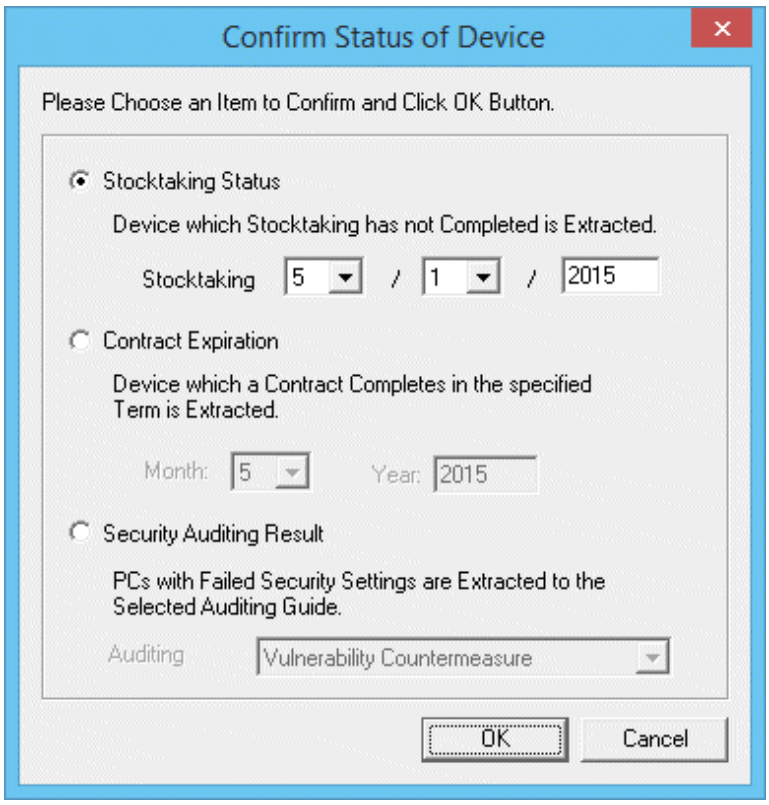
Put the machine configured virtually to a formal configuration position as required.

12.3.4 Confirm Status of Machine

The operation procedure to confirm the machine of specified condition from the machine that has been configured is shown as follows.

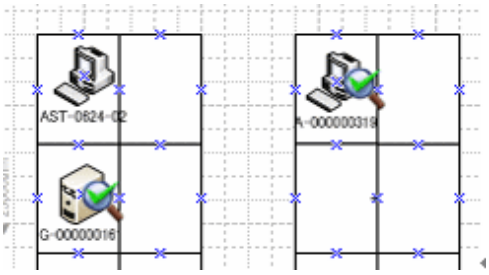
1. From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Confirm Status of Device**.

   The **Confirm Status of Device** window will be displayed.



2. Select the status of one machine to be confirmed, and click the **OK** button.

   For the machine that satisfies condition, the icon of status confirmation will be displayed.



   * From the menu bar of Microsoft(R) Visio(R), select **Desktop Patrol** > **Location Map** > **Hide Confirmation Icon**, the status confirmation icon displayed in the machine can be removed.

   After the confirmation icon has been hidden, repeat the above procedure, the icon can be displayed again.

12.3.5 Icon in Map File

The meaning of icons displayed in map file is as follows.

Icon Image	Icon Name	Description
	Moving Reservation Icon	Icon displayed when reserved for moving to another map for machine
	Status Confirmation Icon	Icon displayed in the machine that matches the following conditions - The machine that matches with search condition in the status confirmation function of machine - The machine exists in the map of others as the machine with same asset management number when saving the map file
	No Ledger Icon	Icon displayed in the machine that does not exists in asset ledger.
	Other Map File Icon	Icon displayed for the machine that has been configured in other map file.
	New Configuration Icon	Icon displayed for the machine that is newly configured

Remarks. "Status Confirmation Icon", "No Ledger Icon", "Other Map File Icon" and "New Configuration Icon" can be hidden through operation of **Desktop Patrol** > **Location Map** > **Hide Confirmation Icons**.

Chapter 13 Output Report

This chapter describes how to output asset information (machine information and contract information) managed by Systemwalker Desktop Patrol and result of security auditing, and power saving setting status .etc. as reports.

Note

About the version and group output result of Microsoft(R) Office Excel

The layout of generated report file and printing result as well as the color scheme of pie chart and bar chart may vary depending on the version of and service pack of Microsoft(R) Office Excel being used.

Note

Reports that do not include smart devices

Smart device information imported to the management ledger is not output to the following reports:

- License usage information report
- Security auditing report
- Power saving settings report
- Power consumption auditing report

13.1 Output Asset Operation Status

The following describes how to output the asset operation status.

- "13.1.1 Procedure"
- "13.1.2 Example of Outputting Asset Operation Status"

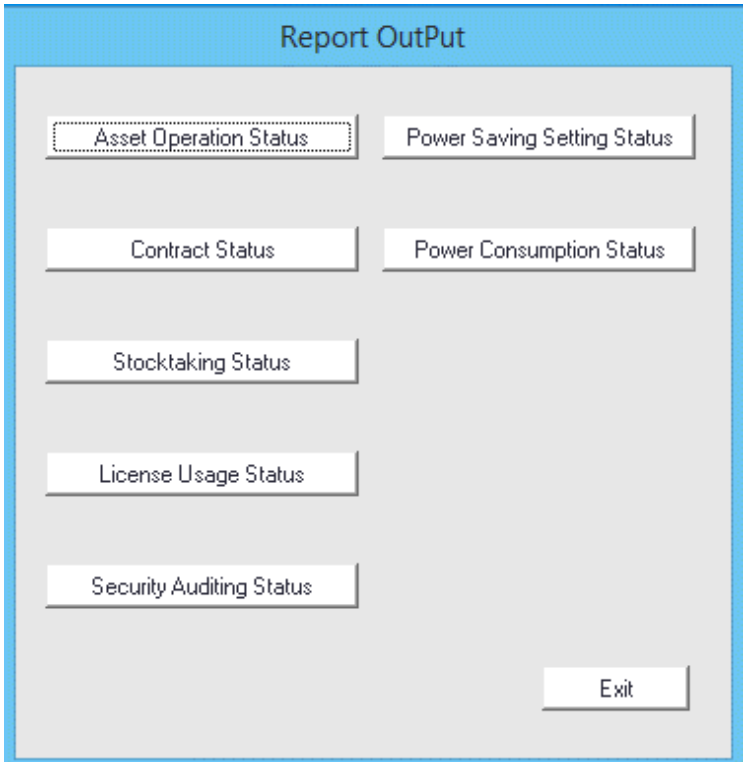
13.1.1 Procedure

The procedure of outputting the asset operation status list is as follows.

1. Log on to the AC menu.

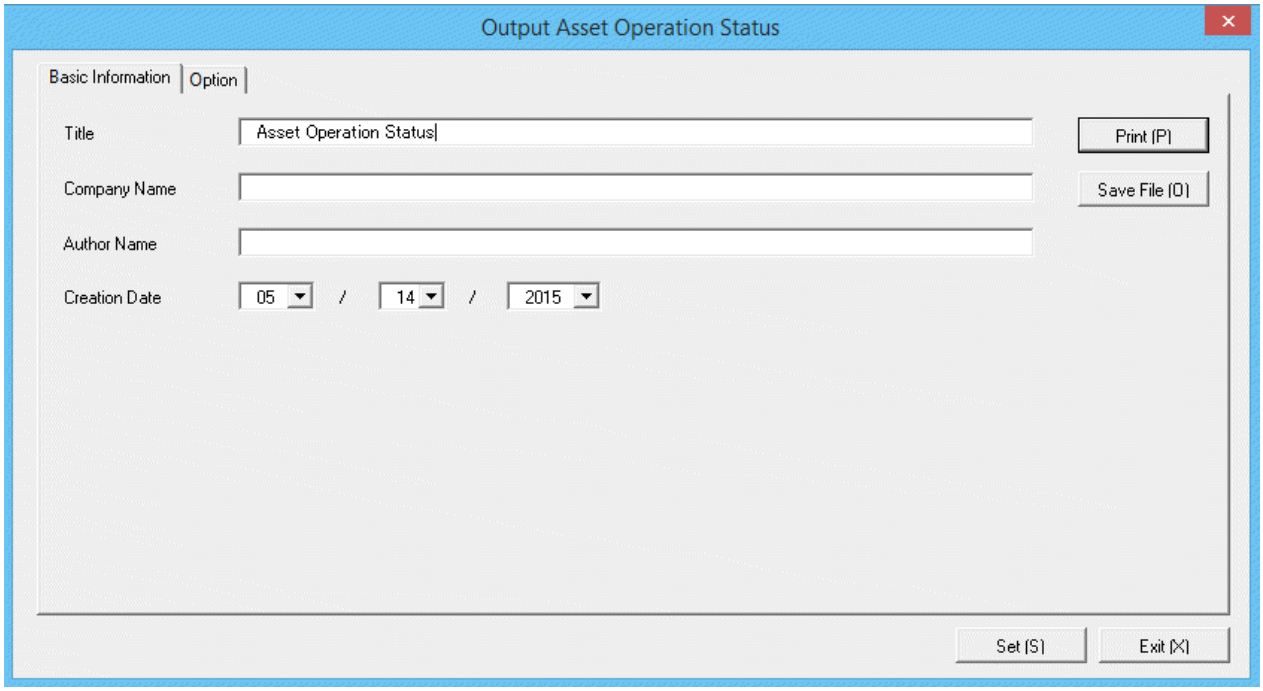
2. Select **Report Output**.

   The following window will be displayed.



3. Click the **Asset Operation Status** button.

   The following window will be displayed.



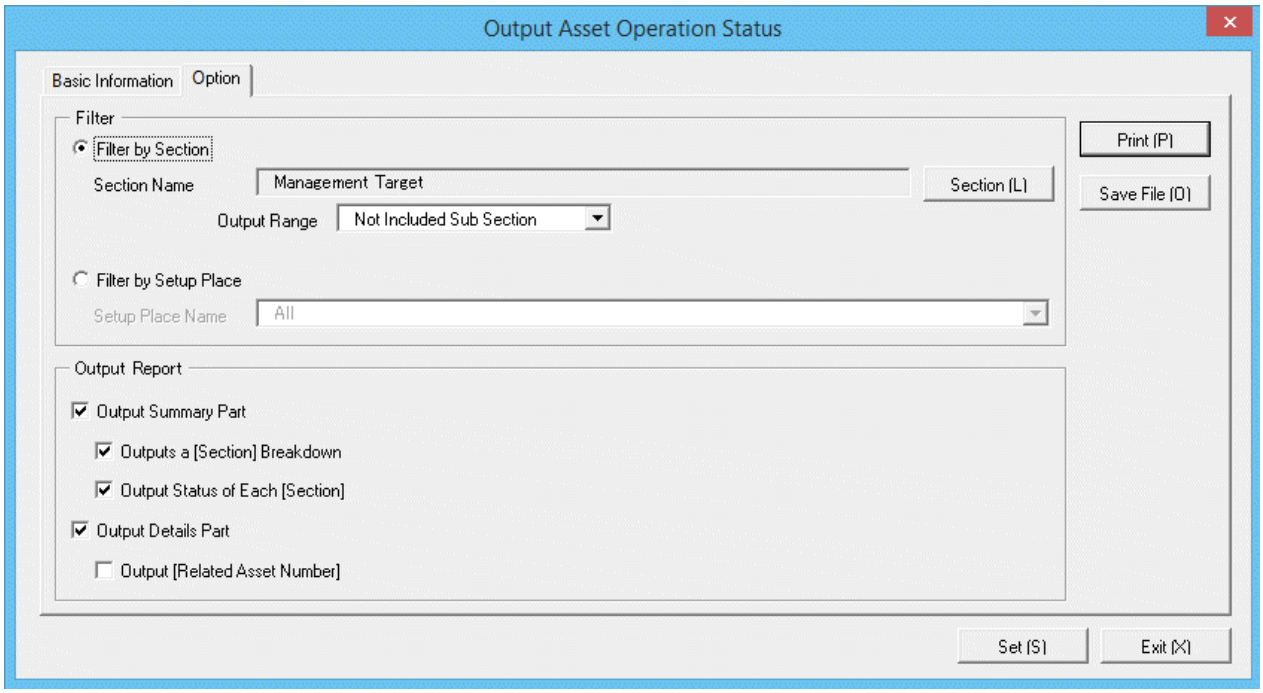
4. Set the items at the time when outputting to report.

   Set the following information.

   In addition, click the **Set** button after setting, and the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth alphanumeric characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Creation Date	Set the creation date to output in report.

The window when the **Option** tab is selected is shown below.



Set the following information.

Tab Name	Item		Description
Option	**Filter**	**Filter by Section**	Select asset operation status list when outputting to report by section unit. **Section Name**: Set the section to be output to report. **Output Range**: Set the filtering range.
		Filter by Setup Place	Select asset operation status list when outputting to report by location unit. **Setup Place Name**: Set the location to be output to report.
	Output Report	**Output Summary Part**	It is selected when outputting the summary part to report. - **Output a Section Breakdown**: Select when outputting items to summary part.

Tab Name	Item		Description
			Select the following and it can be selected only when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name, and select **Entire Section** in the output range of section. - When **Filter by Setup Place** is selected - Select **All** in the location name - **Output Status of Each Section**: Select it when outputting each status in the summary part. Select the following and it can be selected only when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name, and select **Entire Section** in the output range of section. - When **Filter by Setup Place** is selected - Select **All** in the location name
		Output Details Part	Select it when outputting the details part to report. **Output Related Asset Number**: Select when outputting related asset number to the details part of report. It can be selected when only **Output Details Part** is selected.

5. Output report.

   Operate for the following cases.

   In addition, for the relationship between the information set in the previous steps and the report that is output, refer to "13.1.2 Example of Outputting Asset Operation Status" described in the following.

   - Print

     To print the report, click the **Print** button.

   - Save as File

     To save the report as a file, click the **Save File** button.

     The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters..

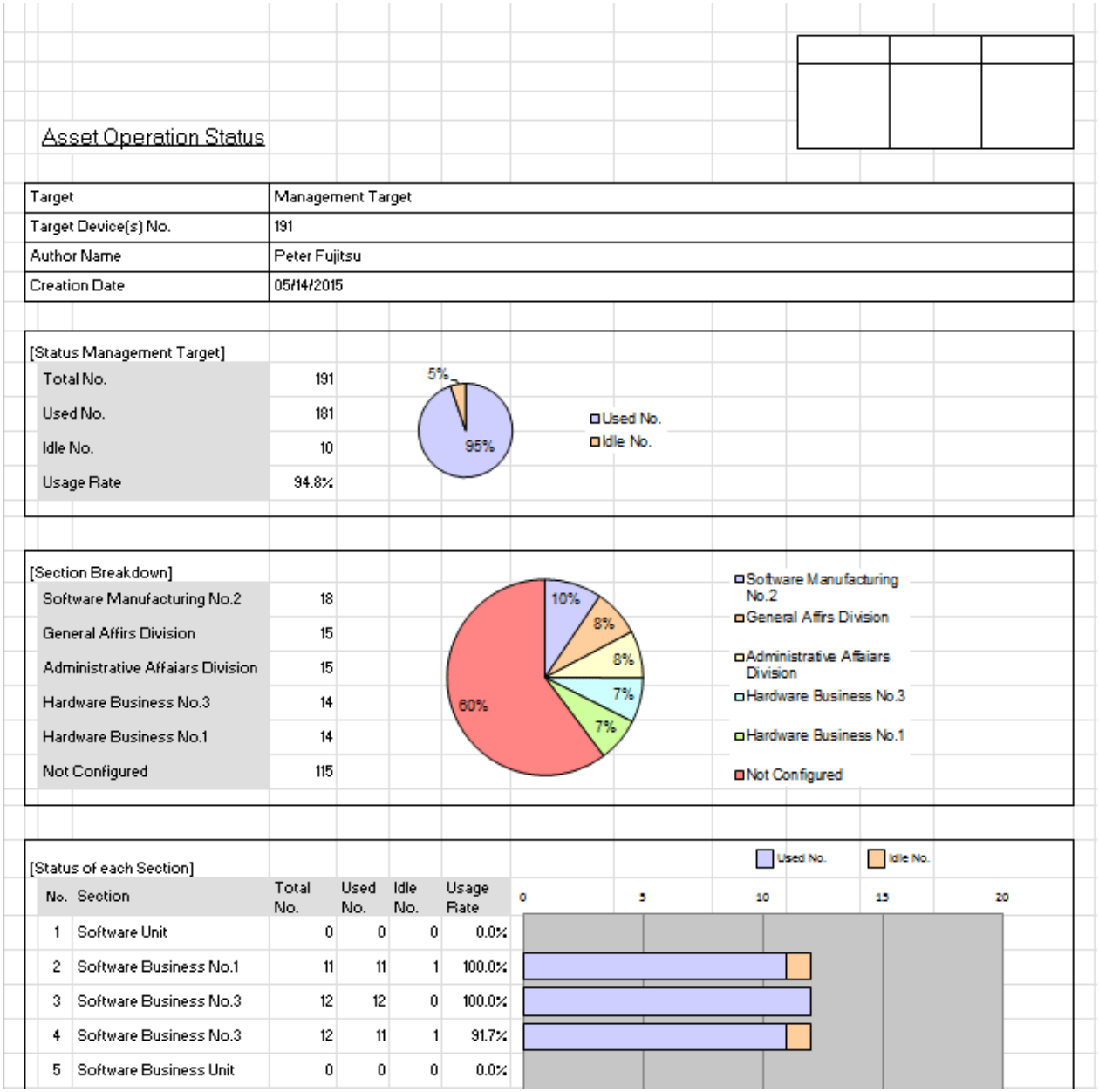
13.1.2 Example of Outputting Asset Operation Status

Report is composed of "Summary Part" and "Details Part". Also, items and status can be output in "Summary Part".

The following describes "Summary Part" and "Details Part" respectively.

Summary part

The "Summary Part" when saved as file is as follows.



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%

The content of the above file is as follows.

Item	Description
Company Name (The set value is displayed)	It is the information set in **Company Name** of the **Basic Information** tab.
Seal Column	It is the column for sealing on the created file. Here, since only the column for sealing is printed, use it freely.
Asset Operation Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Target	It is the name of section or location as object. It is the information set in **Section Name** and **Location Name** of the **Option** tab.

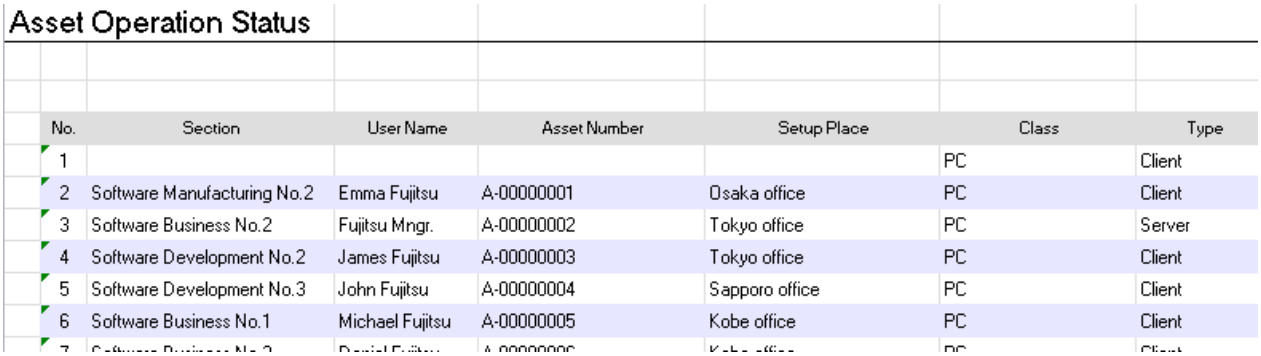
Item		Description
Target Device(s) No.		It is the number of all machines in the section or location as object.
Author Name		Author of the file. it is the information set in **Author Name** of the **Basic Information** tab.
Creation Date		It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Status of Management Target (The selected object is displayed)	**Total No.**	It is the total number of machines in the section or location as object.
	Used No.	It is the number of machines used in the section or location as object.
	Idle No.	It is the number of idle machines in the section or location as object.
	Usage Rate	It is the usage rate of machines in the section or location as object.
Section Breakdown or **Setup Place Breakdown**		It is the proportion of machines held in the section or location as object. The machines owned are ranked in descending order by quantity, and each item of the top 5 and the items of other than top 5 will be displayed.
Status of Each Section or **Status of Each Setup Place**	**No.**	It is the number allocated to the information that has been output.
	Section or **Setup Place**	It is the name of section or location as object. The section or location will be arranged in order and displayed. When **Section Unit** is set in **Extraction Condition** of the **Option** tab, the information of subordinates of the set section will be set.
	Total No.	It is the total number of machines in the section or location as object.
	Used No.	It is the number of machines used in the section or location as object.
	Idle No.	It is the number of idle machines in the section or location as object.
	Usage Rate	It is the usage rate of machines in the section or location as object.

The value displayed in **Target Device(s) No.** and **Status of Management Target** is the total number by adding the number of machines output in **Status of Each Section** or **Status of Each Setup Place** with the number of machines without setting location.

Details part

The "Details Part" when saved as file is as follows.

In addition, maximum 50000 items of information can be output to one sheet. It is output by taking the first to the 50000th item as the "Details Part" sheet, the 50001st item to 100000th item as the "Details Part (2)" sheet, and the 100001st item to 150000th item as the "Details Part (3)" sheet



Asset Operation Status

No.	Section	User Name	Asset Number	Setup Place	Class	Type
1					PC	Client
2	Software Manufacturing No.2	Emma Fujitsu	A-00000001	Osaka office	PC	Client
3	Software Business No.2	Fujitsu Mngr.	A-00000002	Tokyo office	PC	Server
4	Software Development No.2	James Fujitsu	A-00000003	Tokyo office	PC	Client
5	Software Development No.3	John Fujitsu	A-00000004	Sapporo office	PC	Client
6	Software Business No.1	Michael Fujitsu	A-00000005	Kobe office	PC	Client

The content of the above file is as follows. In addition, **Related Asset Number** is ranked and displayed according to ascending order of **Asset Number**.

Item	Description
Asset Operation Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Target	It is the name of section or location as object. It is the information set in **Section Name** and **Location Name** of the **Option** tab.
No.	It is the number allocated to the information that has been output.
Section	It is the information of section.
User Name	It is the user name that uses the machine.
Asset Number	It is the asset number of machine.
Related Asset Number	It is the related asset number of machine.
Setup Place	It is the setting location information of machine.
Class	It is the category information of machine.
Type	It is the type information of machine.
Availability	It is the availability of machine.
Device Name	It is the name to be used as machine.
Collection Date/Time	It is the date and time when information has been registered.

13.2 Output Contract Status

This section describes how to output contract status.

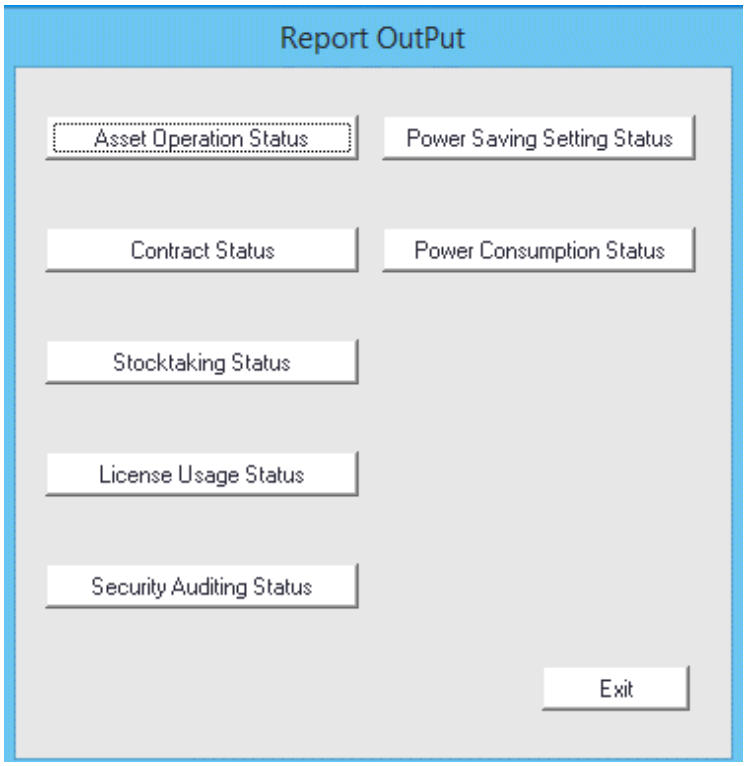
- "13.2.1 Procedure"
- "13.2.2 Example of Outputting Contract Status"

13.2.1 Procedure

The procedure of outputting contract list is as follows.

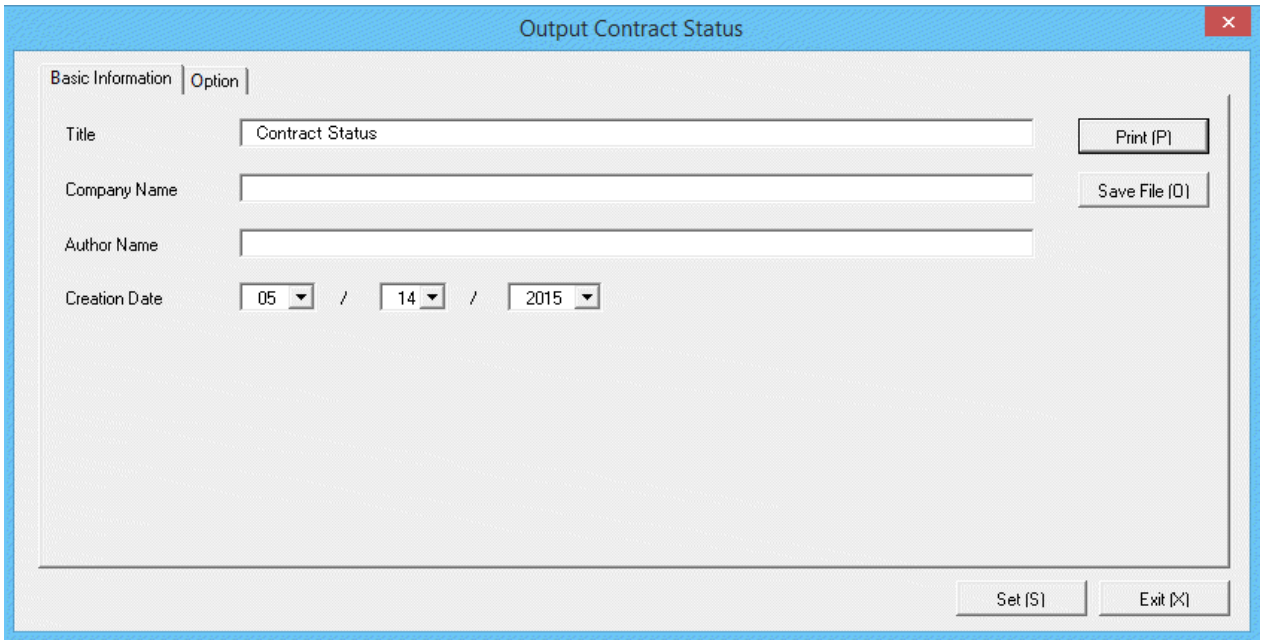
1. Logon to the AC menu.
2. Select **Report Output**.

   The following window will be displayed.



3. Click the **Contract Status** button.

   The following window will be displayed.



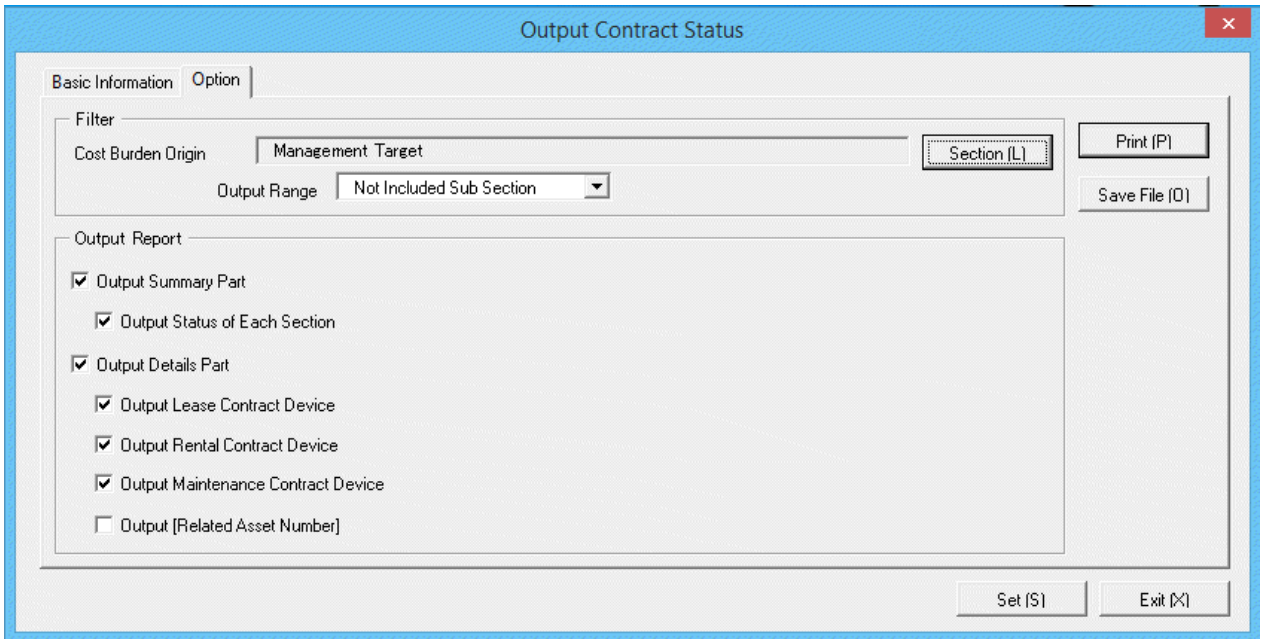
4. Set the items when outputting to report.

   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters or 64 halfwidth characters and symbols can be set.
	Creation Date	Set the creation date to output in report.

The window when the **Option** tab is selected is shown as follows.



Set the following information.

Tab Name	Item		Description
Option	**Filter**	**Cost Burden Origin**	Set the cost bearing party to be output to report.
		Output Range	Set the filtering range.
	Output Report	**Output Summary Part**	It is selected when outputting the summary part to report. **Output Status of Each Section**: It is selected when outputting the status of each section. Select the following. It can only be selected when **Output Summary Part** is selected. - Select **Management Target** in section name - Do not select **Not Configured** in section name, and select **Entire Section** in the output range of section

Tab Name	Item		Description
		Output Details Part	Select it when outputting the details part to report. - **Output Lease Contract Device**: It is selected when outputting the lease contract machine to the details part of report. It can be selected only when **Output Details Part** is selected. - **Output Rental Contract Device**: It is selected when outputting the rental contract machine to the details part of report. It can be selected only when **Output Details Part** is selected. - **Output Maintenance Contract Device**: It is selected when outputting the maintenance contract machine to the details part of report. It can be selected only when **Output Details Part** is selected. - **Output Related Asset Number**: Select when outputting related asset number to the details part of report. It can be selected only when **Output Details Part** is selected.

5. Output report.

   Operate for the following cases.

   In addition, for relationship between the information set according to previous steps and the report that has been output, refer to "13.2.2 Example of Outputting Contract Status" described in the following.

   - Print

     To print the report, click the **Print** button.

   - Save as file

     To save the report as a file, click the **Save File** button.

     The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

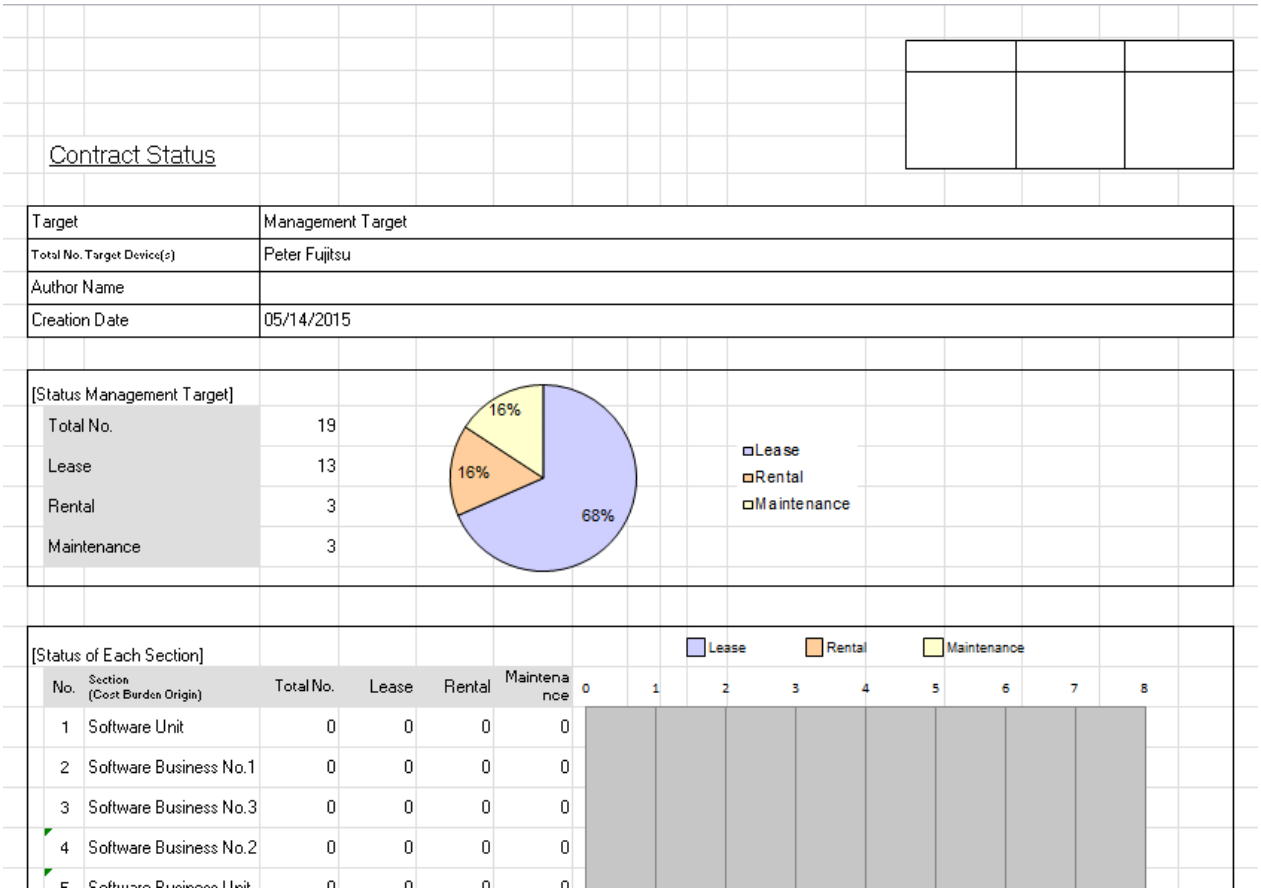
13.2.2 Example of Outputting Contract Status

Report is composed of "Summary Part" and "Details Part". In addition, status of each section can be output in "Summary Part", the lease/rental/maintenance contract information can be output in "Details" part.

The following describes "Summary Part" and "Details Part" respectively.

Summary part

The "Summary Part" when saved as file is as follows.



Contract Status

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

[Status Management Target]

Total No.	19
Lease	13
Rental	3
Maintenance	3

[Status of Each Section]

No.	Section (Cost Burden Origin)	Total No.	Lease	Rental	Maintenance
1	Software Unit	0	0	0	0
2	Software Business No.1	0	0	0	0
3	Software Business No.3	0	0	0	0
4	Software Business No.2	0	0	0	0

The content of the above file is as follows.

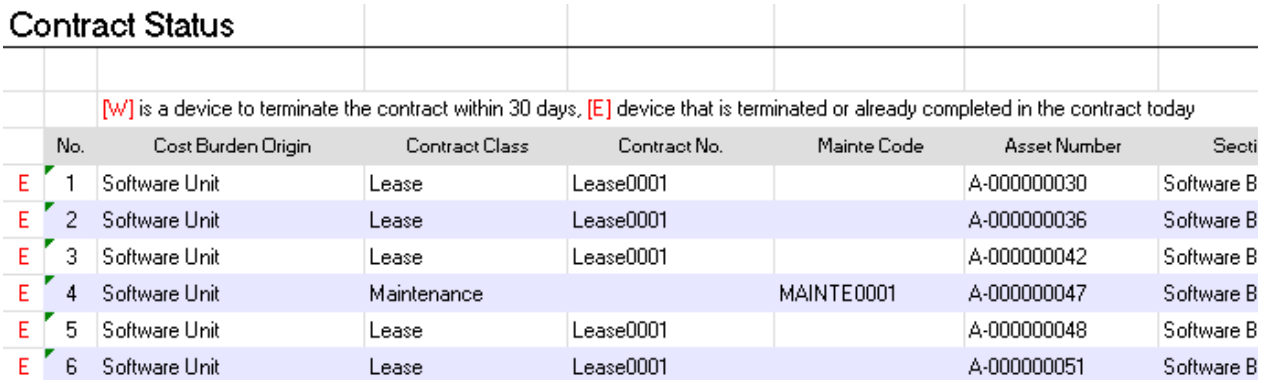
Item		Description
Company Name (The set value is displayed)		It is the information set in **Company Name** of the **Basic Information** tab.
Seal Column		It is the column for sealing on the created file. Only the column for sealing will be printed here, use it freely.
Contract Status (The set value is displayed)		It is the information set in **Title** of the **Basic Information** tab.
Target		It is the name of cost bearing party as object. It is the information set in **Cost Bearing Parity** of the **Option** tab.
Total No. Target Device(s)		It is the total number of machines that have been allocated to the contract among all machines in the cost bearing party as object.
Author Name		Author of the file. it is the information set in **Author Name** of the **Basic Information** tab.
Creation Date		It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Status Management Target (The	**Total No.**	It is the total number of machines that have been allocated to the contract among all machines in the cost bearing party as object.

Item		Description
selected object is displayed)	**Lease**	Number of all least contract machines in the cost bearing party as object.
	Rental	Number of all rental contract machines in the cost bearing party as object.
	Maintenance	Number of all maintenance contract machines in the cost bearing party as object.
Status of Each Section	**No.**	It is the number allocated to the information that has been output.
	Section (Cost Burden Origin)	It is the name of section (Cost Burden Origin) as object. The name of section (Cost Burden Origin) are ranked and displayed in sequence. The information under the set section (Cost Burden Origin) will be output.
	Total No.	It is the total number of machines that have been allocated to the contract among all machines in the cost bearing party as object.
	Lease	Number of all least contract machines in the cost bearing party as object.
	Rental	Number of all rental contract machines in the cost bearing party as object.
	Maintenance	Number of all maintenance contract machines in the cost bearing party as object.

Details part

The "Details Part" when saved as file is as follows.

In addition, maximum 50000 items of information can be output to one sheet. It is output by taking the first to the 50000th item as the "Details Part" sheet, the 50001st item to 100000th item as the "Details Part (2)" sheet, and the 100001st item to 150000th item as the "Details Part (3)" sheet.



Contract Status

[W] is a device to terminate the contract within 30 days, [E] device that is terminated or already completed in the contract today

	No.	Cost Burden Origin	Contract Class	Contract No.	Mainte Code	Asset Number	Secti
E	1	Software Unit	Lease	Lease0001		A-000000030	Software B
E	2	Software Unit	Lease	Lease0001		A-000000036	Software B
E	3	Software Unit	Lease	Lease0001		A-000000042	Software B
E	4	Software Unit	Maintenance		MAINTE0001	A-000000047	Software B
E	5	Software Unit	Lease	Lease0001		A-000000048	Software B
E	6	Software Unit	Lease	Lease0001		A-000000051	Software B

The content of the above file is as follows. In addition, **Related Asset Number** is ranked and displayed according to ascending order of **Asset Number**.

Item	Description
Contract Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.

Item	Description
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Target	It is the name of cost bearing party as object. It is the information set in **Cost Bearing Parity** of the **Option** tab.
W or **E**	It shows the status of contract term. - **W** Display in case of the machine whose contract term will terminate within 30 days. - **E** Display in case of the machine whose contract term will terminate on the current day or has already terminated.
No.	It is the number allocated to the information that has been output.
Cost Burden Origin	It is the information of cost bearing party.
Contract Class	It is the information of contract category.
Contract No.	It is the information of contract number.
Mainte Code	It is the information of maintenance contract number.
Asset Number	It is the asset number of machine.
Related Asset Number	It is the related asset number of machine.
Section	It is the information of section.
User Name	It is the user name that uses the machine.
Setup Place	It is the setting location information of machine.
Class	It is the category information of machine.
Type	It is the type information of machine.
Availability	It is the availability of machine.
Collection Date/Time	It is the date and time when information has been registered.
Contract End Date	Termination date of the established contract.

Remarks. In case of section administrator, for machines out of the range of section they belongs, only the following information can be output.

- **Cost Burden Origin**
- **Contract Class**
- **Contract No.**
- **Mainte Code**
- **Asset Number**
- **Section**
- **User Name**
- **Class**
- **Type**
- **Contract End Date**

13.3 Output Stocktaking Status

This section describes how to output the stocktaking status.

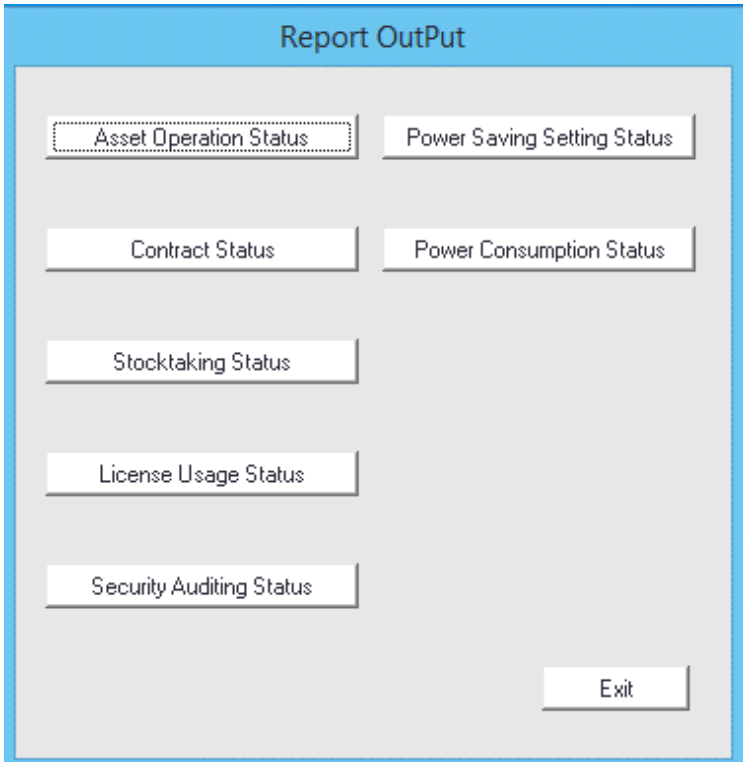
- "13.3.1 Procedure"
- "13.3.2 Example of Outputting Stocktaking Status"

13.3.1 Procedure

The procedure of outputting stocktaking status is as follows.

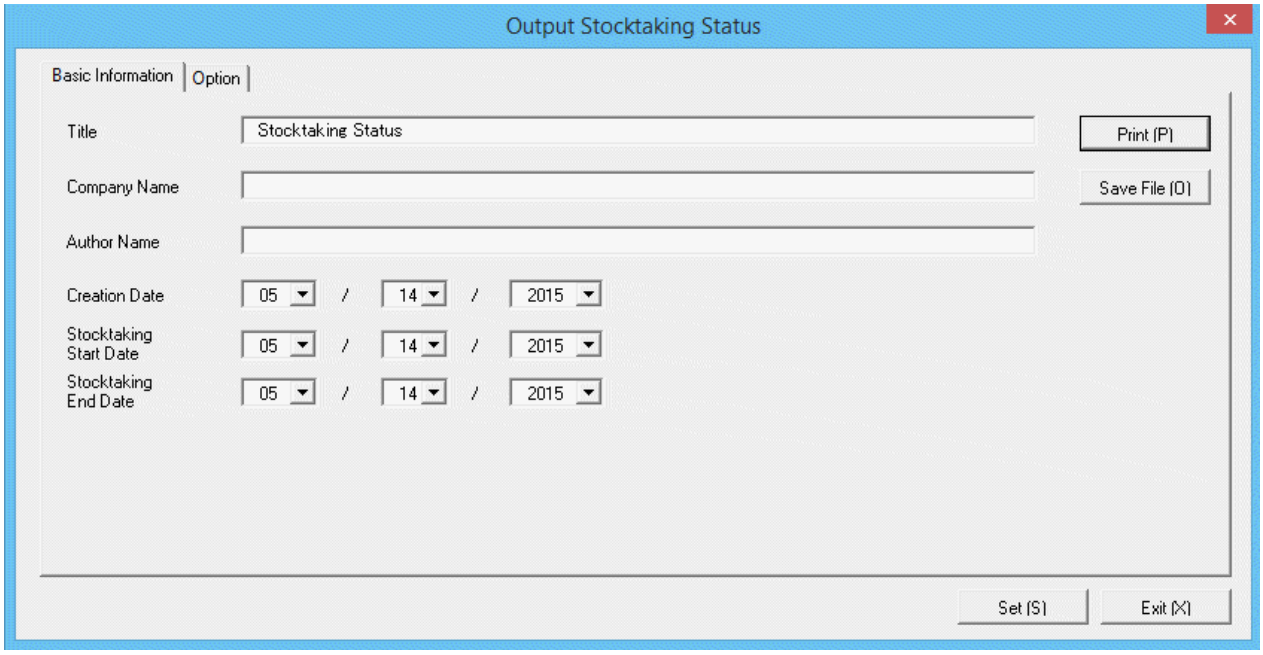
1. Logon to the AC menu.
2. Select **Report Output**.

   The following window will be displayed.



3. Click the **Stocktaking Status** button.

   The following window will be displayed.



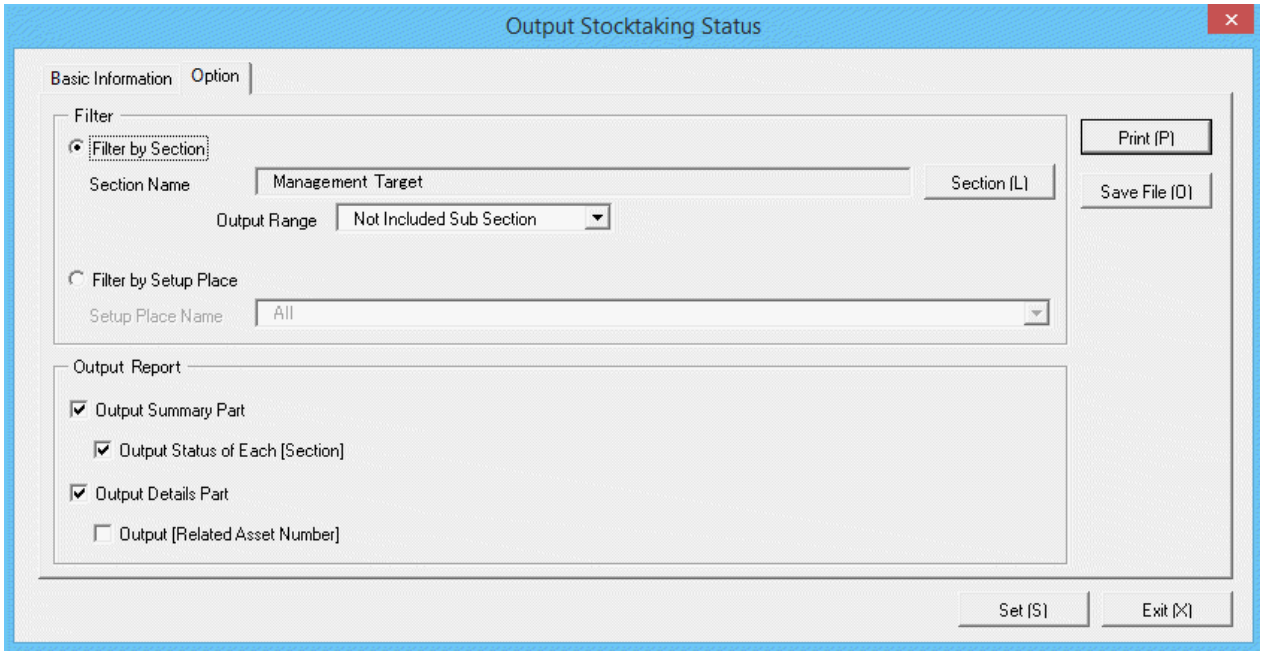
4. Set the items when outputting to report.

   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth alphanumeric characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Creation Date	Set the creation date to output in report.
	Stocktaking Start Date	Set the start date of stocktaking to be output to report.
	Stocktaking End Date	Set the finish date of stocktaking to be output to report.

The window when the **Option** tab is selected is shown as follows.



Set the following information.

Tab Name	Item		Description
Option	**Filter**	**Filter by Section**	Select when outputting the stocktaking status to report by section unit. **Filter by Section**: Set the section to be output to report. **Output Range**: Set the filtering range.
		Filter by Setup Place	Select when outputting the stocktaking status to report by location unit. **Filter by Setup Place**: Set the location to be output to report.
	Output Report	**Output Summary Part**	It is selected when outputting the summary part to report. - **Output Status of Each Section**: Select it when outputting each status in the summary part. Select the following. It can only be selected when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name, and select **Entire Section** in the output range of section. - When **Filter by Setup Place** is selected - Select **All** in the location name
		Output Details Part	Select it when outputting the details part to report. **Output Related Asset Number**: Select it when outputting related asset number to the details part

Tab Name	Item		Description
			of report. It can be selected only when **Output Details Part** is selected.

5. Output report.

   Operate for the following cases.

   In addition, for relationship between the information set according to previous steps and the report that has been output, refer to "13.3.2 Example of Outputting Stocktaking Status" described in the following.

   - Print

     To print the report, click the **Print** button.

   - Save as File

     To save the report as a file, click the **Save File** button.

     The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

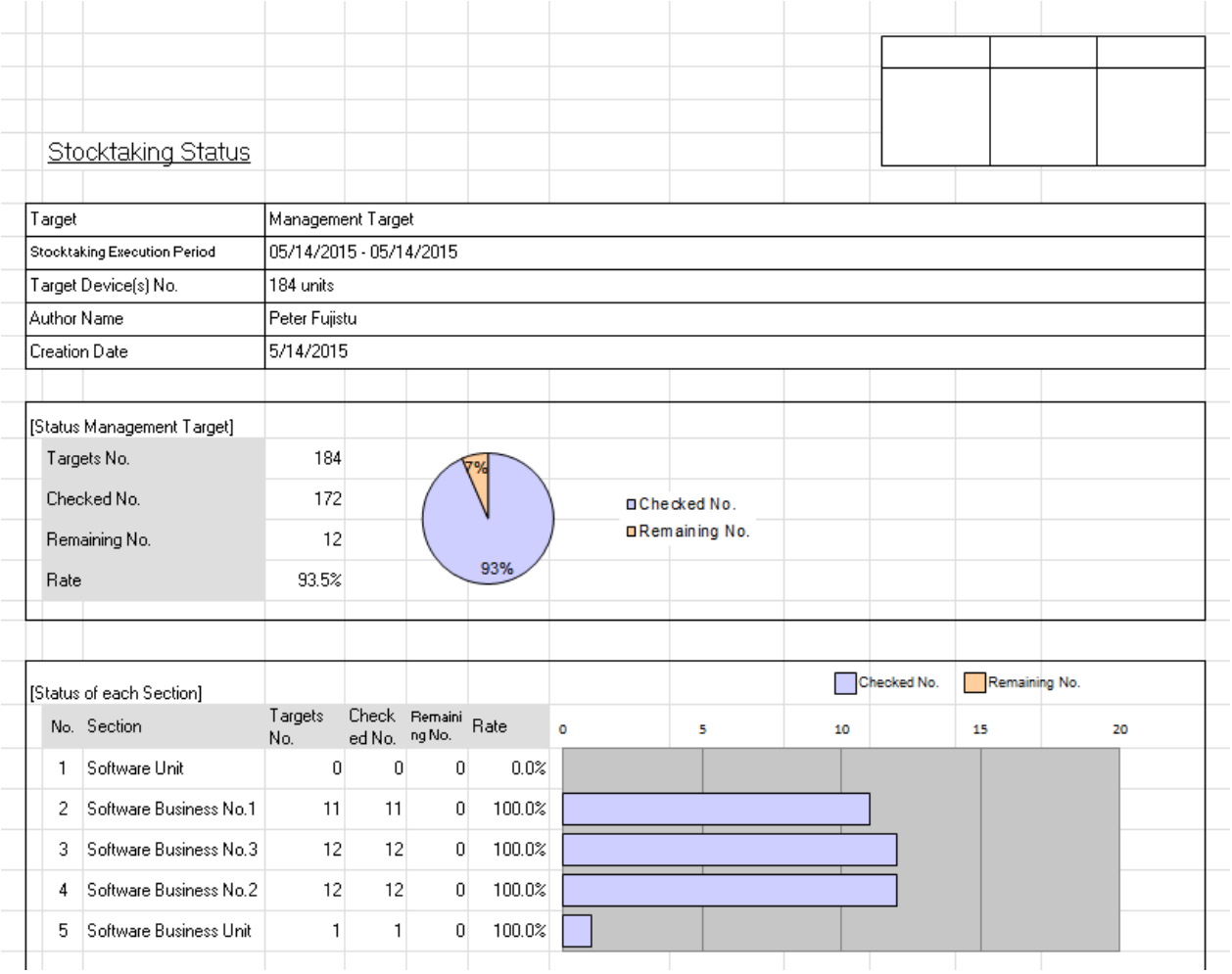
13.3.2 Example of Outputting Stocktaking Status

Report is composed of "Summary Part" and "Details Part". In addition, status can be output in "Summary Part".

The following describes "Summary Part" and "Details Part" respectively.

Summary part

The "Summary Part" when saved as file is as follows.



Stocktaking Status

Target	Management Target
Stocktaking Execution Period	05/14/2015 - 05/14/2015
Target Device(s) No.	184 units
Author Name	Peter Fujistu
Creation Date	5/14/2015

[Status Management Target]

Targets No.	184
Checked No.	172
Remaining No.	12
Rate	93.5%

[Status of each Section]

No.	Section	Targets No.	Checked No.	Remaining No.	Rate
1	Software Unit	0	0	0	0.0%
2	Software Business No.1	11	11	0	100.0%
3	Software Business No.3	12	12	0	100.0%
4	Software Business No.2	12	12	0	100.0%
5	Software Business Unit	1	1	0	100.0%

The content of the above file is as follows.

Item	Description
Company Name (The set value is displayed)	It is the information set in **Company Name** of the **Basic Information** tab.
Seal Column	It is the column for sealing on the created file. Only the column for sealing will be printed here, use it freely.
Stocktaking Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Target	It is the name of section or location as Target. It is the information set in **Section Name** and **Setup Place Name** of the **Option** tab.
Stocktaking Execution Period	It is the execution period of stocktaking. It is the information set in **Stocktaking Start Date** and **Stocktaking End Date** of the **Basic Information** tab.
Target Device(s) No.	It is the number of all machines in section or location as object.
Author Name	Author of the file. It is the information set in **Author Name** of the **Basic Information** tab.
Creation Date	It is the date when file has been created.

Item		Description
		It is the information set in **Creation Date** of the **Basic Information** tab.
Status Management Target (The selected object is displayed)	**Targets No.**	Number of machines for stocktaking in the section or location as object.
	Checked No.	Number of machines with completed stocktaking in the section or location as object.
	Remaining No.	Number of machines with stocktaking not completed in the section or location as object.
	Rate	It is the achievement rate of stocktaking in the section or location as object.
Status of Each Section or **Status of Each Setup Place**	**No.**	It is the number allocated to the information that has been output.
	Section or **Setup Place**	It is the name of section or location as the object. The names of section or location are arranged and displayed in sequence. When setting **Section Unit** is **Extraction Condition** of the **Option** tab, the information of subordinates of the set section will be set.
	Targets No.	Number of machines for stocktaking in the section or location as object.
	Checked No.	Number of machines with completed stocktaking in the section or location as object.
	Remaining No.	Number of machines with stocktaking not completed in the section or location as object.
	Rate	It is the achievement rate of stocktaking in the section or location as object.

The value displayed in **Target Device(s) No.** and **Status of Management Target** is the total number by adding the number of machines output in **Status of Each Section** or **Status of Each Setup Place** with the number of machines without setting location.

Details part

The "Details Part" when saved as file is as follows.

In addition, maximum 50000 items of information can be output to one sheet. It is output by taking the first to the 50000th item as the "Details Part" sheet, the 50001st item to 100000th item as the "Details Part (2)" sheet, and the 100001st item to 150000th item as the "Details Part (3)" sheet.

Stocktaking Status

[E] The Device stocktaking is not yet implemented

Stocktaking

No.	Section	User Name	Asset Number	Stocktaking Status	Collection Date/Time	Setup Place	Cla
1					05/12/2015 08:55:16	Other office	PC
2	Software Development No.2	Emma Fujitsu	A-00000001	o	05/11/2015 19:57:59	Other office	PC
3	Software Business No.2	Fujitsu Mngr.	A-00000002	o	05/07/2015 19:19:57	kobe	PC
4	Software Development No.2	James Fujitsu	A-00000003	o	05/07/2015 19:21:57	headquarters	PC
5	Hardware Development No.3	John Fujitsu	A-00000004	o	05/07/2015 21:53:03	headquarters	PC
6	Software Business No.1	Michael Fujitsu	A-00000005	o	05/07/2015 21:54:51	kobe	PC

The content of the above file is as follows. In addition, **Related Asset Number** is ranked and displayed according to ascending order of **Asset Number**.

Item	Description
Stocktaking Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Stocktaking Period	It is the execution period of stocktaking. It is the information set in **StockTaking Start Date** and **StockTaking End Date** of the **Basic Information** tab.
Target	It is the name of section or location as object. It is the information set in **Section Name** and **Location Name** of the **Option** tab.
E	Display in case of the machine with stocktaking not completed.
No.	It is the number allocated to the information that has been output.
Section	It is the information of section.
User Name	It is the user name that uses the machine.
Asset Number	It is the asset number of machine.
Related Asset Number	It is the related asset number of machine.
Stocktaking Status	It is the stocktaking status of machine. **o** indicates the machine with completed stocktaking, **o** indicates the machine with stocktaking not completed.
Collection Date/Time	It is the date and time when information has been registered.
Setup Place	It is the setting location information of machine.
Class	It is the category information of machine.
Type	It is the type information of machine.
Availability	It is the availability of machine.

13.4 Output License Usage Status

This section describes how to output license usage status.

- "13.4.1 Preparation"
- "13.4.2 Procedure"
- "13.4.3 Example of Outputting License Usage Status"

To use this function, the authority of "System Account" is required.

13.4.1 Preparation

The license usage status outputs the license information managed by Systemwalker Desktop Patrol.

Therefore, if license management is not executed by Systemwalker Desktop Patrol, the license usage status cannot be output.

To output license usage status, perform license management through Systemwalker Desktop Patrol.

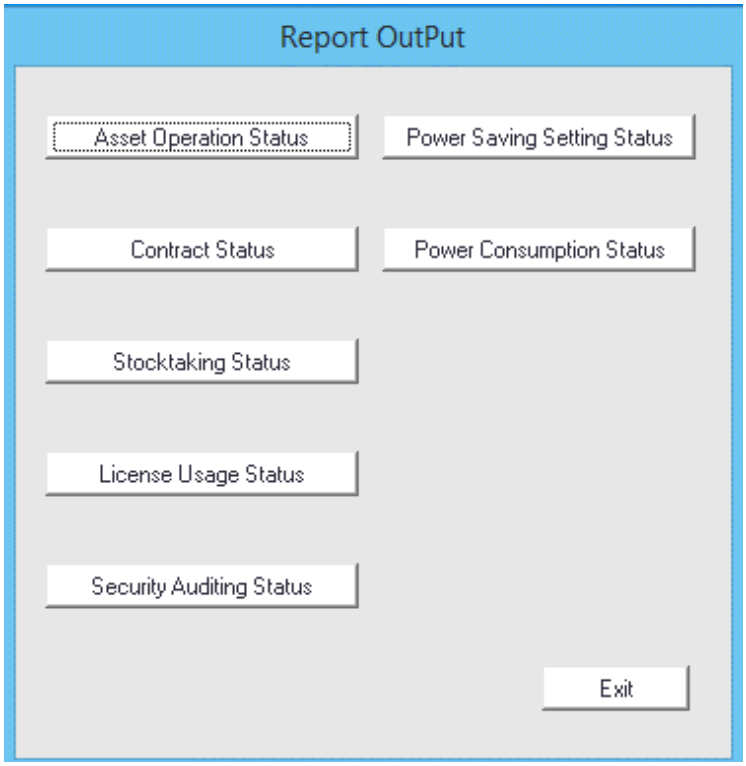
For license management of Systemwalker Desktop Patrol, refer to "Chapter 5 License Management".

13.4.2 Procedure

The procedure of outputting license usage status is as follows.

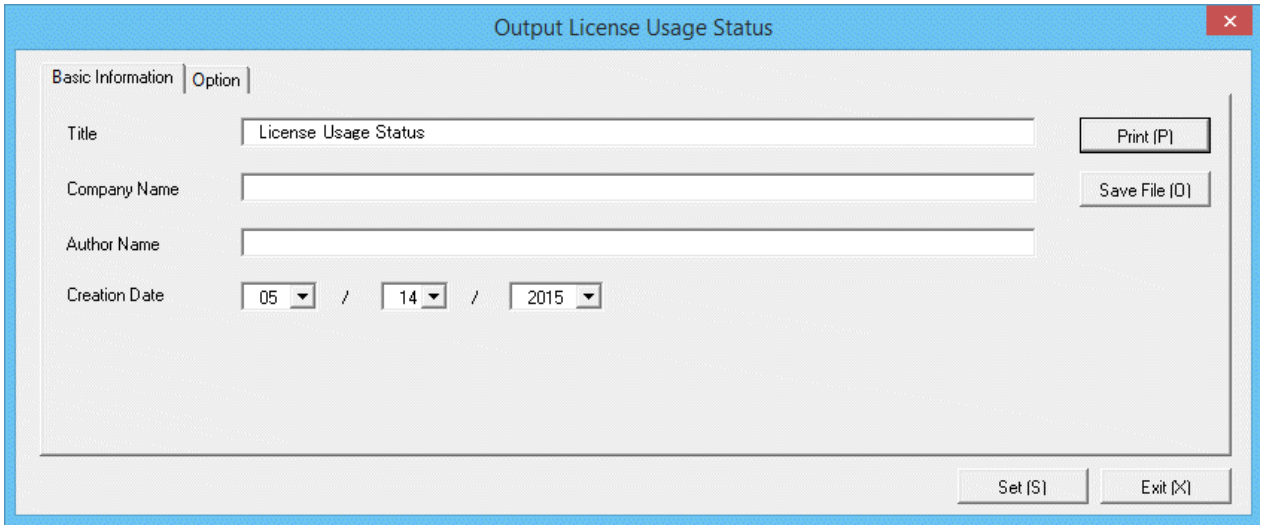
1. Logon to the AC menu.
2. Select **Report Output**.

   The following window will be displayed.



3. Click the **License Usage Status** button.

   The following window will be displayed.



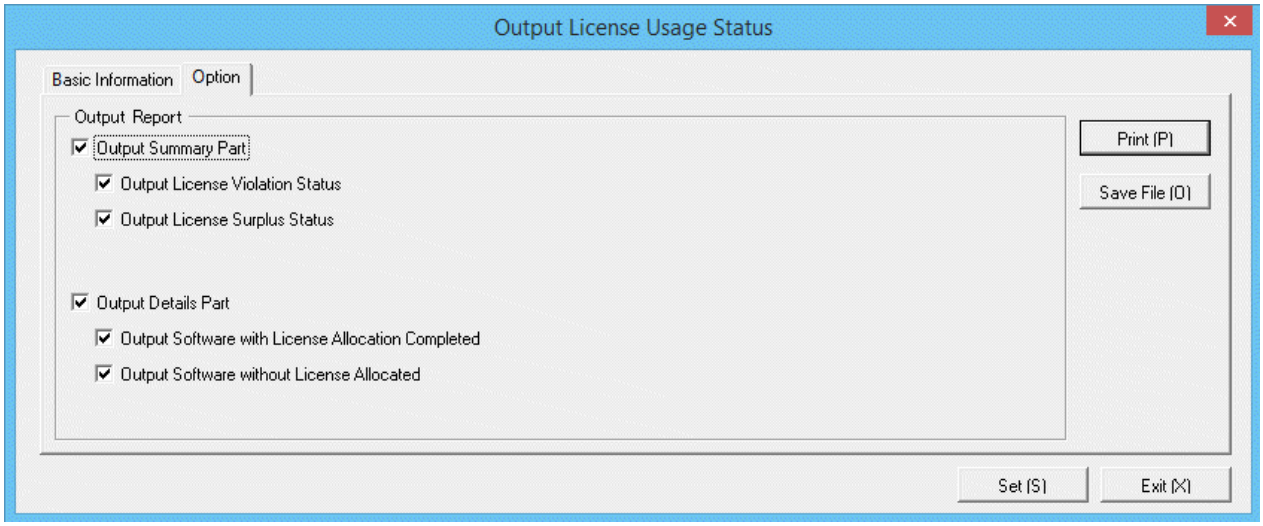
4. Set the items when outputting to report.

   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth alphanumeric characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Creation Date	Set the creation date to output in report.

The window when the **Option** tab is selected is shown as follows.



Set the following information.

Tab Name	Item		Description
Option	**Output Report**	**Output Summary Part**	It is selected when outputting the summary part to report. - **Output License Violation Status**: Select it when outputting the license violation status to the summary part of report. It can be selected only when **Output Summary Part** is selected. - **Output License Surplus Status**: Select it when outputting the license surplus status to the summary part of report. It can be selected only when **Output Summary Part** is selected.
		Output Details Part	Select it when outputting the details part to report. - **Output Software with License Allocation Completed**: Select it when outputting the software with License allocated to the details part of report.

Tab Name	Item		Description
			It can be selected only when **Output Details Part** is selected. - **Output Software without License Allocated**: Select it when outputting the software without License allocated to the details part of report. It can be selected only when **Output Details Part** is selected.

5. Output report.

   Operate for the following cases.

   In addition, for relationship between the information set according to previous steps and the report that has been output, Refer to "13.4.3 Example of Outputting License Usage Status" described in the following.

   - Print

     To print the report, click the **Print** button.

   - Save as File

     To save the report as a file, click the **Save File** button.

     The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

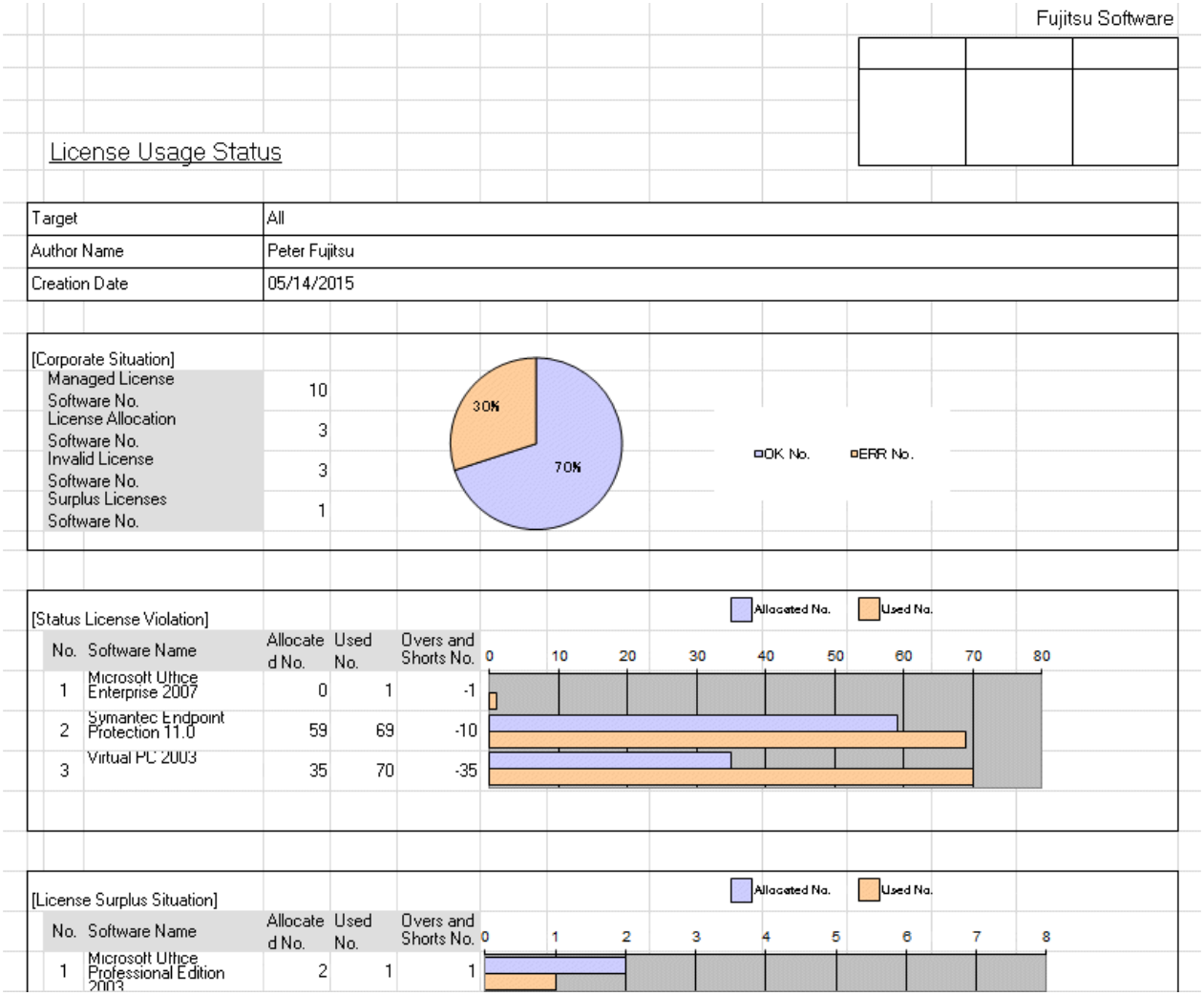
13.4.3 Example of Outputting License Usage Status

Report is composed of "Summary Part" and "Details Part". In addition, detailed information can be output by "Summary Part" and "Details Part".

The following describes "Summary Part" and "Details Part" respectively.

Summary part

The "Summary Part" when saved as file is as follows.



The content of the above file is as follows.

Item		Description
Fujitsu Software (The set value is displayed)		It is the information set in **Company Name** of the **Basic Information** tab.
Seal Column		It is the column for sealing on the created file. Here, since only the column for sealing is printed, use it freely.
License Usage Status (The set value is displayed)		It is the information set in **Title** of the **Basic Information** tab.
Target		It is displayed as **Whole Company**.
Author Name		Author of the file. it is the information set in **Author Name** of the **Basic Information** tab.
Creation Date		It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Corporate Situation	**Managed License Software No.**	It is the number of software with managed license.
	License Allocation Software No.	It is the number of software with allocated license.

Item		Description
	Invalid License Software No.	It is the number of software with license violation. The number of software with license violation is displayed based on the number allocated in the **Allocate License** of Systemwalker Desktop Patrol and the number of software actually installed to PC. Therefore, in the following cases, the number of software with license violation is "2". - The number of license of software A actually purchased is "10" - For software A, the number allocated in **Allocate License** of Systemwalker Desktop Patrol is "8" - The number of software A installed in the PC as the managed object of Systemwalker Desktop Patrol is "10"
	Surplus License Software No.	It is the number of software with surplus license.
Status License Violation	**No.**	It is the number allocated to the information that has been output.
	Software Name	It is the name of software with license violation.
	Allocated No.	It is the number of license owned.
	Used No.	It is the number of license used.
	Overs and Shorts No.	It is the number of license deficient.
License Surplus Situation	**No.**	It is the number allocated to the information that has been output.
	Software Name	It is the name of software with surplus license.
	Allocated No.	It is the number of license owned.
	Used No.	It is the number of license used.
	Overs and Shorts No.	It is number of surplus license.

Details part

The "Details Part" when saved as file is as follows.

License Usage Status

Creation Date: 05/14/2015

[E] The software has caused a violation of license

Target: All

	No.	Software Name	Allocated No.	Used No.	Overs and Shorts Results
	1	Windows 2003 Server	0	0	0
	2	Windows Server 2008	0	0	0
	3	Windows 8 Pro	0	0	0
	4	Windows XP Professional	0	0	0
	5	Systemwalker Centric Manager AC	0	0	0
E	6	Microsoft Visio Professional 2010	0	1	-1
E	7	Adobe Reader	59	69	-10
	8	Symantec Endpoint Protection 11.1	2	1	1
	9	Adobe Dimensions 3.0	0	0	-1
	10	Symantec Endpoint Protection 11.2	0	0	-2
	11	Microsoft Office Enterprise 2010	0	-2	-2

The content of the above file is as follows. In addition, the name of **Software Name** is arranged and displayed in sequence.

Item	Description
License Usage Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Target	It is displayed as **Whole Company**.
E	Display in the case that software which has caused the number of licenses violation
No.	It is the number allocated to the information that has been output.
Software Name	It is the name of software
Allocated No.	It is the number of allocated licenses.
Used No.	It is the number of license used.
Overs and Shorts Results	It is the excess or deficiency result of License.

13.5 Output Security Auditing Status

This section describes how to output security auditing status.

- "13.5.1 Preparation"
- "13.5.2 Procedure"
- "13.5.3 Example of Outputting Security Auditing Status"

To use this function, the authority of "System Account" is required.

13.5.1 Preparation

It describes how to set the auditing indicator to be used in security auditing.

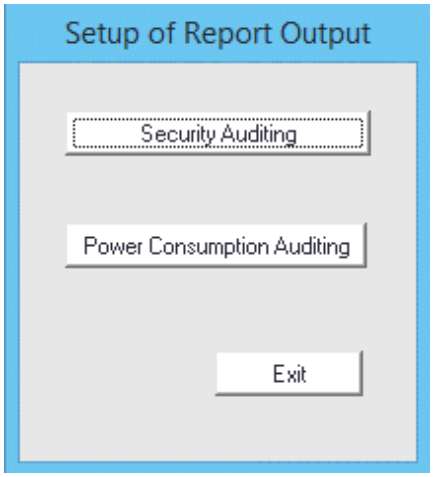
In addition, it is not required to set auditing indicator when the recommended auditing indicator provided by Systemwalker Desktop Patrol is not to be modified.

The procedure is as follow.

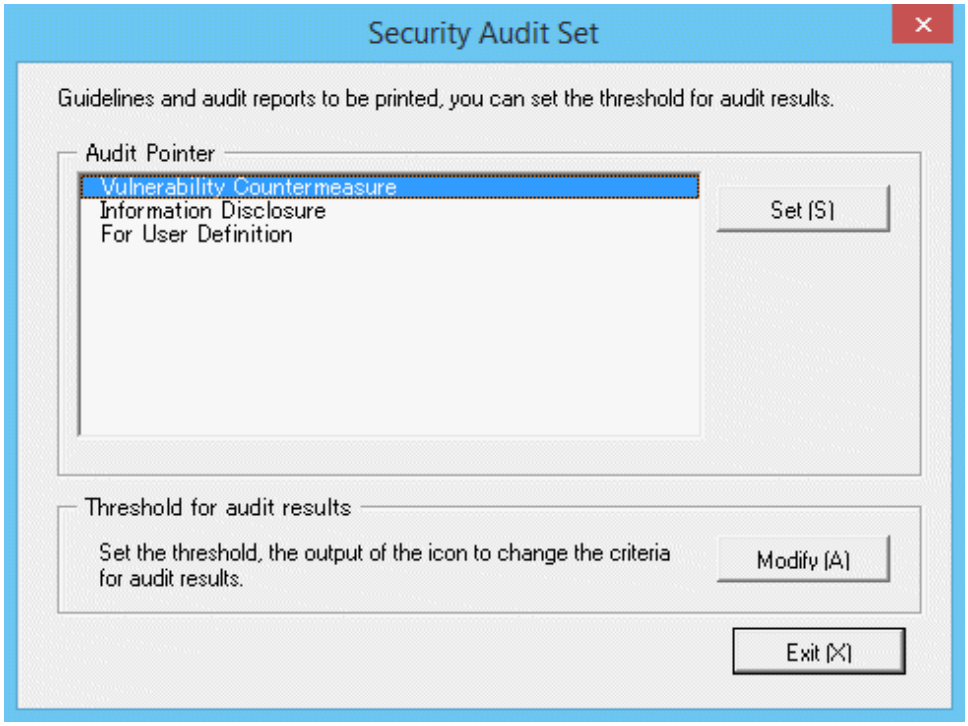
1. Log on to the AC menu.

2. Click **Setup of Report**.

   The following window will be displayed.



3. Click the **Security Auditing** button, and the **Security Audit Set** window will be displayed.

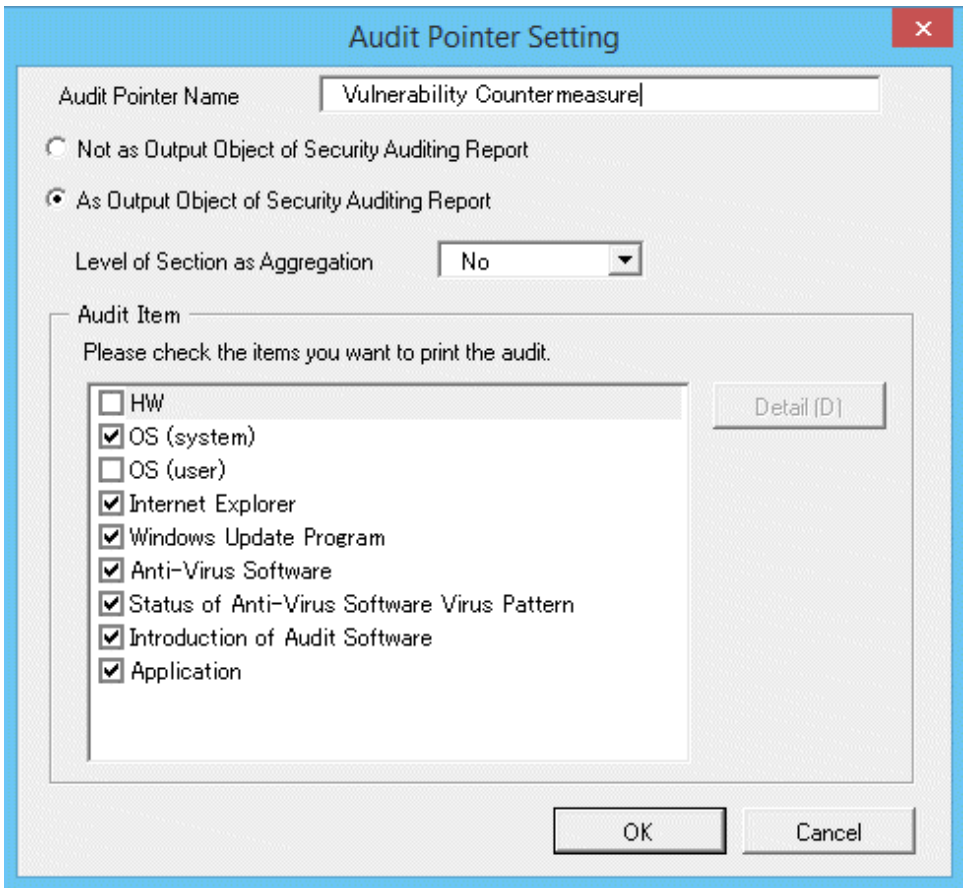


4. Select the **Audit Pointer** to be modified, and click the **Set** button of **Audit Pointer**.

   To newly define the auditing indicator, select **For User Definition**. To edit the recommended indicator, select **Information Disclosure** or **Vulnerability Countermeasure**.

   In addition, the setting of each auditing item is selected by combination of operation method and environment.

The **Audit Pointer Setting** window will be displayed.



Set the following information, and click the **OK** button.

Item		Description
Audit Pointer Name		Set the name of auditing indicator. Up to 16 fullwidth characters or 32 halfwidth alphanumeric characters and symbols can be set.
Not as Output Object of Security Auditing Report		Select when not to output security auditing report.
As Output Object of Security Auditing Report		Select to output security auditing report.
Level of Section as Aggregation (Note 1)		Not specify or select from level 1 to level 9.
Audit Item	**HW**	Select it when BIOS status is included in the output item of security auditing report.
	OS (System)	Select it when status of OS settings related to the system such as logon status and settings of automatic update are included in the output item of security auditing report.
	OS (User)	Select it when status of OS settings related to use such as screen saver is included in the output item of security auditing report.
	Internet Explorer	Select it when the setting status of security zone status of Internet Explorer is included in the output item of security auditing report.

Item		Description
	Windows Update Program (Note 2)	Select it when the setting status of patch installation such as OS is included in the output item of security auditing report.
	Anti-Virus Software	Select it when the setting status of installation status of anti-virus software and real-time search .etc is included in the output item of security auditing report.
	Status of Anti-Virus Software Virus Pattern	Select it when the application status of virus patter is included in the output item of security auditing report.
	Access Control	Select it when the application status of prohibition operation is included in the output item of security auditing report.
	Introduction of Audit Software	Select it when the setting status of auditing software installation status is included in the output item of security auditing report.
	Application	Select it when the setting status of application such as Google Desktop function and firewall settings are included in the output item of security auditing report.
Detail		Display the window to set whether to output the auditing for each item. For setting items, refer to "Items of auditing indicator".

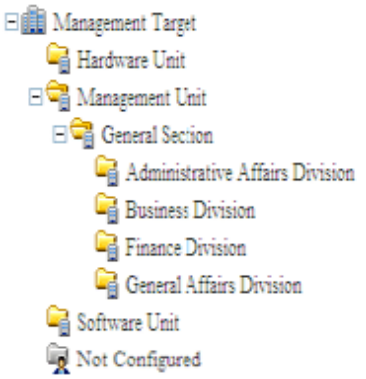
Note 1) It is the section level when aggregating sections with high achievement rates and sections with low achievement rates.

In the following example, when the second level is specified as the section level, the unit displayed as section is as follows.

- Upper-level section
- General section (including subordinate sections)

In the "General Section" of the second level, the PC under the "Business Division", "Finance Division", "Administrative Affairs Division" and "General Affairs Division" will be aggregated and sections with high achievement rates and sections with low achievement rates will be judged in the aggregation content.

In addition, for the "Software Unit", "Hardware Unit" and "Management Unit" in the higher level than the second level, it will be aggregated as one section of "Upper-level Section", and sections with high achievement rates and sections with low achievement rates will be judged in the "Upper-level Section".



In addition, if no level has been set, all sections will be targets of sections with high achievement rates and sections with low achievement rates. In addition, for PC without configuration, no judgment of sections with high achievement rates and sections with low achievement rates will be included.

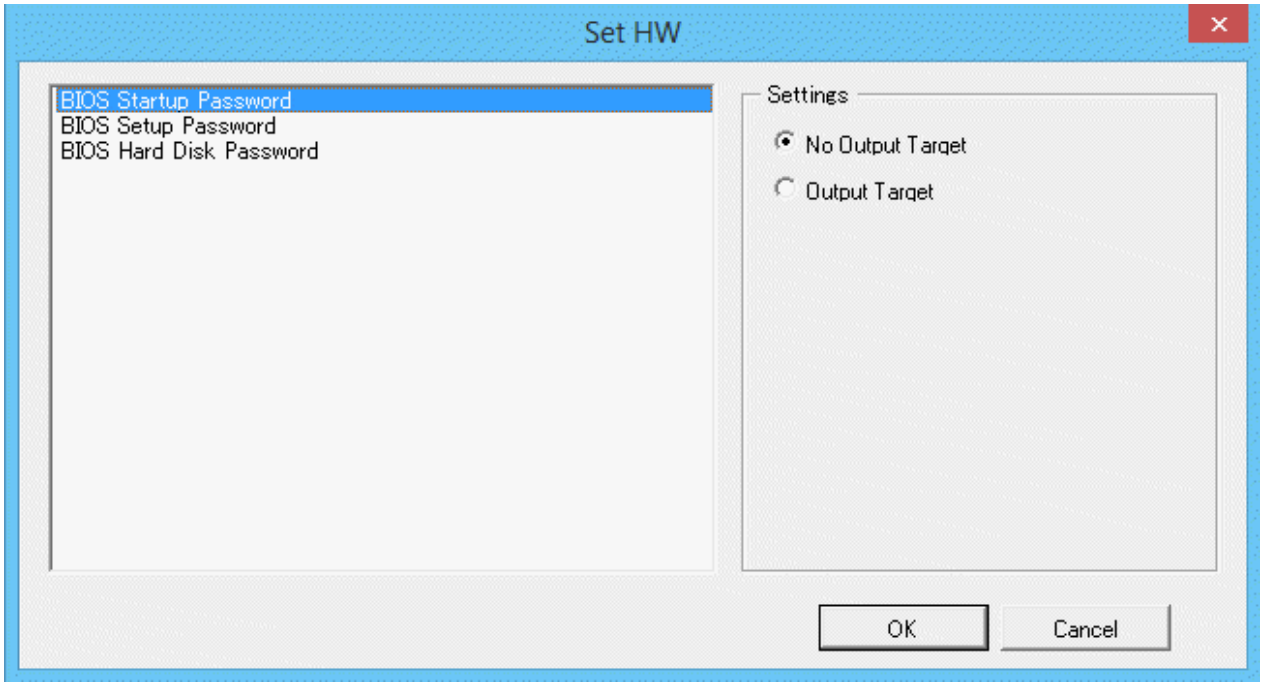
Note 2) Select the patch installation status using the patch distribution information managed by Systemwalker Desktop Patrol. In addition, For the patch to be selected, it is required to select automatic patch installation **Distribution** > **Security Patches Distribution** window in the main menu. For the patch without selection of automatic patch installation, it will not be selected.

If automatic patch installation is not executed, set **Not as Auditing Target** in the **Details** window.

If all patches included in the patch distribution information are installed to PC, this PC will be processed as the PC whose patch installation is OK. Even if one patch is not installed, it will be processed as the PC of ERR. The patch is not installed can be confirmed from the window of Systemwalker Desktop Patrol.

For information on how to confirm the patch not installed, refer to "3.2.1 View Inventory Information".

To modify the output standard of each auditing item, select each auditing item and click the **Details** button. The following is the window when **Hardware** is selected.



Set the following information, and click the **OK** button.

Item		Description
BIOS Startup Password		For the startup password of BIOS, select when setting the output to report.
BIOS Setup Password		For the setting password of BIOS, select when setting the output to report.
BIOS Hard Disk Password		For the hard disk password of BIOS, select when setting the output to report.
Settings (Note)	**No Output Target**	Select when the selected items are not taken as output target.
	Output Target	Select when the selected items are taken as output target.
	Items Judged as OK	For **Unable to Collect**, **Not Set** and **Has been Set**, l select the items that are judged as OK.

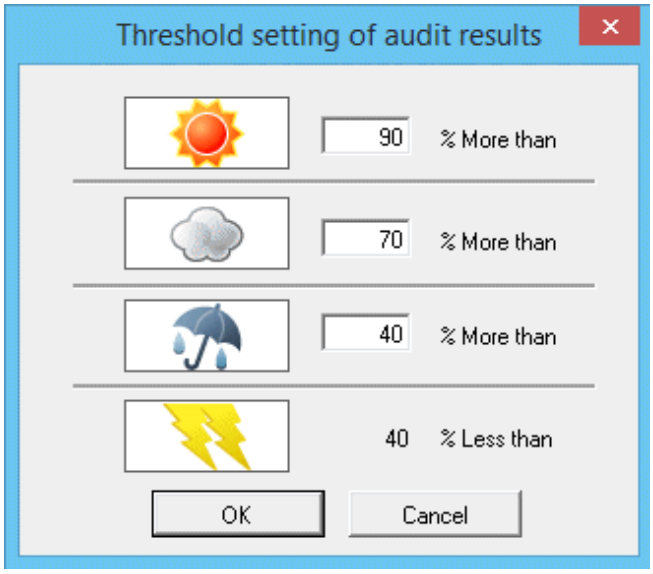
Note) Setting of judgment standard can be set for each auditing item of **Access Control Status**.

Set the auditing items apart from **Hardware** in the same way.

In addition, **Item Name** displayed in the setting window may vary depending on the item of auditing indicator. For other auditing items, refer to "Items of auditing indicator".

5. To modify the threshold value of auditing result, click the **Modify** button of **Threshold for audit results**.

   In the **Threshold setting of audit results** window, the output standard of icon can be modified.



   Set the following information, and click the **OK** button.

Item	Description
Threshold value of **Sunny** icon	Only single-byte number can be set. The initial value is over 90%.
Threshold value of **Overcast** icon	Only single-byte number can be set. The initial value is over 70%. Set a value that is smaller than the threshold value of **Sunny**.
Threshold value of **Rainy** icon	Only single-byte number can be set. The initial value is over 50%. Set a value that is smaller than the threshold value of **Overcast**

   Save the icon to the following folder and the icon can be modified.

   Registration folder of image file

AC installation directory\images

   Image file/file name

Image File	File Name
	best.bmp
	better.bmp
	bad.bmp
	worse.bmp

Size/Format of image file

	Size/Format
Width	82 pixels (Note)
Height	36 pixels (Note)
Format	bmp format

Note) when the image file of a different size is used, displayed as the above size.

Point

Modification of image file

- The modification of image file is only effective in the modified AC terminal. To unify image files in all AC terminals, replace the image file of all AC terminals.
- There are following methods to restore image file.
  - Before modification, when avoiding the icon of product, configure the avoided product icon to the registration folder again.
  - Before modification, when the icon of product is not avoided, delete the icon after modification and re-install the AC of this product. (it is not need to uninstall since it is overwriting installation)
- When the image file is displayed as blank, reasons such as files being damaged or insufficient should be considered. When it is displayed as blank, check the saving target of icon and restore through preparing a new image or restoring the above image file.

Items of auditing indicator

It describes the items of monitoring indicator.

For content of each item, refer to "3.2.6 View Security Information".

For the following items, whether the auditing report will be output as output target of auditing report can be set in each item unit.

HW (Note)

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
BIOS Startup Password	Not as output object	As output object
BIOS Setup Password	Not as output object	As output object
BIOS Hard Disk Password	Not as output object	As output object

Note) In case of virtual PC, since the hardware is **Unable to Audit**, the **Hardware Type** will be displayed as **Virtual PC**, and **Hardware** will be displayed as **-** in the report.

OS (System)

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Automatic Logon	Not as output object	As output object

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Welcome To Use	Not as output object	Not as output object
Last User Name	Not as output object	Not as output object
Security of Guest Account	Not as output object	As output object
Settings of Automatic Update	Not as output object	Not as output object
User Account Control (UAC)	Not as output object	Not as output object
Insecure Shared Folder	Not as output object	As output object
Require a Password on Wakeup	Not as output object	Not as output object
Set Complicated Password Required	Not as output object	Not as output object

OS (User)

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Screen Saver	Not as output object	As output object
Screen Saver Password	Not as output object	As output object
Password of Logon User	Not as output object	As output object

Internet Explorer

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Internet Zone	As output object	As output object

Introduction of Audit Software

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Check whether Systemwalker Desktop Patrol CT is installed (whether inventory information is collected)	As output object	As output object

Windows Update Program

Setting Item	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Check the patch installation status using the patch distribution information managed by Systemwalker Desktop Patrol	As output object	As output object

Anti-virus Software

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Installation of Anti-virus Software	As output object	As output object
Real-time Scan Status of Anti-virus Software	As output object	As output object
Scheduled Scan Status of Anti-virus Software	Not as output object	Not as output object
Scan Scope of Anti-virus Software	Not as output object	Not as output object

Status of Anti-virus Software Virus Pattern

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Check whether the latest virus pattern has been applied	As output object	As output object

Access Control

It can be used after Systemwalker Desktop KeeperV13.0.0 or later has been installed.

Information	Content	Initial Value of Recommended Auditing Indicator	
		Vulnerability Countermeasure	Information Disclosure
File Export Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Normal export		
	Encrypted export		
	Unable to export		
Printing Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
PrintScreen Key Prohibition	Unable to collect	Not as output object	Not as output object

Information	Content	Initial Value of Recommended Auditing Indicator	
		Vulnerability Countermeasure	Information Disclosure
	No		
	Yes		
Logon Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Application Startup Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
E-mail File Attachment Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Allow encrypted file only		
	Prohibit specified extensions only		
	Allow specified extensions only		
Application Startup Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Application Termination Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Window Title Obtaining Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
E-mail Sending Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Command operation log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Device Configuration Change Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Printing operation log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
File Export Log	Unable to collect	Not as output object	Not as output object

Information	Content	Initial Value of Recommended Auditing Indicator	
		Vulnerability Countermeasure	Information Disclosure
	No		
	Yes		
File Operation Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Logon/Logoff Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
External Application log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
PrintScreen Key Operation log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
File Export Utility	Unable to collect	Not as output object	Not as output object
	Normal export		
	Encrypted export		
	Unable to export		
Reading prohibition of removable drive	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
USB Device Individual Identification	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Web Operation Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
FTP Operation Log	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Confirmation of Recipient Address	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
URL Access Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		

Information	Content	Initial Value of Recommended Auditing Indicator	
		Vulnerability Countermeasure	Information Disclosure
FTP Server Connection Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		
Web Download Prohibition	Unable to collect	Not as output object	Not as output object
	No		
	Yes		

Application

Information	Initial Value of Recommended Auditing Indicator	
	Vulnerability Countermeasure	Information Disclosure
Firewall	As output object	As output object
Adoption of Encryption software	Not as output object	Not as output object
Google Desktop **Search Across Computers**	Not as output object	As output object
Detection of Banned Software Status	Not as output object	Not as output object

For the settings of whether to perform auditing of each auditing items, refer to "4.2.2.1 Set the Auditing Items of Security Settings".

In addition, the auditing result output in the security auditing report is consistent with the auditing result in the diagnosis result of operation settings (security auditing). For judgment method, refer to "Diagnosis Result" of "4.3.1.2 Structure of Security Diagnosis Result Window".

For PC imported through linking with other products of Systemwalker Desktop Patrol, the auditing result is as follows.

- Auditing items that are judged as OK

  Import Auditing Software
  Windows Update Program

- Auditing items that are judged as ERR

  Anti-Virus Software
  Virus Pattern Status of Anti-virus Software

- Items except the above

  Judged as OK.

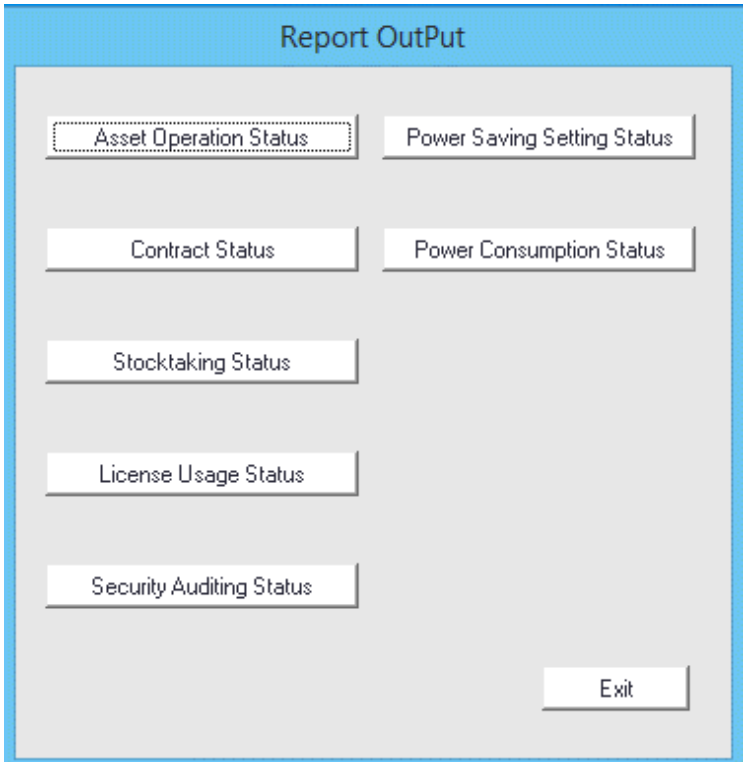
13.5.2 Procedure

The procedure of outputting security auditing is as follows.

1. Logon to the AC menu.

2. Select **Report Output**.

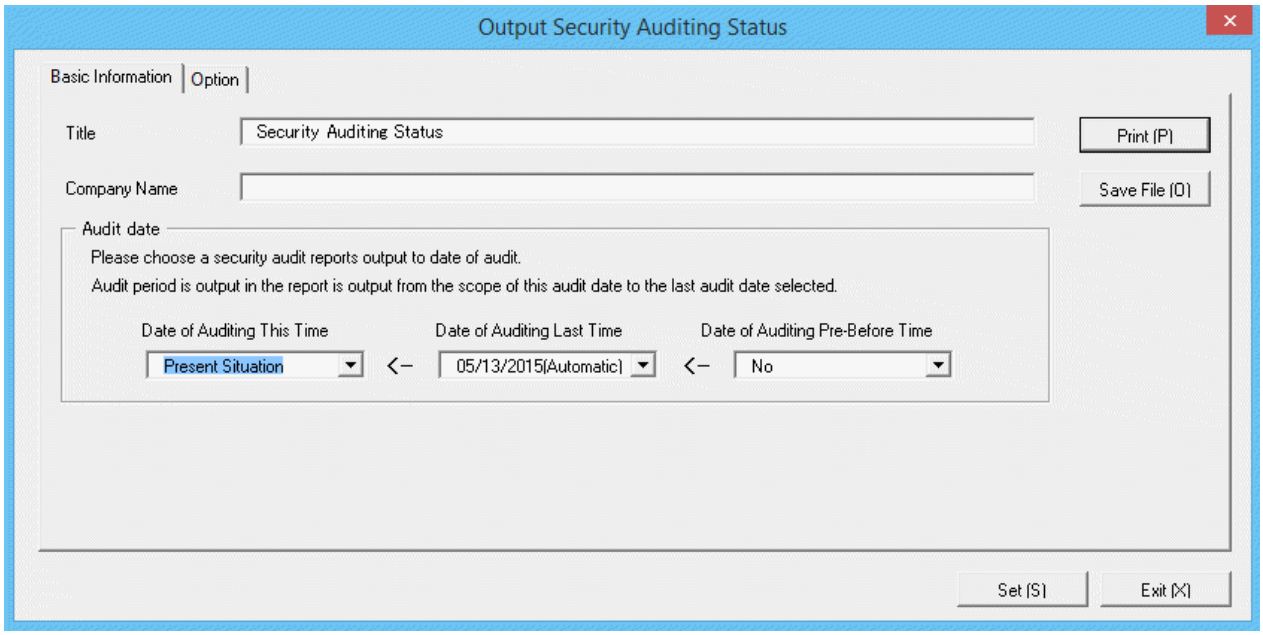
   The following window will be displayed.



3. In the sub-menu of **Report Output**, click the **Security Auditing Status** button.

   The **Output Security Auditing Status** window will be displayed.

4. Set the basic information to be output to report in the **Basic Information** tab.



   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth alphanumeric characters and symbols be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Date of Auditing This Time	Specify the auditing date of this time to be output to report. (Note 1)
	Date of Auditing Last Time	Specify the auditing date of last time to be output to report. (Note 1)
	Date of Auditing Pre-Before Time	Specify the auditing date of the time before last to be output to report.(Note 1)

Note 1)

Select the auditing date in the date displayed in the check box. The items displayed in the auditing date are as follows.

- Current status

  Select it when executing security auditing and outputting the result as auditing result at the time to output to report. Only the auditing date of this time can be selected.

- MM/DD/ YYYY (Automatic)

  Select it to use the auditing date of the displayed date.

  (Automatic) is displayed in case of the auditing date when auditing in scheduled execution.

- MM/DD/ YYYY (Manual)

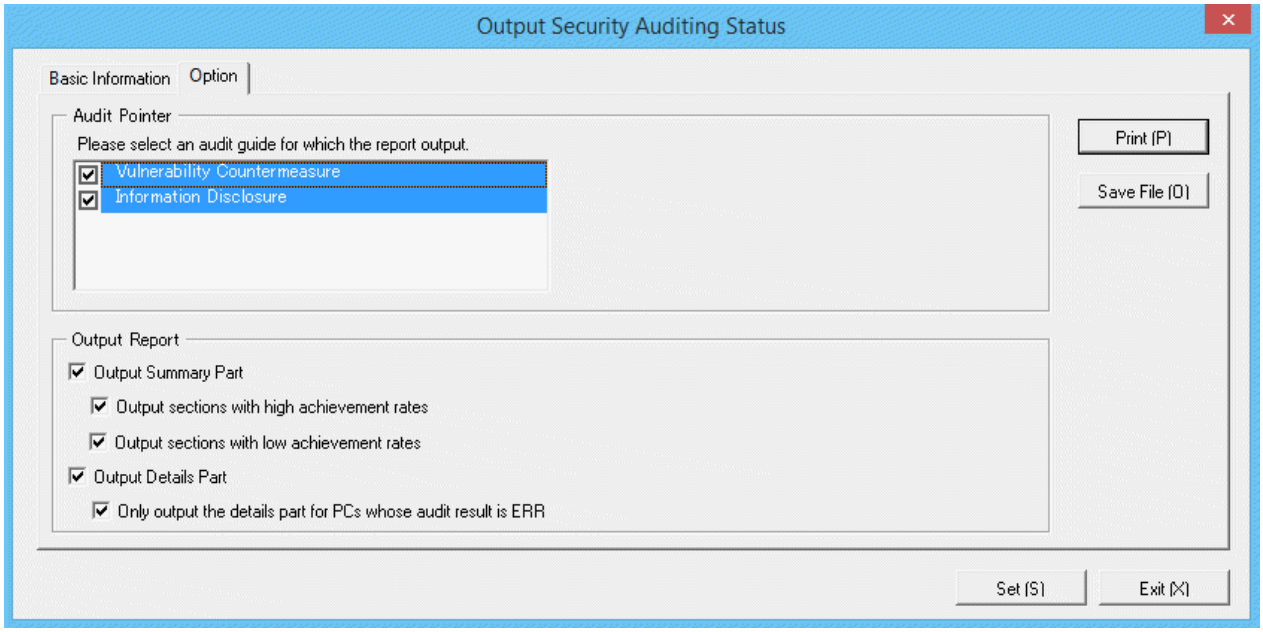
  Select it to use the auditing date of the displayed date.

  (Manual) is displayed in case of the auditing date when specifying **Current Status** in auditing date of this time and report is output.

- No specification

  Select it when you will not output auditing result to report. Only the auditing date of last time and the time before last can be selected.

5. Select the **Option** tab, and set the operation information for report.



Set the following information.

Tab Name	Item		Description
Option	**Audit Pointer**		Select the auditing indicator to be output to security auditing report. (multiple selection is allowed)
	Output Report	**Output Summary Part**	Select it when outputting the summary part. - **Output section with high achievement rates**: Select it when outputting the best sections. It can be selected only when **Output Summary Part** is selected. - **Output section with low achievement rates**: Select it when outputting the worst sections. It can be selected only when **Output Summary Part** is selected.
		Output Details Part	Select it when outputting the details part. - **Only output the details part for PCs whose audit result is ERR**: Select it when only the PC whose auditing result is ERR will be output to the details part. It can be selected only when **Output Details Part** is selected.

6. Output report.

Operate for the following cases.

- Print

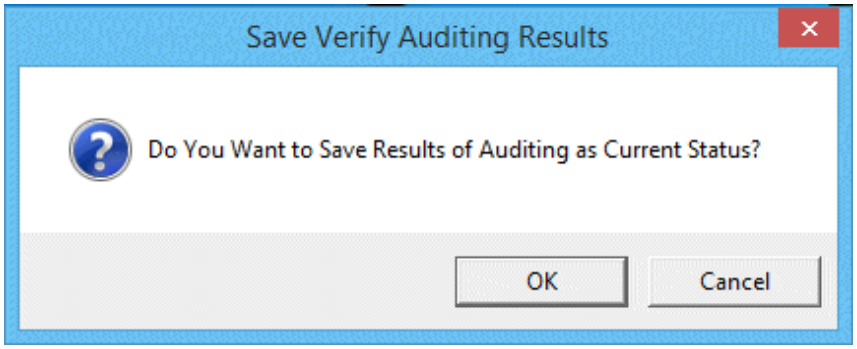
  To print the report, click the **Print** button.

- Save as File

  To save the report as a file, click the **Save File** button.

  The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

As **Date of Auditing This Time**, when **Present Situation** is selected, the following information will be displayed.



7. To save the result of security auditing executed this time, click the **OK** button.

   When the result of security auditing is saved, selection can be made from the auditing date of the **Output Security Auditing Status** window.

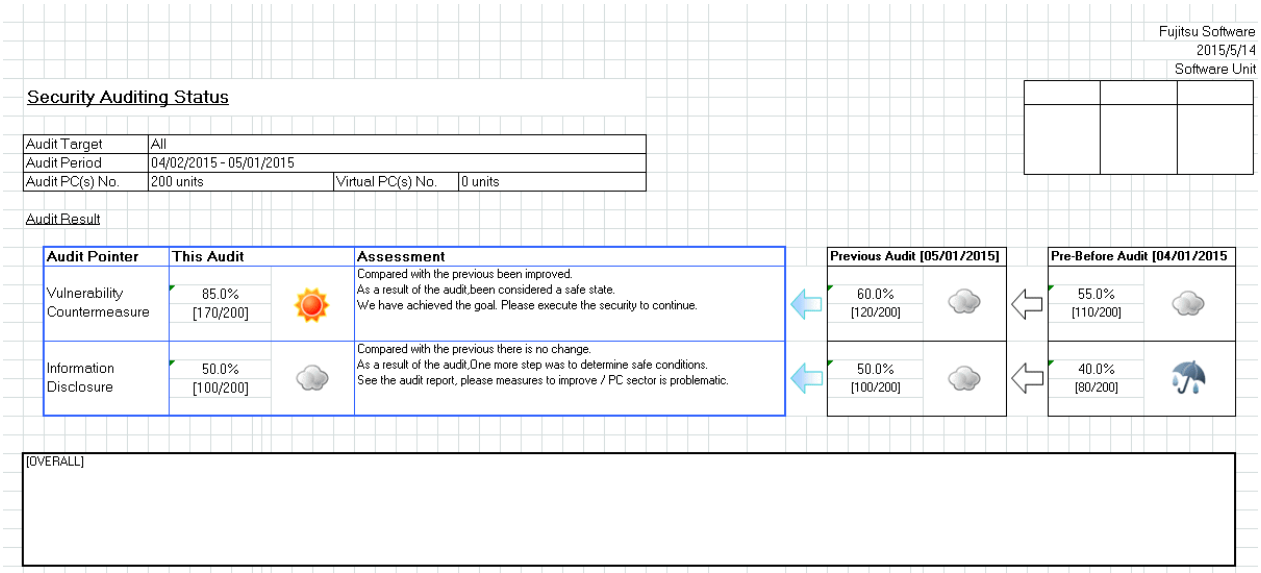
13.5.3 Example of Outputting Security Auditing Status

The report is composed of "Summary Part", "Audit Report Part" and "Details Part".

The following describes each of the "Summary Part", "Auditing Report Part" and "Details Part".

Summary part

The "Summary Part" when saved as file is as follows.



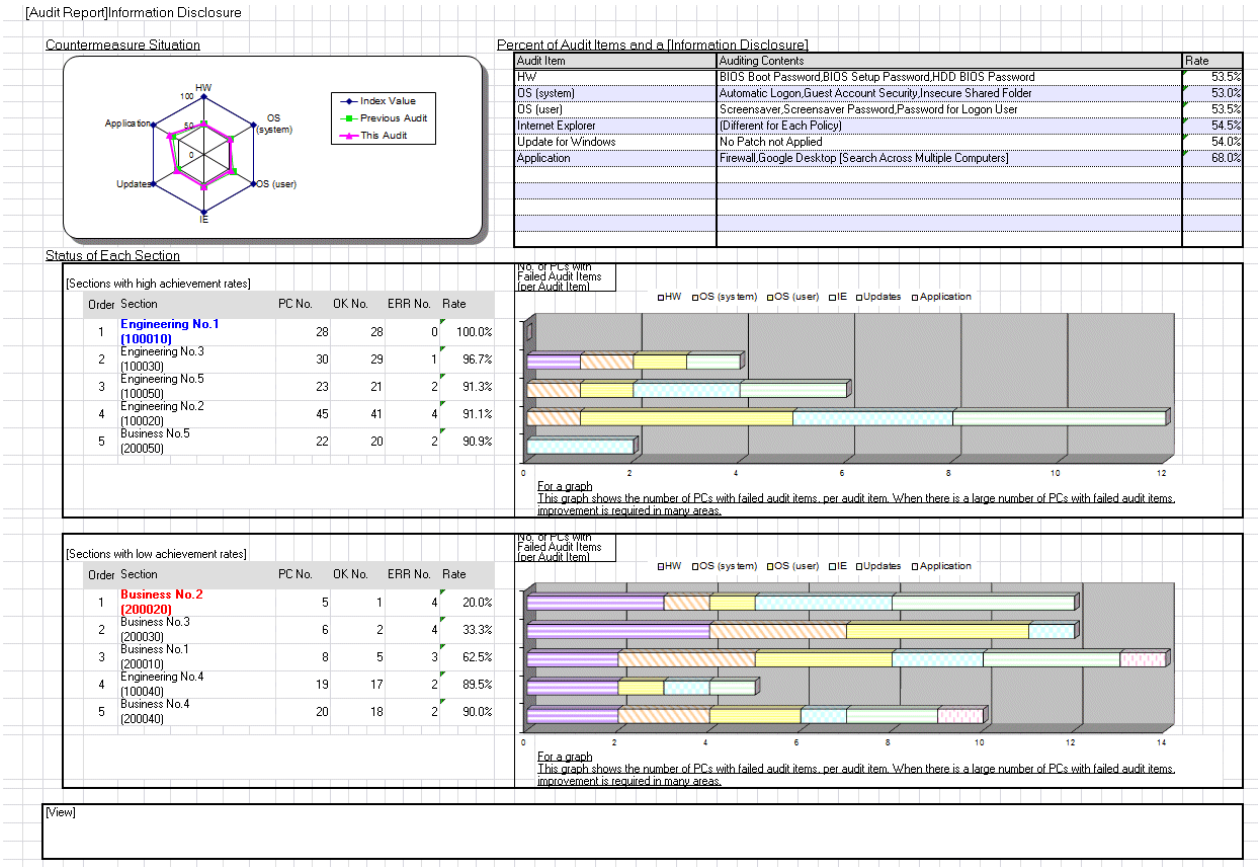
The content of the above file is as follows.

Item	Description
Fujitsu Software (The set value is displayed)	It is the information set in **Company Name** of the **Basic Information** tab.

Item	Description
Date	It is the date when report is output.
Software Unit	It is the section to which the user that outputs the report belongs.
Seal Column	It is the column for sealing on the created file. Here, since only the column for sealing is printed, use it freely.
Security Auditing Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Audit Target	It is displayed as **Whole Company**.
Audit Period	It is the information set in **Auditing Date** of the **Basic Information** tab.
Audit PC(s) No.	It is the number of PCs targeted for security auditing.
Virtual PC(s) No.	It is the number of virtual PCs targeted for security auditing.
Audit Result	**Audit Pointer** The auditing result is displayed according to auditing indicator. **This Audit** The assessment result of auditing this time is displayed. It is the number of PCs of **OK number/Total number** format in [].The icon of auditing result is displayed according to the OK number and threshold value settings. In case of virtual PC, the OK number will be counted. **Assessment** The assessment is displayed for auditing result. **Previous Audit/Pre-Before Auditing** The auditing result of last time and the time before last is displayed.
OVERALL	It is the column for recording comment for auditing result. Here, since only the record column will be printed, use it freely.

Auditing report part

When saved as file, the "Audit Report Part" is as follows.



The content of the above file is as follows.

Item	Description
Audit Report (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Countermeasure Situation	The index value reaches 100% (All PCs are OK), the radar chart for this auditing and last auditing will be displayed according to auditing item.
Percent of Audit Items and a *n*	The name, auditing content and achievement rate will be displayed according to auditing items.
Status of Each Section	**Sections with high achievement rates** In descending order of achievement rate from high to low, the top 5 sections will be displayed. It is the section code in the brackets. **Sections with low achievement rates** In descending order of achievement rate from high to low, the top 5 sections will be displayed. It is the section code in the brackets. **Level *n*** The section level of the aggregation object will be displayed. **Number of ERR for Each Auditing Item** The number of PCs as ERR in each auditing item will be displayed by graph.
View	It is the column for recording comments for auditing result. Here, since only the record column will be printed, use it freely.

Note

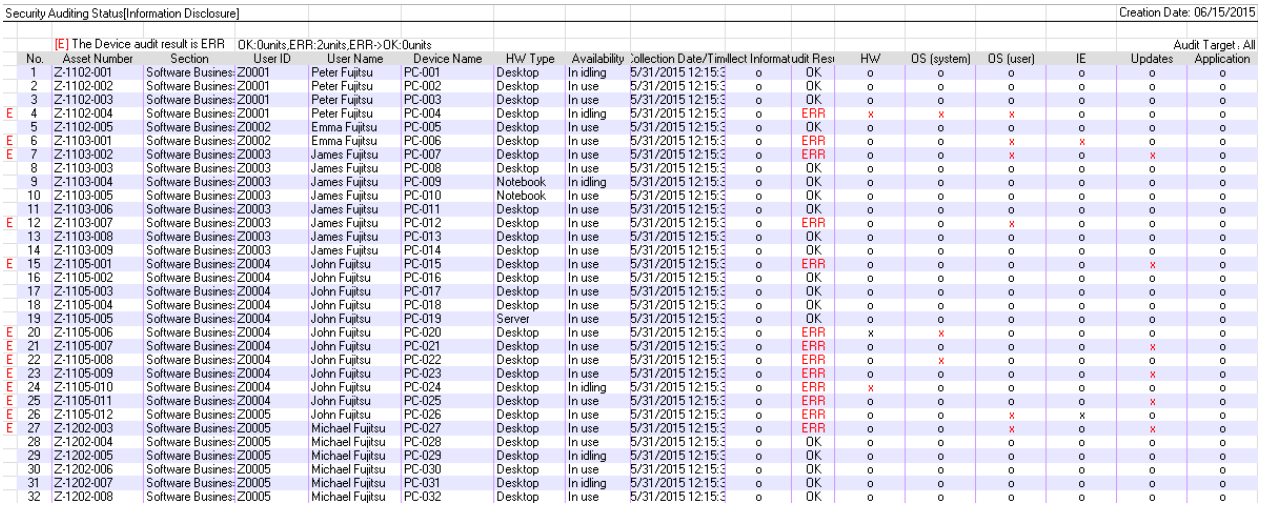
About graph output in the auditing report part

For the crossbar graph in the auditing report part, when the version earlier than Microsoft(R) Office Excel 2003 is used, the number of items of crossbar graph that is less than 3 will be output as 2D, and the number of items that is more than 4 will be output as 3D. However, when Microsoft(R) Office Excel 2007 or later is used, it will be output as 2D regardless of the number of items of crossbar graph.

In addition, in case of Microsoft(R) Office Excel 2007 or later, the color scheme and display location of notes of radar chart and crossbar graph in auditing report part contains some differences from the versions prior to Microsoft(R) Office Excel 2003.

Details part

The "Details Part" when saved as file is as follows.



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	Collection Date/Time	Collect Informat	Audit Resu	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

The content of the above file is as follows. In addition, in the result of security auditing, the name of **Section** is displayed in sequence.

Item	Description
Security Auditing Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
OK	It is the number of machines with auditing result as **OK**.
ERR	It is the number of machines with auditing result as **ERR**.
ERR->OK	It is the number of machines with auditing result as **ERR->OK**.
Audit Target	It is displayed as **Whole Company**.
E	The machine with auditing result as ERR will be displayed.
No.	It is the number allocated to the information that has been output.
Asset Number	It is the asset number of machine.
Section	It is the information of section. The registered "Section Management Information" is imported by Systemwalker Desktop Patrol.
User ID	It is the user ID of the user who uses the machine. It is the information of **User ID** registered as machine information.
User Name	It is the user name that uses the machine.

Item	Description
	The registered "User Management Information" is imported by Systemwalker Desktop Patrol.
Device Name	It is the name to be used as machine. It is the information of **Machine Name** registered as machine information.
HW Type	It is the hardware type information of machine. (Output the type of desktop/laptop/server/virtual PC.)
Availability	It is the availability of machine. It is the information of **Availability** registered as machine information.
Collection Date/Time	It is the date and time when information has been registered.
Collect Information	It shows whether it exists on the database of Systemwalker Desktop Patrol as inventory information. **o** is the situation when existing as inventory information, **x** is the situation when not existing as inventory information, Through the operation in Systemwalker Desktop Patrol, when the PC information is deleted by the disposal management function and when the inventory information is deleted manually, it is **x**.
Audit Result	**Items of Auditing Indicator** is displayed as **OK** in case of all **o**. When **x -> o** is contained but **x** is not contained in the auditing result, it will be displayed as **ERR -> OK**. When **x** exists in the auditing result, it will be displayed as **ERR**.
Items of Auditing Indicator	The auditing result will be displayed according to auditing item. When the auditing result is OK, **o** will be displayed. When the auditing result is ERR, **x** will be displayed. When the diagnosis result is set to OK manually, **x -> o** will be displayed. In case of non auditing object, - will be displayed. For description of each item, refer to "Items of auditing indicator".

13.6 Output Power Saving Setting Status

This section describes how to output the power saving setting status.

- "13.5.2 Procedure"
- "13.6.2 Example of Outputting Power Saving Setting Status"

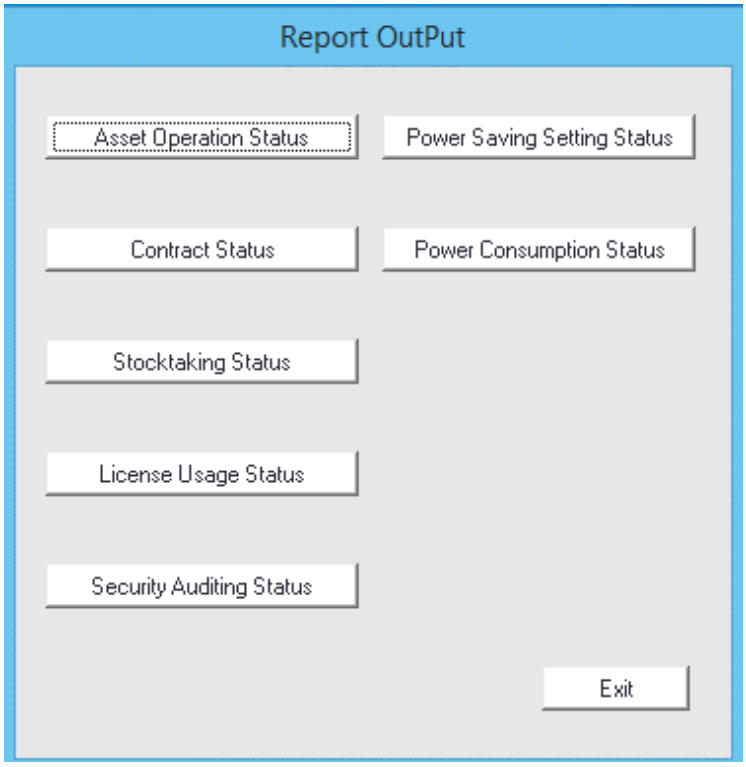
13.6.1 Procedure

The procedure of outputting power saving setting status is as follows.

1. Log on to the AC menu.

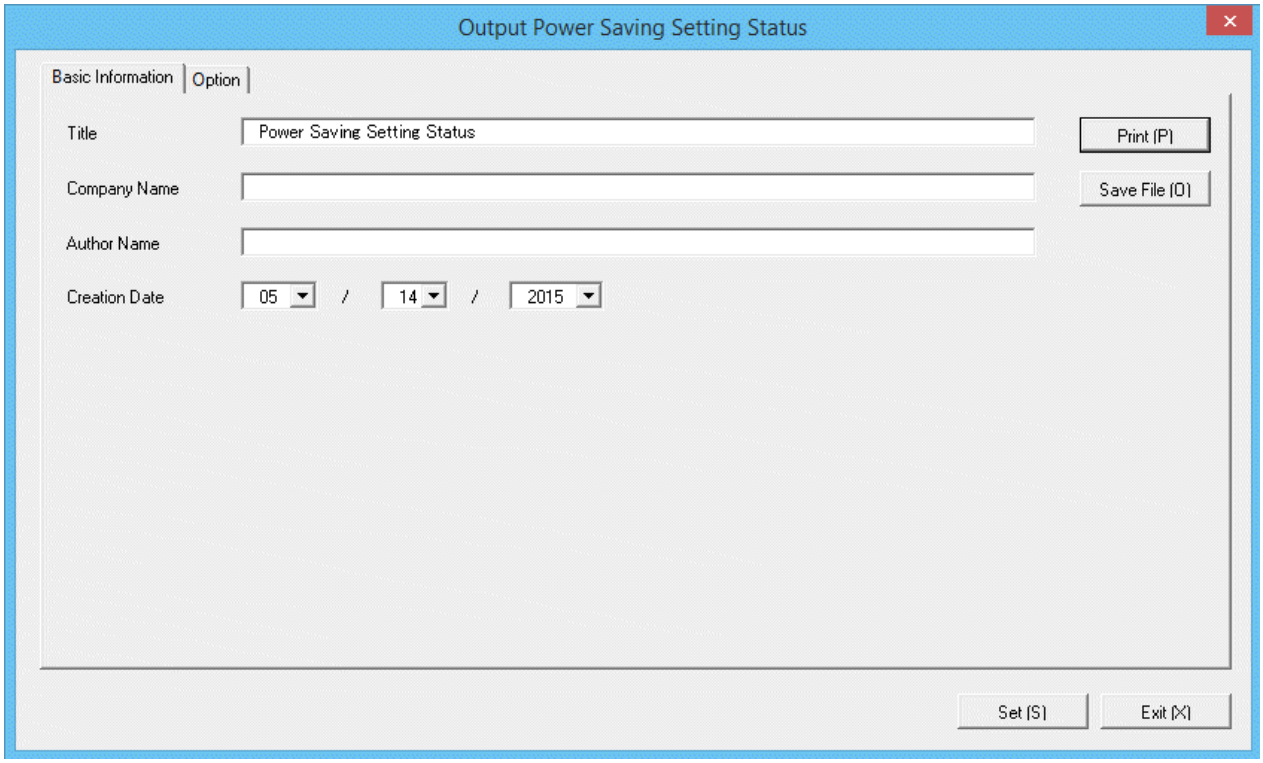
2. Select **Report OutPut**.

   The following window will be displayed.



3. Click the **Power Saving Setting Status** button.

   The following window will be displayed.

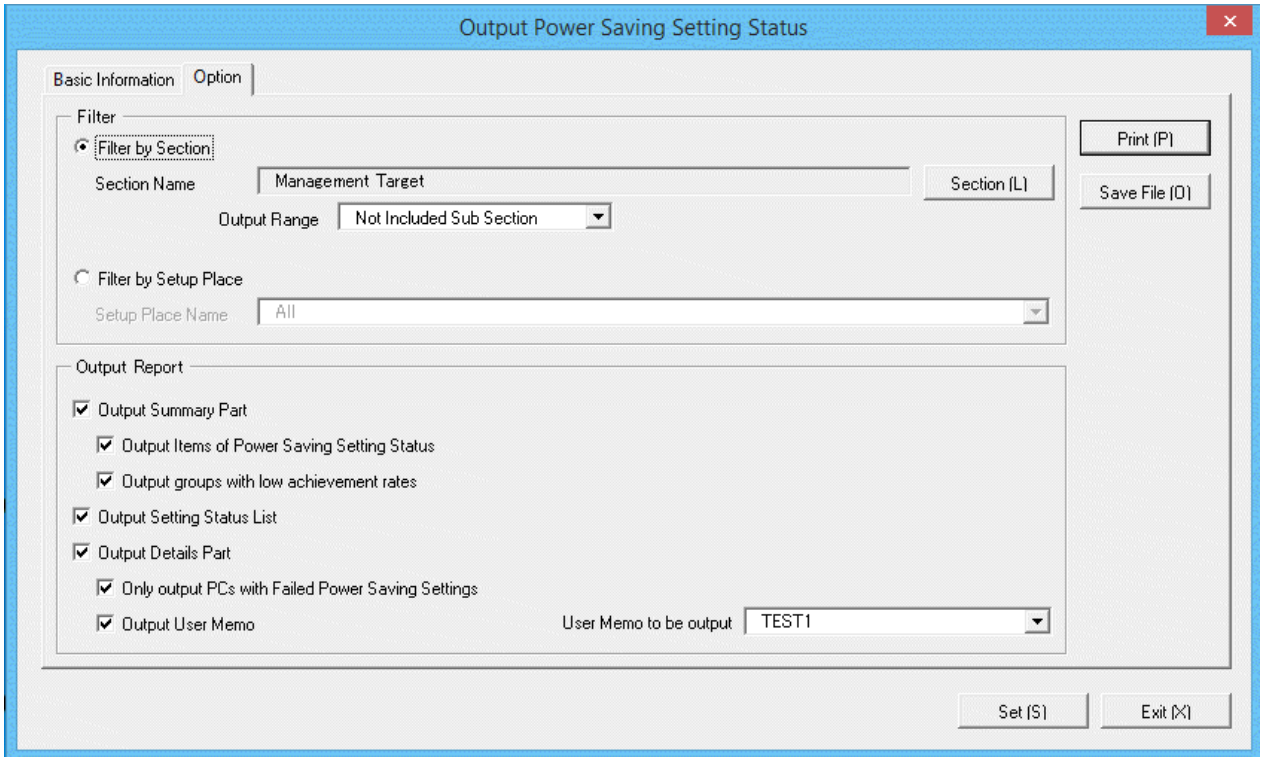


   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters and 50 halfwidth alphanumeric characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters and 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters and 64 halfwidth alphanumeric characters and symbols can be set.
	Creation Date	Set the creation date to output in report.

4. Select the **Option** tab to set the option information for report.



Set the following information.

Tab Name	Item		Description
Option	**Filter**	**Filter by Section**	Select it when outputting power saving setting status to report by section unit. - **Section Name**: Set the section to be output to report. - **Output Range**: Set the filtering range.
		Filter by Setup Place	Select it when outputting power saving setting status to report by location unit. - **Setup Place Name**:

Tab Name	Item		Description
			Set the location to be output to report.
	Output Report	**Output Summary Part**	It is selected when outputting the summary part to report. - **Output Items of Power Saving Setting Status**: Select it when outputting items of power saving setting status to the summary part. It can be selected only when **Output Summary Part** is selected. - **Output groups with low achievement rates**: Select it when outputting each status in the summary part. Select the following. It can only be selected when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name, select **Included Sub Section** in the output range of section - When **Filter by Setup Place** is selected - Select **All** in the location name
		Output Setting Status List	Select it when outputting the setting status list. It can be selected only when the following is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name, select **Included Sub Section** in the output range of section
		Output Details Part	Select it when outputting the details part. - **Only Output the PCs with Failed Power Saving Settings**: Select it when only the PC whose power saving setting is failed in the details part. It can be selected only when **Output Details Part** is selected. - **Output User Memo**: Set whether to output the user memo of machine as one item of details part of machine. In addition, to output, select the user memo to be output.(Note)

Note) In user memo, the output relating to the power saving settings such as whether PC is required to work 24 hours can be used as the document for judging the existence of product of correspondent PC from the details part.

5. Output report.

   Operate for the following cases.

   - Print

     To print the report, click the **Print** button.

   - Save as File

     To save the report as a file, click the **Save File** button.

     The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

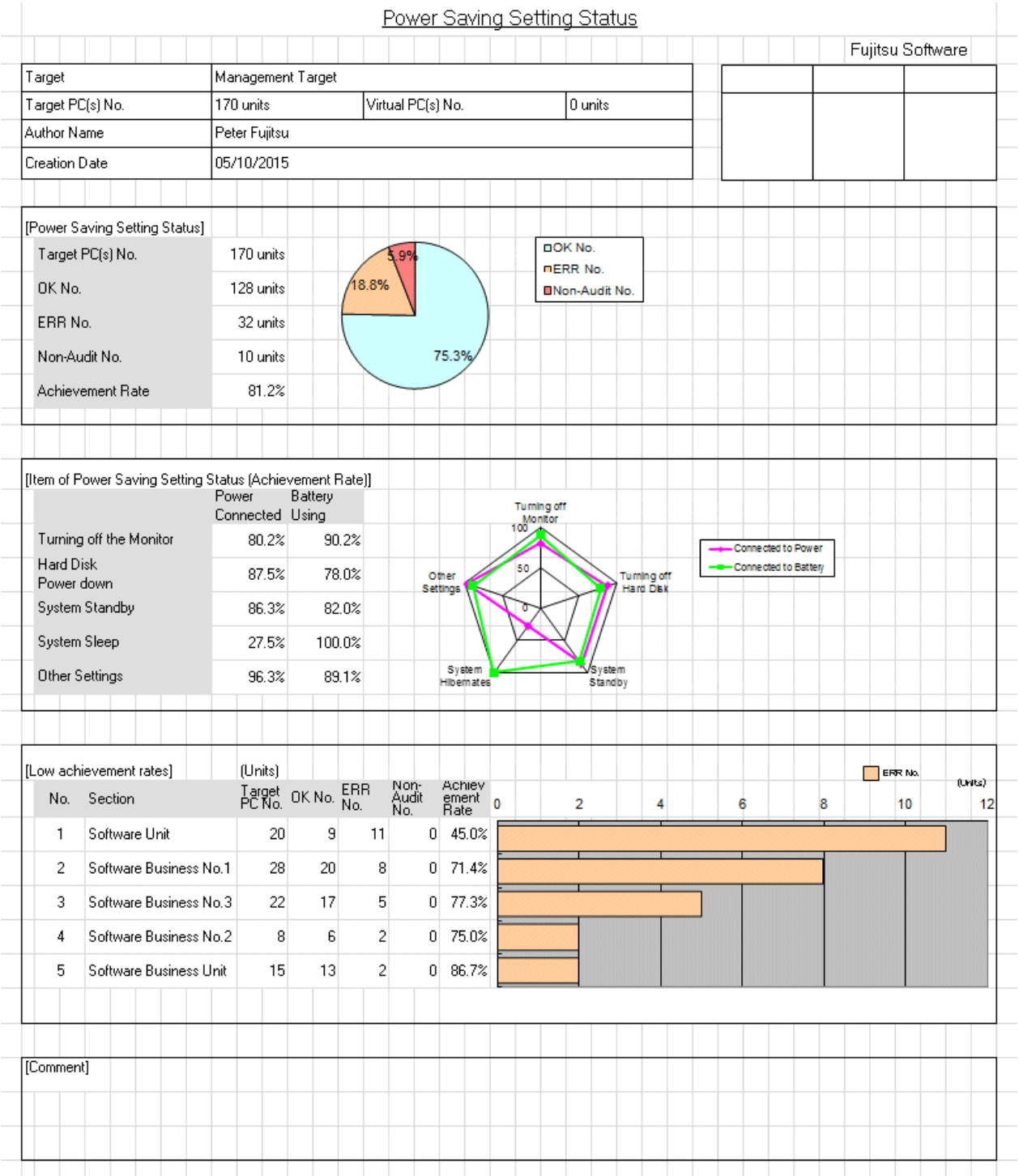
13.6.2 Example of Outputting Power Saving Setting Status

The report is composed of "Summary Part", "List of Setting Status", and "Details Part".

The following describes each of the "Summary Part", "List of Setting Status" and "Details Part".

Summary part

The "Summary Part" when saved as file is as follows.



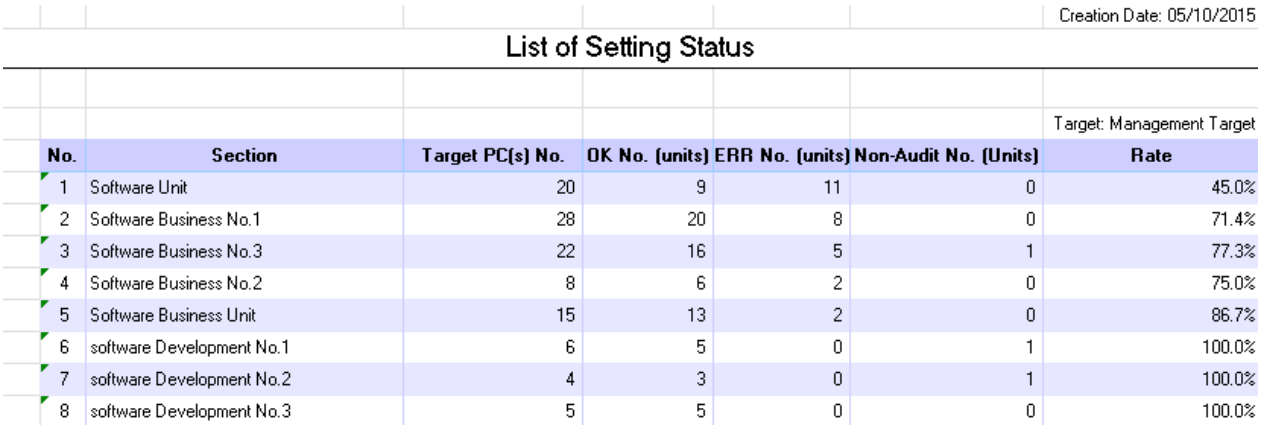
The content of the above file is as follows.

Item	Description
Fujitsu Software (The set value is displayed)	It is the information set in **Company Name** of the **Basic Information** tab.
Seal Column	It is the column for sealing on the created file. Here, since only the column for sealing is printed, use it freely.
Power Saving Setting Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.

Item		Description
Target		It is the name of section or location as object. It is the information set in **Section Name** and **Location Name** of the **Option** tab.
Target PC(s) No.		It is the number of all PCs in section or location as object.
Virtual PC(s) No.		It is the number of all virtual PCs in section or location as object.
Author Name		Author of the file. it is the information set in **Author Name** of the **Basic Information** tab.
Creation Date		It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Power Saving Setting Status	**Target PC(s) No.**	It is the number of PCs in the section or location as object.
	OK No.	It is the number of PCs whose auditing result of power saving setting is OK. Target at the PC with all auditing items are Octet power setting items of non-auditing object will be processed as OK and aggregated.
	ERR No.	It is the number of PC whose auditing result of power saving setting is ERR and the PC requires attention. Even if one auditing result is ERR and the power setting item that requires attention exists, the PC will be targeted.
	Non-Audit No.	It is the number of PC that is unable to be audited since power saving information is not collected in CT. It is unable to collect in any of the following cases. - When the CT prior to V13.2 is used - When inventory information is imported through linking with other product - In case of virtual PC
	Achievement Rate	It is the achievement rate of power saving setting in the section or location as object.
Item of Power Saving Setting Status (Achievement Rate)		The index value reaches 100% (All PCs are OK). The radar chart for power saving setting status will be output by power saving setting item when connecting to power/using battery. *The PC whose power saving information isn't collected in CT will be processed as OK and aggregated. *For PC without battery such as desktop PC, the achievement rate of item when using battery is not included.
Low Achievement Rates		Output the number of PCs of sections with low achievement rates/ location, number of OK sets,number of ERR sets,achievement rate. In addition, the number of ERR sets of each section is output in crossbar graph.
Comment		It is the input column for comment such as opinions.

List of setting status

The "List of Setting Status" when saved as file is as follows.



Creation Date: 05/10/2015

List of Setting Status

Target: Management Target

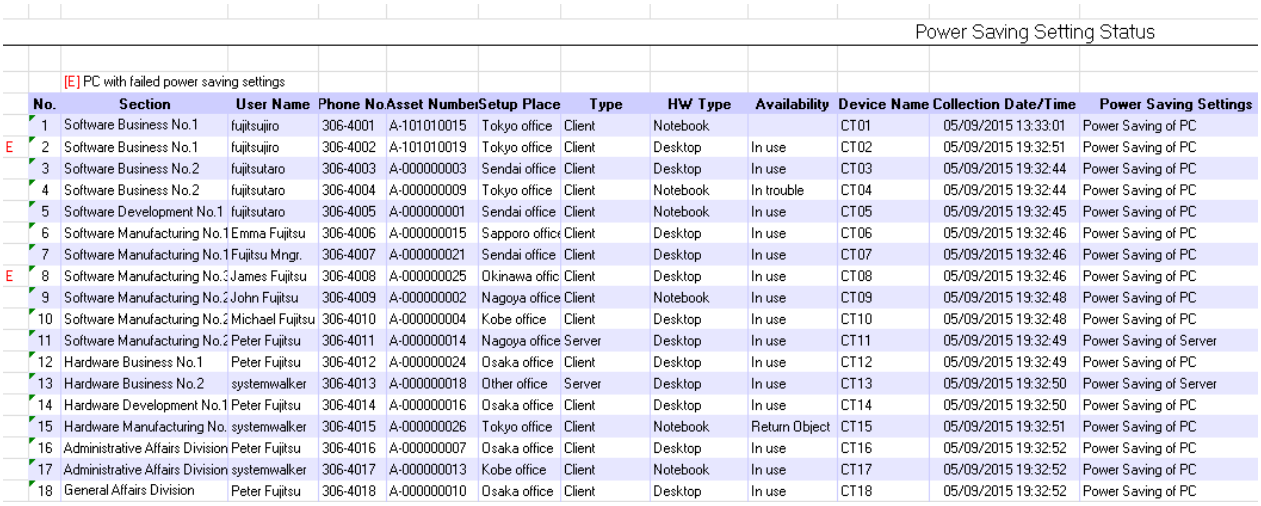
No.	Section	Target PC(s) No.	OK No. (units)	ERR No. (units)	Non-Audit No. (Units)	Rate
1	Software Unit	20	9	11	0	45.0%
2	Software Business No.1	28	20	8	0	71.4%
3	Software Business No.3	22	16	5	1	77.3%
4	Software Business No.2	8	6	2	0	75.0%
5	Software Business Unit	15	13	2	0	86.7%
6	software Development No.1	6	5	0	1	100.0%
7	software Development No.2	4	3	0	1	100.0%
8	software Development No.3	5	5	0	0	100.0%

The content of the above file is as follows.

Item	Description
No.	It is the number allocated to the information that has been output.
Section/Setup Place	It is the information of section/location.
Target PC(s) No.	It is the number of PC for power saving settings of the current month.
OK No.	It is the number of PC in which power saving setting is performed.
ERR No.	It is the number of PC in which power saving setting is not performed.
Non-Audit No.	It is the number of PC that cannot be audited.
Rate	It is the proportion of PC for which power saving setting is not performed.

Details part

The "Details Part" when saved as file is as follows.



Power Saving Setting Status

[E] PC with failed power saving settings

	No.	Section	User Name	Phone No.	Asset Number	Setup Place	Type	HW Type	Availability	Device Name	Collection Date/Time	Power Saving Settings
	1	Software Business No.1	fujitsujiro	306-4001	A-101010015	Tokyo office	Client	Notebook		CT01	05/09/2015 13:33:01	Power Saving of PC
E	2	Software Business No.1	fujitsujiro	306-4002	A-101010019	Tokyo office	Client	Desktop	In use	CT02	05/09/2015 19:32:51	Power Saving of PC
	3	Software Business No.2	fujitsutaro	306-4003	A-000000003	Sendai office	Client	Desktop	In use	CT03	05/09/2015 19:32:44	Power Saving of PC
	4	Software Business No.2	fujitsutaro	306-4004	A-000000009	Tokyo office	Client	Notebook	In trouble	CT04	05/09/2015 19:32:44	Power Saving of PC
	5	Software Development No.1	fujitsutaro	306-4005	A-000000001	Sendai office	Client	Notebook	In use	CT05	05/09/2015 19:32:45	Power Saving of PC
	6	Software Manufacturing No.1	Emma Fujitsu	306-4006	A-000000015	Sapporo office	Client	Desktop	In use	CT06	05/09/2015 19:32:46	Power Saving of PC
	7	Software Manufacturing No.1	Fujitsu Mngr.	306-4007	A-000000021	Sendai office	Client	Desktop	In use	CT07	05/09/2015 19:32:46	Power Saving of PC
E	8	Software Manufacturing No.3	James Fujitsu	306-4008	A-000000025	Okinawa offic	Client	Desktop	In use	CT08	05/09/2015 19:32:46	Power Saving of PC
	9	Software Manufacturing No.2	John Fujitsu	306-4009	A-000000002	Nagoya office	Client	Notebook	In use	CT09	05/09/2015 19:32:48	Power Saving of PC
	10	Software Manufacturing No.2	Michael Fujitsu	306-4010	A-000000004	Kobe office	Client	Desktop	In use	CT10	05/09/2015 19:32:48	Power Saving of PC
	11	Software Manufacturing No.2	Peter Fujitsu	306-4011	A-000000014	Nagoya office	Server	Desktop	In use	CT11	05/09/2015 19:32:49	Power Saving of Server
	12	Hardware Business No.1	Peter Fujitsu	306-4012	A-000000024	Osaka office	Client	Desktop	In use	CT12	05/09/2015 19:32:49	Power Saving of PC
	13	Hardware Business No.2	systemwalker	306-4013	A-000000018	Other office	Server	Desktop	In use	CT13	05/09/2015 19:32:50	Power Saving of Server
	14	Hardware Development No.1	Peter Fujitsu	306-4014	A-000000016	Osaka office	Client	Desktop	In use	CT14	05/09/2015 19:32:50	Power Saving of PC
	15	Hardware Manufacturing No.	systemwalker	306-4015	A-000000026	Tokyo office	Client	Notebook	Return Object	CT15	05/09/2015 19:32:51	Power Saving of PC
	16	Administrative Affairs Division	Peter Fujitsu	306-4016	A-000000007	Osaka office	Client	Desktop	In use	CT16	05/09/2015 19:32:52	Power Saving of PC
	17	Administrative Affairs Division	systemwalker	306-4017	A-000000013	Kobe office	Client	Notebook	In use	CT17	05/09/2015 19:32:52	Power Saving of PC
	18	General Affairs Division	Peter Fujitsu	306-4018	A-000000010	Osaka office	Client	Desktop	In use	CT18	05/09/2015 19:32:52	Power Saving of PC

The content of the above file is as follows.

Section (It is **Setting Location** when specifying location unit), **Related Asset Number**, **Asset Number** are arranged and displayed in ascending order.

Item	Description
E	Display it when the PC with ERR exists in the power saving setting.
No.	It is the number allocated to the information that has been output.
Section	It is the information of section.
User Name	It is the user name that uses the machine.
Phone No.	It is the telephone number of the user name that uses the machine.
Asset Number	It is the asset number of machine.
Setup Place	It is the setting location information of machine.
Type	It is the type information of machine.
HW Type	It is the hardware type information of machine. (Output the type of desktop/laptop/server/virtual PC.)
Availability	It is the availability of machine.
Device Name	It is used as the name of machine.
Collection Date/Time	It is the date and time when information has been registered.
User Memo	Output the selected user memo only when **Output user memo** is selected in the **Option** tab.
Power Saving Setting Status	It is the setting name of power saving setting.
Allow/Not Allow Audit	Output whether auditing is allowed or not. - Allow: PC that can collect power saving information and allows auditing. - Not allow: PC that cannot be audited since power saving information is not collected. It is unable to collect in any of the following cases. - When the CT prior to V13.2 is used - When inventory information is imported through linking with other product - In case of virtual PC
Monitor Power **HD Power** **System Standby** **System Sleep** **Other Settings**	Output the actual performance value and auditing result of power saving setting. The auditing result is output as follows. - o: Auditing result is OK - x: Auditing result is ERR - W: Auditing result is attention - -: Auditing result is information or non-auditing object *Output the actual performance value as - for the PC in which the power saving information is not collected in CT. *For the PC with battery such as laptop, output by separating with / when connecting to power/using battery. ***Other Setting Item**, only the PC with Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 and Windows Server(R) 2012 will be audited.

Item	Description
	Output o when all the auditing result of object items is OK, otherwise, output x. It is the setting name of power saving setting.

Note

If **Connection Server** in the **Server** tab of the **Environment Setup** window of CT is changed from the host name specified when building CS or DS, then the new server may be judged not to be an auditing target and may not be aggregated.

13.7 Output Power Consumption Status

This section describes how to output the power consumption.

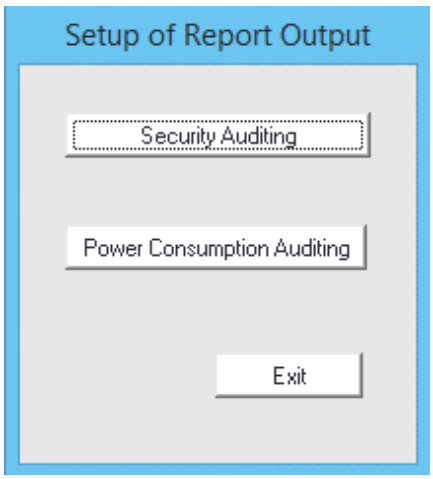
- "13.7.1 Preparation"
- "13.7.2 Procedure"
- "13.7.3 Example of Outputting Power Consumption Status"

13.7.1 Preparation

Perform the setting to be used in the calculation of power consumption.

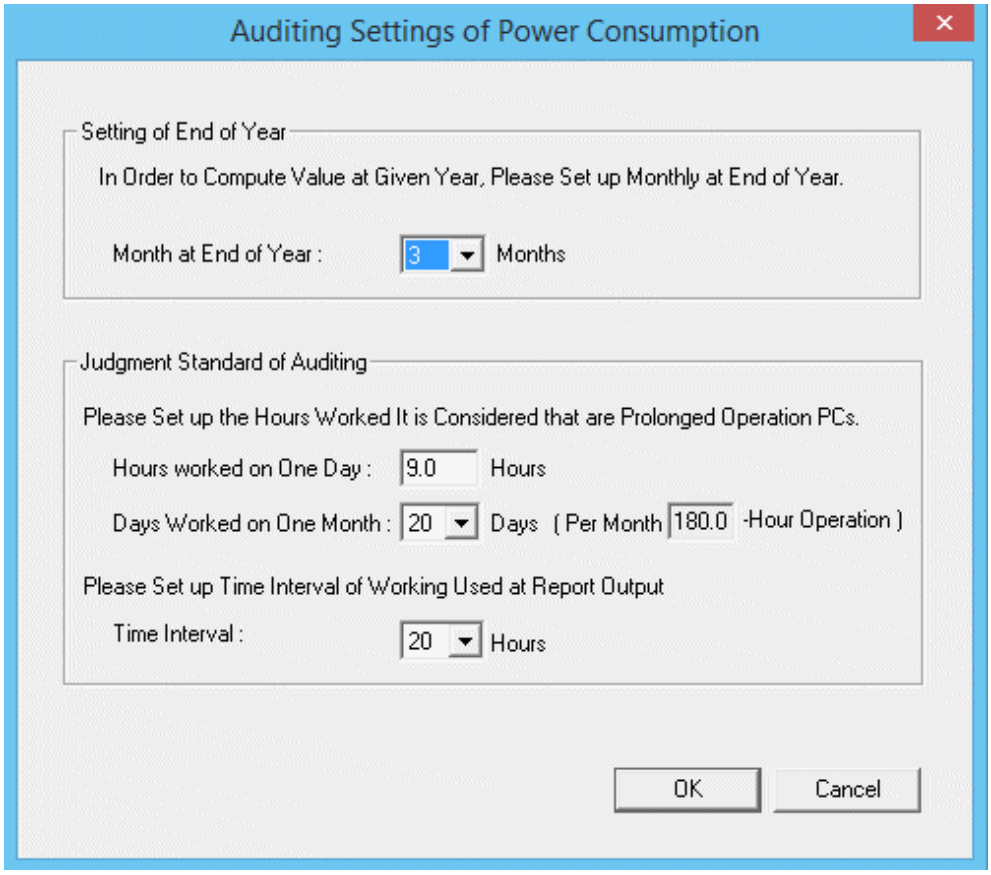
1. Logon to the AC menu.
2. Select **Setup of Report**.

   The following window will be displayed.



3. Select **Power Consumption Auditing**.

   The following window will be displayed.



4. Set the following items.

Item	Description
Setting of End of Year	Select the month as the end of fiscal year from the pull-down menu.
Judgment Standard of Auditing	Set the PC operation time of one day and the number of days of one month as the judgment standard of operation time. The PC operation time of one month calculated based on this will become the judgment result of PC of long-time operation. The number of the days of one month is used for outputting the number of PCs that work 24 hours over many days in the report as the judgment standard of days of 24h operation. Example) the PC operation time of one day is set to 8.0h, the number of days of one month is set to 20days, and the time interval is set to 20h, the number of PCs with the operation time of 160h, 180h, 200h can be confirmed in the report.

5. Click the **OK** button to save the set value.

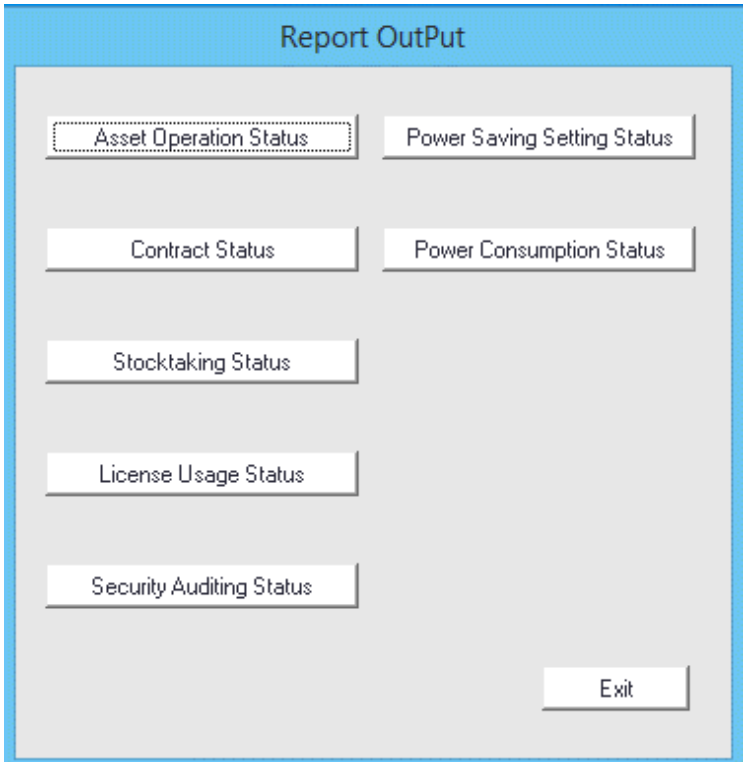
13.7.2 Procedure

The procedure of outputting power consumption is as follows.

1. Logon to the AC menu.

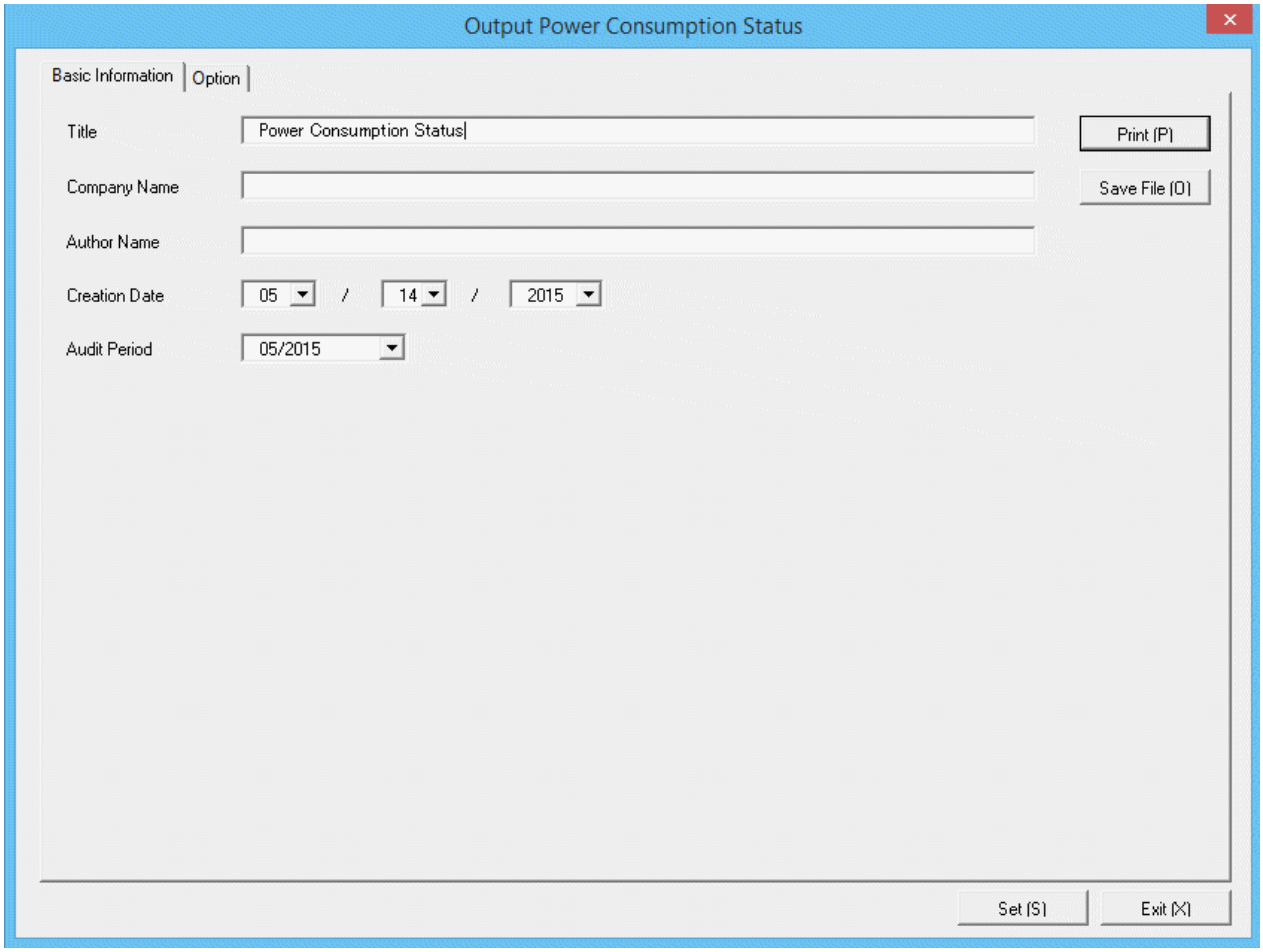
2. Select **Report Output**.

   The following window will be displayed.



3. Click the **Power Consumption Status** button.

   The following window will be displayed.

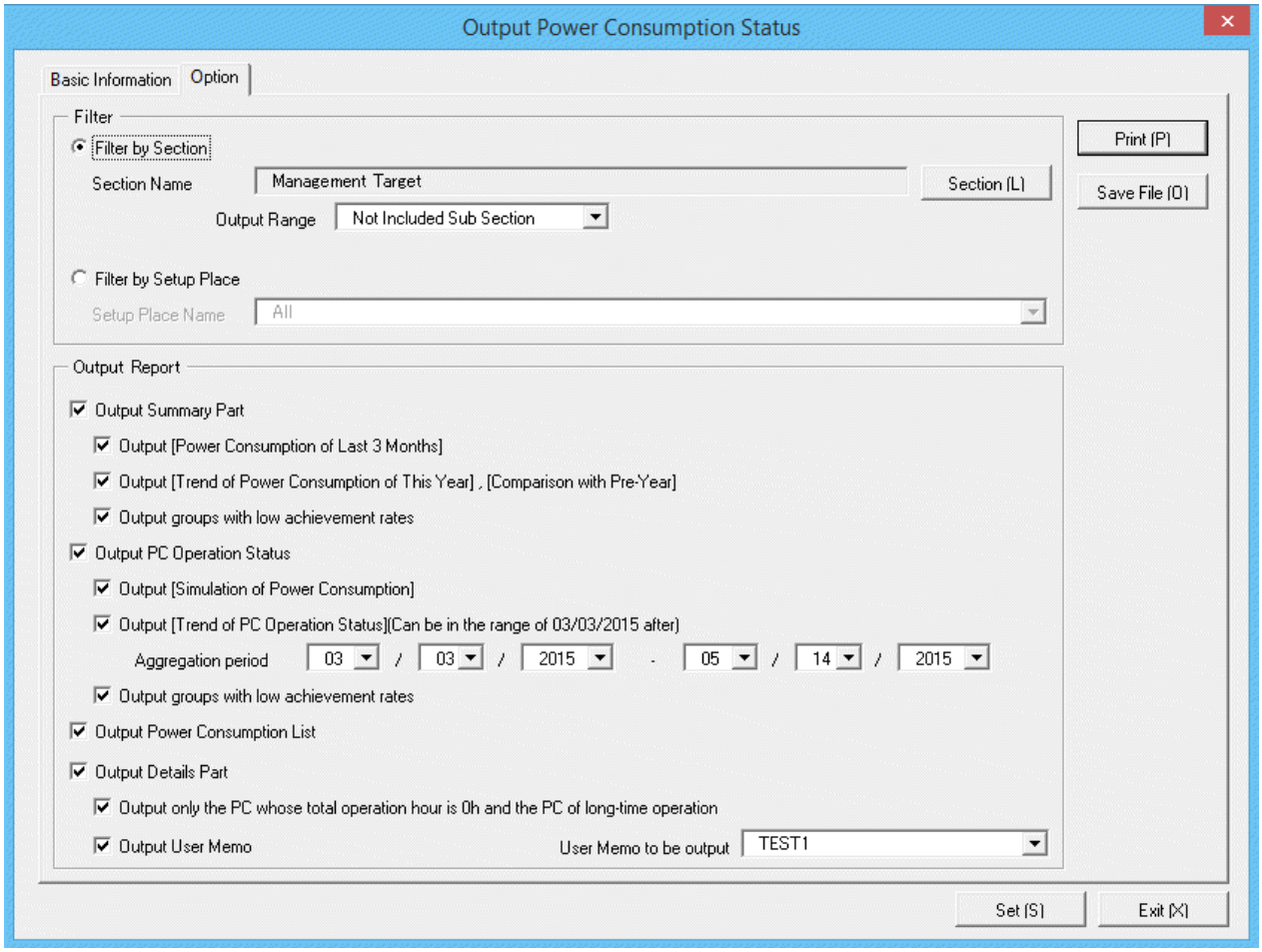


   Set the following information.

   In addition, click the **Set** button after setting, the set information can be displayed at next startup.

Tab Name	Item	Description
Basic Information	**Title**	Set the title name to be output to report. Up to 25 fullwidth characters or 50 halfwidth alphanumeric characters and symbols can be set.
	Company Name	Set the company name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Author Name	Set the author name to be output to report. Up to 32 fullwidth characters or 64 halfwidth alphanumeric characters and symbols can be set.
	Creation Date	Set the creation date to output in report.
	Audit Period	Set the month as the auditing target of power consumption. Selection from the current month to two months before can be made. Example: When it is November now, November and October can be selected

4. Select the **Option** tab to set the option information for report.



Set the following information.

Tab Name	Item		Description
Option	**Filter**	**Filter by Section**	Select it when outputting the auditing result of power consumption to report by section unit. - **Section Name**: Set the section to be output to report. - **Output Range**: Set the filtering range.
		Filter by Setup Place	Select it when outputting the auditing result of power consumption to report by location unit. - **Setup Place Name**: Set the location to be output to report.
	Output Reports	**Output Summary Part**	It is selected when outputting the summary part to report. - **Output Power Consumption of Last 3 Months**: Select it when outputting **Power Consumption of Last 3 Months** in summary part.

Tab Name	Item		Description
			It can be selected only when **Output Summary Part** is selected. - **Output Trend of Power Consumption of This Year** , **Comparison with Pre-Year**: Select it when outputting **Trend of Power Consumption of This Year** and **Comparison with Pre-Year** to the summary part. It can be selected only when **Output Summary Part** is selected.
			- **Output groups with low achievement rates**: Select it when outputting sections with low achievement rates (and setting location). Select the following. It can only be selected when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name - When **Filter by Setup Place** is selected - Select **All** in the location name
		Output PC Operation Status	Select it when outputting PC operation status. - **Output Simulation of Power Consumption**: Select it when outputting **Power Consumption of Last 3 Months** in PC operation status. It can be selected only when **Output PC Operation Status** is selected. - **Output Trend of PC Operation Status**: Select it when outputting **Trend of PC Operation Status** in PC operation status. It can be selected only when **Output PC Operation Status** is selected. In addition, when selected, set the aggregation period. - **Output groups with low achievement rates**: Select it when outputting sections with low achievement rates (and setting location). The following can be selected only when **Trend of PC Operation Status** is selected. - When **Filter by Section** is selected

Tab Name	Item		Description
			- Select **Management Target** in section name - Do not select **Not Configured** in section name - When **Filter by Setup Place** is selected - Select **All** in the location name
		Output Power Consumption List	Select it when outputting the power consumption list. Select the following. It can only be selected when **Output Summary Part** is selected. - When **Filter by Section** is selected - Select **Management Target** in section name - Do not select **Not Configured** in section name. - When **Filter by Setup Place** is selected - Select **Whole Company** in location name
		Output Details Part	Select it when outputting the details part. - **Output only the PC whose total operation hour is 0h and the PC of long-time operation**: Select only when outputting the PC that is not working or works long-time in details part. It can be selected only when **Output Details Part** is selected. - **Output User Memo**: Set whether to output the user memo of machine as one item of details part of machine. In addition, to output, select the user memo to be output.(Note)

Note) In user memo, the output relating to the power saving settings such as whether PC is required to work 24 hours can be used as the document for judging the existence of product of correspondent PC from the details part.

5. Output report.

Operate for the following cases.

- Print

  To print the report, click the **Print** button.

- Save as File

  To save the report as a file, click the **Save File** button.

  The file name to be saved can be set with the absolute path that is effective in Windows that is no more than 218 characters.

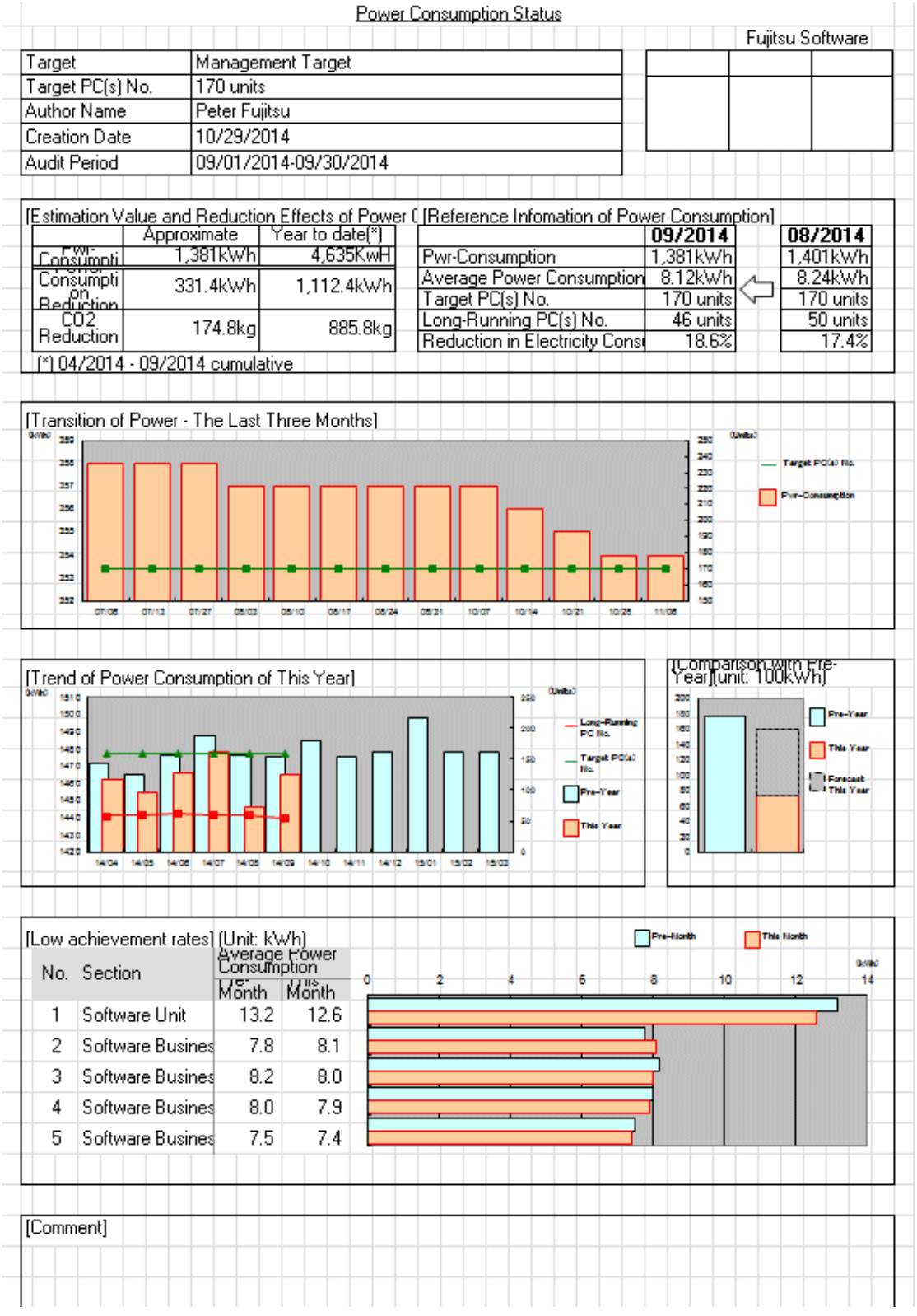
13.7.3 Example of Outputting Power Consumption Status

The report is composed of "Summary Part", "PC Availability", "List of Power Consumption", and "Details Part".

The following describes each of the "Summary Part", "PC Availability", "List of Power Consumption", and "Details Part".

Summary part

The "Summary Part" when saved as file is as follows.



The content of the above file is as follows.

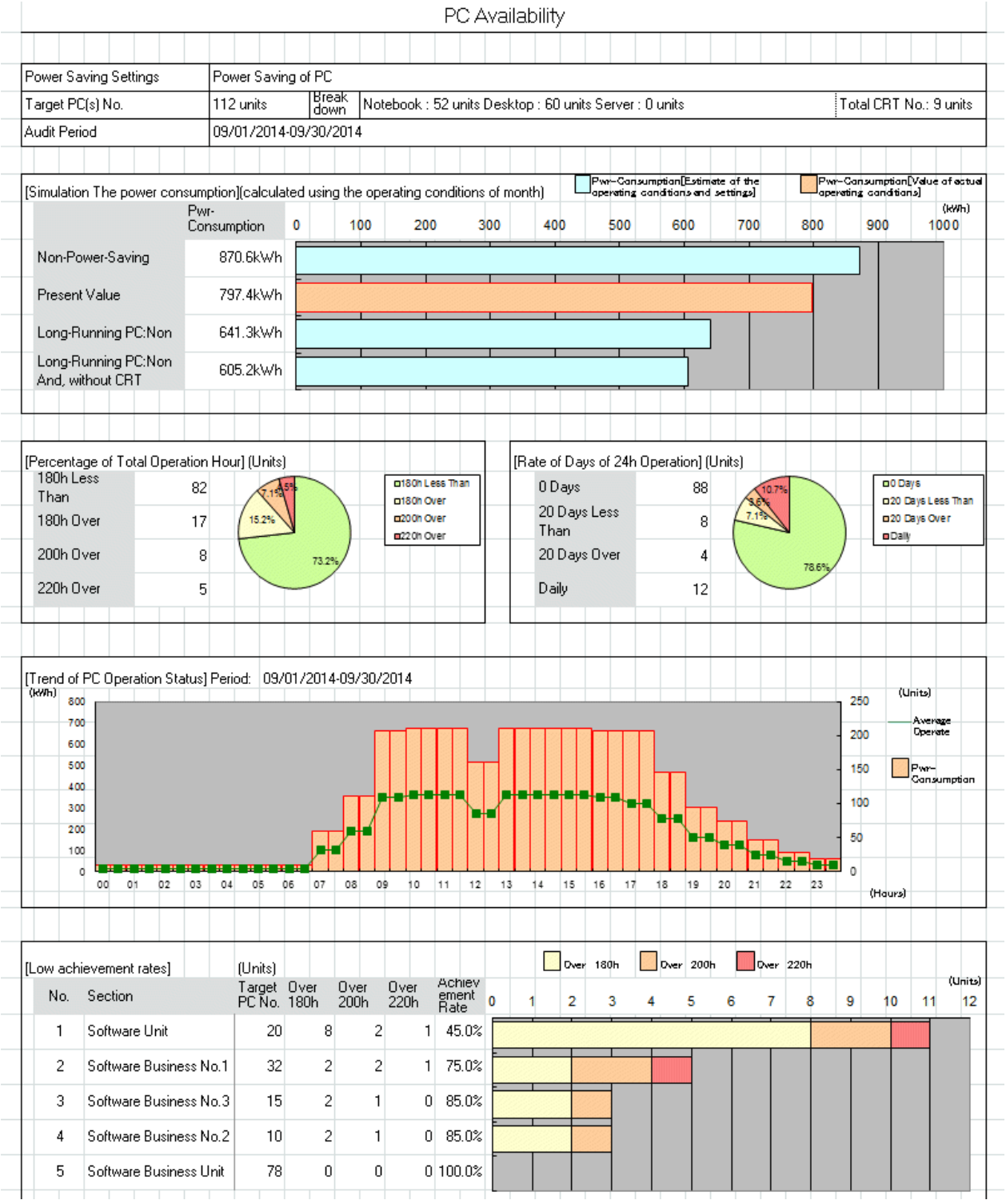
Item	Description
Fujitsu Software (The set value is displayed)	It is the information set in **Company Name** of the **Basic Information** tab.

Item	Description
Seal Column	It is the column for sealing on the created file. Here, since only the column for sealing is printed, use it freely.
Power Consumption Status (The set value is displayed)	It is the information set in **Title** of the **Basic Information** tab.
Target	It is the name of section or location as object. It is the information set in **Section Name** and **Setup Name** of the **Option** tab.
Target PC(s) No.	Among all PC in the section or location as the object, the version of CT is V14 or later, and it is the number of PCs working in the current month.
Author Name	Author of the file. it is the information set in **Author Name** of the **Basic Information** tab.
Creation Date	It is the date when file has been created. It is the information set in **Creation Date** of the **Basic Information** tab.
Audit Period	It is the period of month as auditing object. It is the information set in **Audit Period** in the **Basic Information** tab.
Estimation Value and Reduction Effects of Power Consumption	Output Power consumption reduction amount of Power consumption, reduction amount of CO2, estimation value of current month and total value of the year separately.
Reference Information of Power Consumption	Output the following information as the comparison information to the last month. - Power consumption - Average power consumption - Target PC(s) No. - Long-Running PC(s) No. - Reduction in Electricity Consumption
Transition of Power - The Last Three Months	Output the power consumption in the last 3 months and total of number of PCs by weeks.
Trend of Power Consumption of This Year	Output the power consumption of this year and total number of PCs by months. When the data of power consumption of last year exists, output the total.
Comparison with Pre-Year	Output the total value of last year and this year based on the month set in aggregation month. The predicted value till the end month of the year will be output for this year. Example: Set the aggregation month to March, and the current month is Nov. 2008 Period of last year: April 2007 ~ March 2008 Period of this year: April 2008 ~ October 2008 November 2008 ~ March 2009 (Prediction value) Calculation method of prediction value: Get the monthly average of the actual achievement of this year, multiply it with the number of remaining months to get the prediction value.
Low achievement rates	Output 5 sections with low achievement rates/locations according to the average power consumption of one PC of each section/location.

Item	Description
Comment	It is the input column for comment such as opinions.

PC availability

The "PC Availability" when saved as file is as follows.

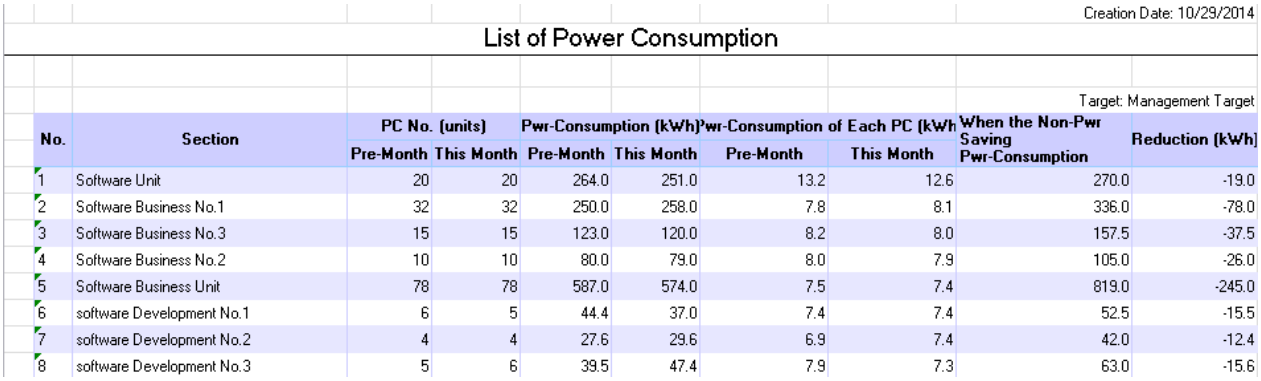


The content of the above file is as follows.

Item	Description
Power Saving Settings	It is the setting name of power saving setting as the object.
Target PC(s) No.	It is the PC set in the power saving setting as report object, and the number of PCs that are working in the current month.
Simulation of Power Consumption	Output the result of simulated power consumption. The following four types of result will be output. a. When power saving setting is not applicable Calculate not as the power saving operation in PC operation. b. When power saving setting is applicable The current actual performance value is equivalent to this. c. In the above "b" and PC without long-time operation Example: when 160h is set as the judgment standard of operation time PCs that work over 160h will be calculated as working 160h. d. In the above "c" and PC without CRT display Calculate the power consumption when replacing the CRT display with LCD. Without CRT display, the output value remains the same as "c".
Percentage of Total Operation Hour	Output the rate of PC that works long-time with pie chart.
Rate of Days of 24h Operation	Output the rate of PC that works 24h with pie chart.
Trend of PC Operation Status	Output the average number of PC of 24h operation in the specified period and power consumption with a graph.
Low achievement rates	Output 5 sections with low achievement rates/location of reduced achievement rate of PC of long-time operation.

List of power consumption

The "List of Power Consumption" when saved as file is as follows.



Creation Date: 10/29/2014

List of Power Consumption

Target: Management Target

No.	Section	PC No. (units)		Pwr-Consumption (kWh)		Pwr-Consumption of Each PC (kWh		When the Non-Pwr Saving Pwr-Consumption	Reduction (kWh)
		Pre-Month	This Month	Pre-Month	This Month	Pre-Month	This Month		
1	Software Unit	20	20	264.0	251.0	13.2	12.6	270.0	-19.0
2	Software Business No.1	32	32	250.0	258.0	7.8	8.1	336.0	-78.0
3	Software Business No.3	15	15	123.0	120.0	8.2	8.0	157.5	-37.5
4	Software Business No.2	10	10	80.0	79.0	8.0	7.9	105.0	-26.0
5	Software Business Unit	78	78	587.0	574.0	7.5	7.4	819.0	-245.0
6	software Development No.1	6	5	44.4	37.0	7.4	7.4	52.5	-15.5
7	software Development No.2	4	4	27.6	29.6	6.9	7.4	42.0	-12.4
8	software Development No.3	5	6	39.5	47.4	7.9	7.3	63.0	-15.6

Item	Description
No.	It is the number allocated to the information that has been output.
Section/Setup Place	It is the information of section/location.
PCs	It is the number of PCs of section/location. - **Pre-Month**:

Item	Description
	It is the number of PCs as auditing object last month. - **This Month**: It is the number of PCs as auditing object this month.
Pwr-Consumption	It is the power consumption of section/location. - **Pre-Month**: It is the power consumption of last month. - **This Month**: It is the power consumption of this month.
Pwr-Consumption of Each PC	It is the average power consumption of each PC in section/location. - **Pre-Month**: It is the average power consumption of each PC of last month. - **This Month**: It is the average power consumption of each PC of this month.
When the Non-Power Saving Pwr-Consumption	It is the assumed value of power consumption in non power saving calculated from the actual achievement of PC.
Reduction	It is the differential value between power consumption and power consumption in non power saving of current month.

Details part

The "Details Part" when saved as file is as follows.

Power Consumption Status

[E] The long-running PC, [W] a PC running the total time of 0h

	No.	Section	User Name	Phone No.	Asset Number	Setup Place	Type	HW Type	Availability	Device Name	Collection Date/Time	Running Necessity 24h	Power Saving Settings	Allow
	1	Software Business No.1	James Fujitsu	306-4001	A-101010015	Tokyo office	Client	Notebook		CT01	09/30/2014 13:33:01	Unnecessary	Power Saving of PC	
	2	Software Business No.1	Emma Fujitsu	306-4002	A-101010019	Tokyo office	Client	Desktop	In use	CT02	09/30/2014 19:32:51	Unnecessary	Power Saving of PC	
W	3	Software Business No.2	Michael Fujitsu	306-4003	A-000000003	Sendai office	Client	Desktop	In use	CT03	09/30/2014 19:32:44	Unnecessary	Power Saving of PC	
E	4	Software Business No.2	John Fujitsu	306-4004	A-000000009	Tokyo office	Client	Notebook	In tronble	CT04	09/30/2014 19:32:44	Unnecessary	Power Saving of PC	
E	5	Software Development No.1	Fujitsu Mngr.	306-4005	A-000000001	Sendai office	Client	Notebook	In use	CT05	09/30/2014 19:32:45	Unnecessary	Power Saving of PC	
	6	Software Manufacturing No.1	Emma Fujitsu	306-4006	A-000000015	Sapporo office	Client	Desktop	In use	CT06	09/30/2014 19:32:46	Unnecessary	Power Saving of PC	
E	7	Software Manufacturing No.1	Fujitsu Mngr.	306-4007	A-000000021	Sendai office	Client	Desktop	In use	CT07	09/30/2014 19:32:46	Unnecessary	Power Saving of PC	
E	8	Software Manufacturing No.3	James Fujitsu	306-4008	A-000000025	Okinawa office	Client	Desktop	In use	CT08	09/30/2014 19:32:46	Unnecessary	Power Saving of PC	
E	9	Software Manufacturing No.2	John Fujitsu	306-4009	A-000000002	Nagoya office	Client	Desktop	In use	CT09	09/30/2014 19:32:48	Unnecessary	Power Saving of PC	
	10	Software Manufacturing No.2	Michael Fujitsu	306-4010	A-000000004	Kobe office	Client	Desktop	In use	CT10	09/30/2014 19:32:48	Unnecessary	Power Saving of PC	
E	11	Software Manufacturing No.2	Peter Fujitsu	306-4011	A-000000014	Nagoya office	Server	Desktop	In use	CT11	09/30/2014 19:32:49	Necessary	Power Saving of Server	
	12	Hardware Business No.1	Peter Fujitsu	306-4012	A-000000024	Osaka office	Client	Desktop	In use	CT12	09/30/2014 19:32:49	Unnecessary	Power Saving of PC	
E	13	Hardware Business No.2	Emma Fujitsu	306-4013	A-000000018	Other office	Server	Desktop	In use	CT13	09/30/2014 19:32:50	Necessary	Power Saving of Server	
	14	Hardware Development No.1	Peter Fujitsu	306-4014	A-000000016	Osaka office	Client	Desktop	In use	CT14	09/30/2014 19:32:50	Unnecessary	Power Saving of PC	
E	15	Hardware Manufacturing No.2	Michael Fujitsu	306-4015	A-000000026	Tokyo office	Client	Notebook	Return Object	CT15	09/30/2014 19:32:51	Unnecessary	Power Saving of PC	
	16	Administrative Affairs Division	Peter Fujitsu	306-4016	A-000000007	Osaka office	Client	Desktop	In use	CT16	09/30/2014 19:32:52	Unnecessary	Power Saving of PC	
	17	Administrative Affairs Division	John Fujitsu	306-4017	A-000000013	Kobe office	Client	Notebook	In use	CT17	09/30/2014 19:32:52	Unnecessary	Power Saving of PC	
	18	General Affairs Division	Peter Fujitsu	306-4018	A-000000010	Osaka office	Client	Desktop	In use	CT18	09/30/2014 19:32:52	Unnecessary	Power Saving of PC	

The content of the above file is as follows.

Section (it is **Setting Location** when specifying location unit), **Related Asset Number**, **Asset Number** are arranged and displayed in ascending order.

Item	Description
W or **E**	It shows the status of operation time. **W**: PC that is not working (operation time is 0h). **E**: PC that is working long-time (operation time is more than the specified time).
No.	It is the number allocated to the information that has been output.

Item	Description
Section	It is the information of section.
User Name	It is the user name that uses the machine.
Phone No.	It is the telephone number of the user name that uses the machine.
Asset Number	It is the asset number of machine.
Setup Place	It is the setting location information of machine.
Type	It is the type information of machine.
HW Type	It is the hardware type information of machine. (Output the type of desktop/laptop/server/virtual PC.)
Availability	It is the availability of machine.
Device Name	It is the name to be used as machine.
Collection Date/Time	It is the date and time when information has been registered.
User Memo	Output the selected user memo only when **Output User Memo** is selected in the **Option** tab.
Power Saving Settings	It is the setting name of power saving setting.
Allow/Not Allow Audit	Output whether auditing is allows. - Allow: PC that can collect power saving information and can be audited - Not allowed: PC that cannot be audited since CT does not collect power information (the CT prior to V13.3 is used, or imported through linking with other product .etc)
Power Consumption of Pre-Month	It is the power consumption of last month.
Power Consumption	It is the power consumption of this month.
Total Operation Hour	It is the total operation hours.
System Standby Time	It is the total hours of system standby.
24h Operation Days	It is the total number of days of 24h operation.

Note

If **Connection Server** in the **Server** tab of the **Environment Setup** window of CT is changed from the host name specified when building CS or DS, then the new server may be judged not to be an auditing target and may not be aggregated.

Chapter 14 Link with Other Products

This chapter explains how Systemwalker Desktop Patrol is linked to other products.

14.1 Event Linkage

Systemwalker Desktop Patrol is linked to events of the following products.

- Windows version, after Systemwalker CentricMGR V10.0L20

Event linkage has the following 2 applications. In event linkage, the message produced in Systemwalker Desktop Patrol can be displayed in the above products.

- Event linkage based on alarm notification
- Event linkage based on event log output

It's necessary to set up Systemwalker Desktop Patrol to link the events. In addition, refer to Systemwalker Centric Manage Manual for Settings of the other products.

14.1.1 Event linkage Based on Alarm Notification

See below for the event linkage steps based on alarm notification.

Settings of Systemwalker Centric Manager

Set Systemwalker Centric Manager to be auditing the PC event log installed with CS. Refer to Systemwalker Centric Manager Manual for Settings method.

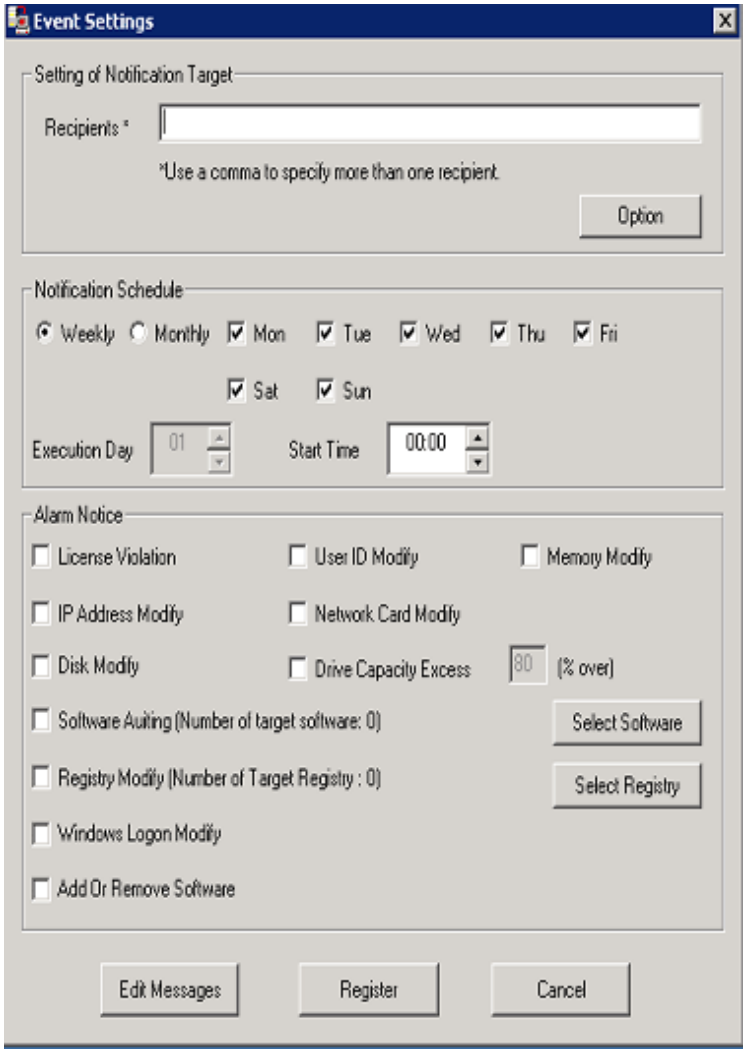
Settings of Systemwalker Desktop Patrol

Take the following steps.

1. Set up "alarm notification".

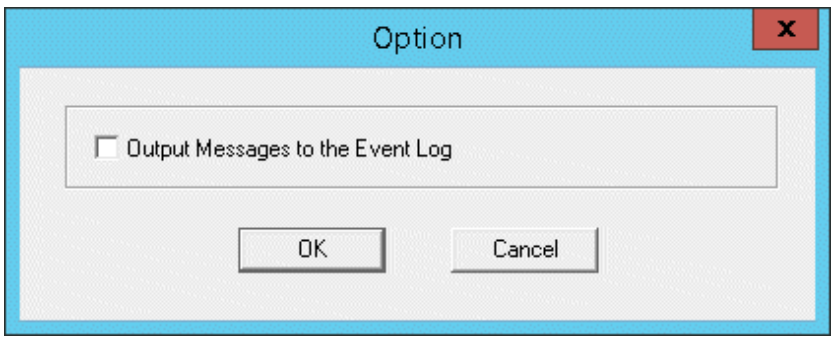
   Refer to "2.5 Set Alarm Notification" for settings of alarm notification.

After the settings is finished, the **Event Settings** window will be displayed.



2. Click **Option** button.

   The **Option** window will be displayed.



3. Select the check box of **Output Messages to the Event Log**, Click the **OK** button.
4. Click the **Register** button in the window of **Event Settings**.

14.1.2 Event linkage Based on Event Log Output

Take the following steps for event linkage based on event log output.

Settings of Systemwalker Centric Manager

Set Systemwalker Centric Manager to be auditing the PC event log installed with CS and DS. Refer to Systemwalker Centric Manager Manual for settings method.

Settings of Systemwalker Desktop Patrol

Initial value after installation of Systemwalker Desktop Patrol is set to be log output of all kinds of events. The file will be edited and defined when changing output of the event log.

Difference	Initial action at product import	Output settings
Information	Output	Can be modified (output/no output)
Warning	Output	Can be modified (output/no output)
Error	Output	Cannot be modified (always output)

Remarks: source name of event log is "DTPServer".

File name

Edit the definition file under CS or DS.

Systemwalker Desktop Patrol Installation Directory\common\etc\dtpevent

Edit item

Item/key name	Explanation	Set value
EVENT	Section name	-
INFO	Output information log or not	One of the following settings. 0: No output 1: Output (Default)
WARNING	Output warning log or not	One of the following settings. 0: No output 1: Output (Default)

Example of definition file

```
[EVENT]
INFO=1
WARNING=1
```

Auditing method

Source name of the event log output from Systemwalker Desktop Patrol is set to be "DTPServer". The event log with source name of "DTPServer" will be audited in Systemwalker Centric Manager.

As for auditing method of Systemwalker Centric Manager, refer to Systemwalker Centric Manager Manual.

14.2 Collection of Inventory Information

In Systemwalker Desktop Patrol, the following methods can be adopted to collect Inventory information gathered by other products' function.

- Inventory information collected by Systemwalker Centric Manager
- Inventory information collected by CSV linkage

The following Inventory information can be collected.

Collect Information	Collection method		
	Centric Manager linkage		CSV linkage
	Windows	UNIX	
Hardware information	Y	Y	Y
Software information-Document search	Y(Note 1)	N	Y
Software information - Registry search (Search of procedure name)	Y	N	Y
Software information - Registry search (Search of any key and value)	N	N	Y
User information	Y(Note 2)	Y(Note 2)	Y
Software operation status	N	N	Y
Registry information	N	N	N
EXE information	N	N	N

Y: Collectable

N: Not collectable

Note 1) It may not be able to collect Inventory with an Agentless monitoring. Refer to "Systemwalker Centric Manager Manual" for collection.

Note 2) It is not possible to collect Inventory with an Agentless monitoring.

See below for the version of Systemwalker Centric Manager which can be linked.

Product name	Remarks
After Systemwalker Centric Manager V13.0.0	It is able to link with Operation Management Server and Section Management Server (Note).

Note)

It is only able to link with the Operation Management Server when Inventory is collected with an Agentless monitoring. Coexistence with the Operation Management Server is also realized in the case of coexistence with Centric Manager. Inventory information will be imported from the Operation Management Server in lack of coexistence with Centric Manager.

14.2.1 Inventory Information Collection with Systemwalker Centric Manager

The procedure of collecting Inventory information with function of Systemwalker Centric Manager is as follows.

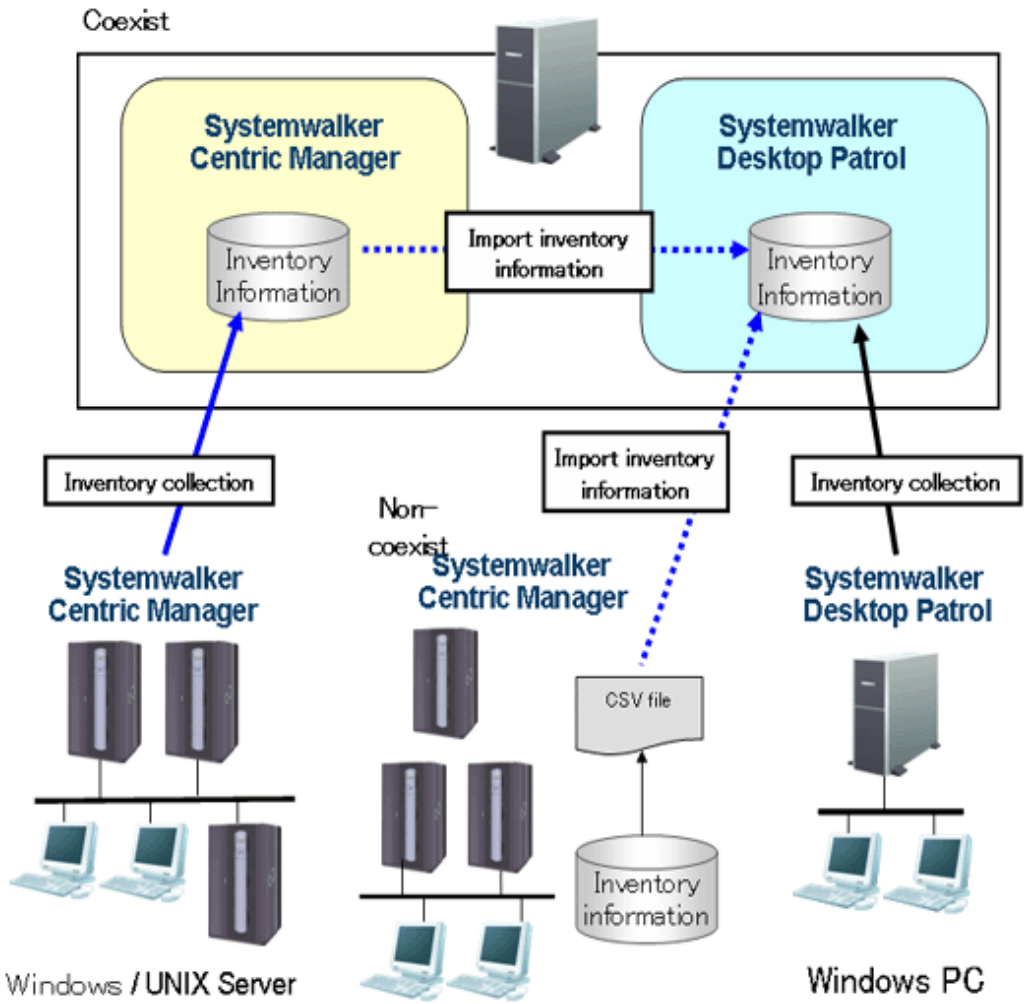
Linkage method

There are following two linkage methods to collect Inventory information with function of Systemwalker Centric Manager.

- Linkage method of coexistence of Systemwalker Desktop Patrol and Systemwalker Centric Manager(Coexistence type)

- Linkage method of non-coexistence of Systemwalker Desktop Patrol and Systemwalker Centric Manager(Non-coexistence type)

The application scheme is described respectively as below.



The following describes the linkage methods separately with and without coexistence with Systemwalker Centric Manager.

14.2.1.1 Linkage Method with Coexistence with Systemwalker Centric Manager

In PC installed with Systemwalker Centric Manager, by installing CS or DS, the Inventory information collected through function of Systemwalker Centric Manager can be imported to Systemwalker Desktop Patrol.

Systemwalker Centric Manager and Systemwalker Desktop Patrol shall be set up separately in the case of Inventory information collection through linkage with Systemwalker Centric Manager.

Settings of Systemwalker Centric Manager

The procedure of setting Systemwalker Centric Manager is shown as follows.

1. Output software search condition of Systemwalker Desktop Patrol.

   Using the following command to output the definition of software search condition registered in the software dictionary of Systemwalker Desktop Patrol. Output the software search condition selected in **Environment Setup** > **Software Auditing** in main menu.

   This definition is the software dictionary that collects Inventory in Systemwalker Centric Manager.

```
DTP Installation directory\FJSVsbiis\bin\EtpSoftDic.exe
```

Refer to *Systemwalker Desktop Patrol Reference Manual* for detailed information about the command of "EtpSoftDic.exe".

2. Software dictionary format changed to Systemwalker Centric Manager and registration.

   Execute the following command, change the software search condition output from "Step 1" to software dictionary format of Systemwalker Centric Manager and register.

   Change in the state that the Software Dictionary Editor window of the resource distribution function of Systemwalker Centric Manager has not been initiated.

   ```
   DTP Installation directory\FJSVsbiis\bin\SoftDicCMGR.exe
   ```

   Refer to *Systemwalker Desktop Patrol Reference Manual* for detailed information about the command of "SoftDicCMGR.exe".

3. Distribute and install the software dictionary to each server/client of Systemwalker Centric Manager.

   By distributing and installing the software dictionary, the software information of server/client of Systemwalker Centric Manager running in Windows can be collected.

   The software information of Systemwalker Centric Manager running in UNIX and part of the software information using an Agentless monitoring will not be collected.

   Refer to Systemwalker Centric Manager Manual for distribution method.

Settings of Systemwalker Desktop Patrol

The procedure of setting Systemwalker Desktop Patrol is shown as follows.

1. Set for importing the Inventory information collected by Systemwalker Centric Manager to Systemwalker Desktop Patrol.

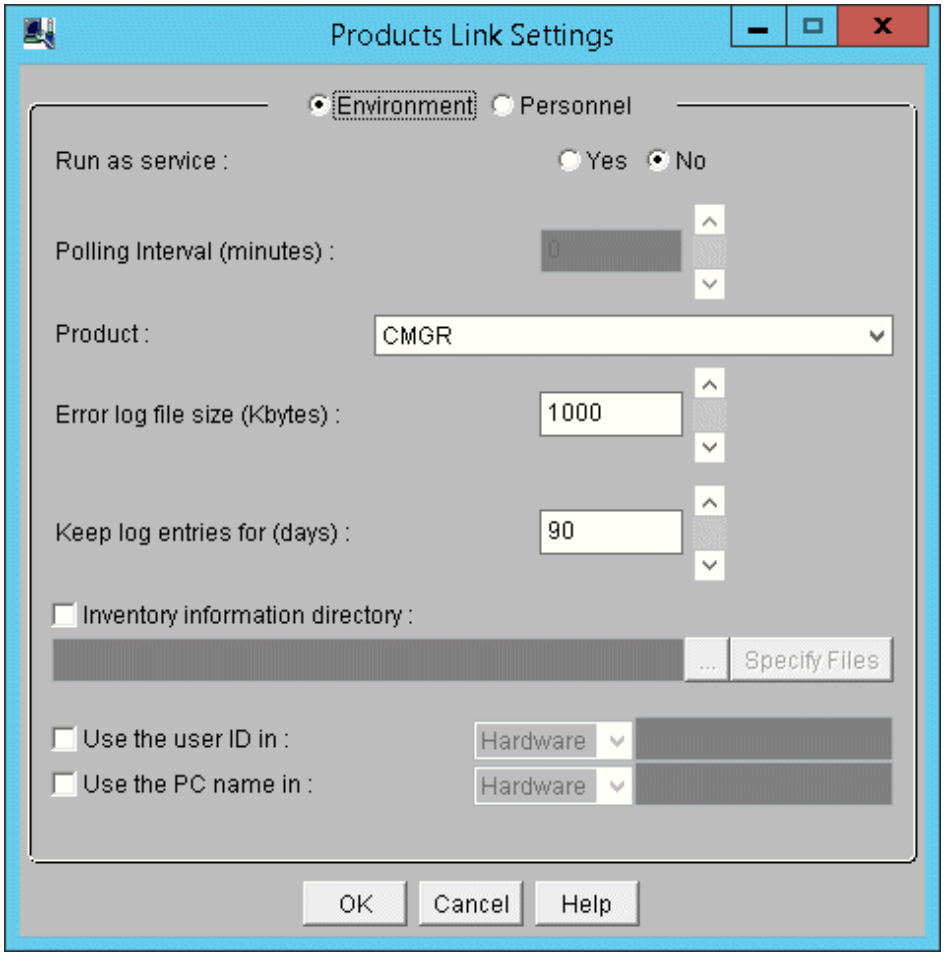
   - Import with CS

     Select **Start** > **Procedure** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Linkage with other products-Environment Setup**, or **Apps** > **Systemwalker Desktop Patrol** > **Products Link Settings**.

   - Import with DS

     Run "iisSettings.exe" in "DTP installation directory\FJSVsbiis\bin".

The **Products Link Settings** window will be displayed.



a. Enter the following information, click the **OK** button.

Item	Explanation
Run as service	- When **Yes** is selected The Inventory information collected will be imported automatically according to polling interval. - When **No** is selected Inventory information will not be imported automatically. Execute the "InvSend.exe" command to import Inventory information. *__No__ must be selected in lack of coexistence with Systemwalker Centric Manager.
Polling Interval(minute)	Specify import interval of Inventory information.
Product	Select **CMGR** in the drop down list.
Error log file size (Kbytes)	Specify file size of error log.
Keep log entries for (days)	Specify number of days to save the log when error occurs as record.
Use the user ID in	Refer to the following "Settings of user ID and PC name".

Item	Explanation
Use the PC name in	Refer to the following "Settings of user ID and PC name".

Remarks: Items set in **Use the user ID in** and **Use the PC name in** have preference over the settings of **User ID** and **PC Name** when the single choice button of **Personnel** is selected.

b. The settings will be reflected when the Inventory information is collected in the next time.

2. Linkage function of other products won't start just after the installation is finished. Restart the "ITBudgetMGR (INV)" service in **Management tools** > **Service** after the above settings is finished.

Notes

Initial setting of the Inventory information collected by Systemwalker Centric Manager is only import of client information. Edit the following file to collect the server's Inventory information.

DTP Installation directory\FJSVsbiis\env\FJSVsbiis.ini

Cancel the note of "#CollectNode=all" to the above file (#).

Thereby, the Inventory information of the server in coexistence with Systemwalker Desktop Patrol will also be imported, therefore, in the settings of Systemwalker Centric Manager, change to the settings that the Inventory information of the server in coexistence with Systemwalker Desktop Patrol will not be collected.

Settings of user ID and PC name

- When user ID and PC name is omitted

In Systemwalker Desktop Patrol, user ID and PC name is used to identify Inventory information of each PC.

User ID, PC name and the following information will be set automatically when Inventory information collected by Systemwalker Centric Manager is imported to Systemwalker Desktop Patrol.

User ID	Host name of CS and DS Set to be the first 20 character s in the host name displayed in **Server list** in **Environment Setup** > **CS/DS Settings and Status** in main menu. If the user ID is repetitive, change the steps under "When designating user ID and PC name".
PC name	IP address of each PC

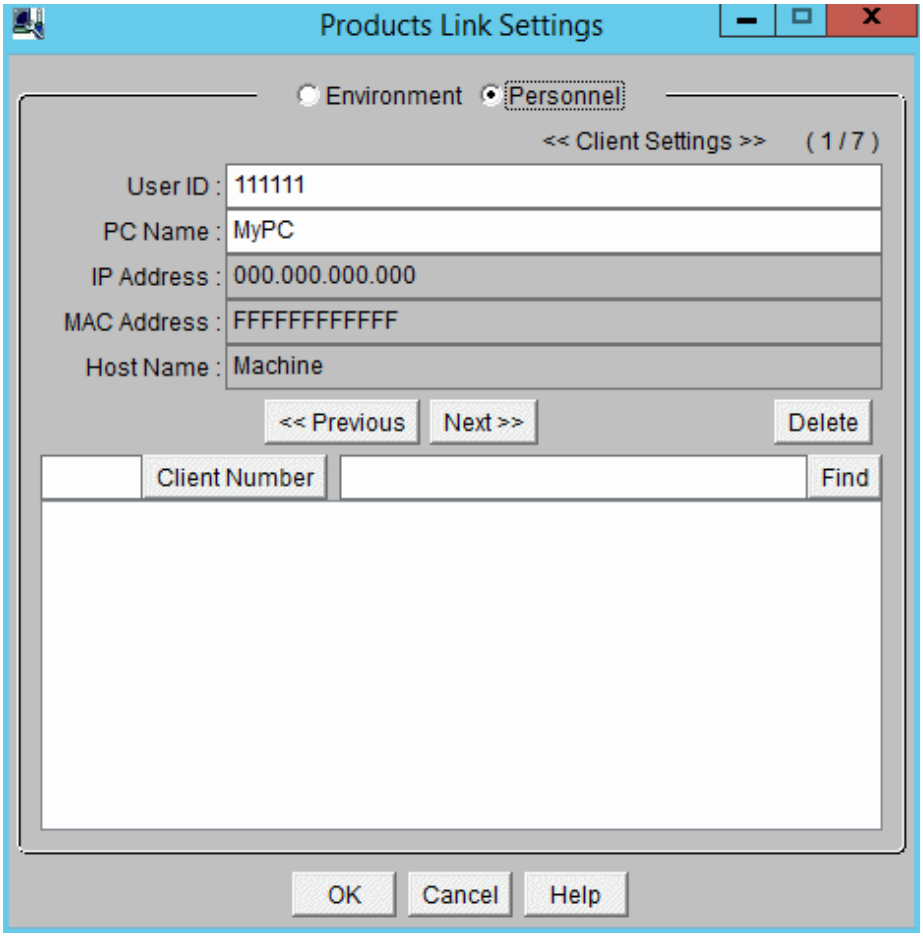
Note

If the PC name is omitted and only an IPv6 address is used, the colon (:) of the IPv6 address is changed to a period (.).

To change the user ID and PC name of inventory information imported to Systemwalker Desktop Patrol, select **Personnel** in **Products Link Settings** and set the user ID and PC name.

Before selecting **Personnel**, in **Product**, select the collection method to be used for importing to Systemwalker Desktop Patrol.

If you select the wrong value in **Product** and then select **Personnel**, click **Cancel** to close the **Products Link Settings** window. Open the **Products Link Settings** window again and select the correct value in **Product**.



- When designating user ID and PC name

  - **Use the user ID in**: set random message in the hardware information and user information of the Inventory information collected.

    Example) When value "2" is used in user information

    Select "User" in the drop-down list, input "2,2" in the right column.

  - **Use the PC name in**: set random message in the hardware information and user information of the Inventory information collected.

    Example) When the host name of the hardware information is used

    Select "Hardware" in the drop-down list, input "6" in the right column.

14.2.1.2 Linkage Method without Coexistence with Systemwalker Centric Manager

In UNIX server and PC not installed with Systemwalker Centric Manager, the Inventory information can be collected through function of Systemwalker Centric Manager and imported to Systemwalker Desktop Patrol.

Systemwalker Centric Manager and Systemwalker Desktop Patrol shall be set up separately in the case of Inventory information collection through linkage with Systemwalker Centric Manager.

Settings of Systemwalker Centric Manager

Take the following steps to set up Systemwalker Centric Manager.

1. Output of software retrieval condition of Systemwalker Desktop Patrol.

   Using the following command to output the definition of software retrieval condition registered in the software dictionary of Systemwalker Desktop Patrol. Output the software retrieval condition selected in **Environment Setup** > **Software Auditing** in main menu.

   This definition is the software dictionary when Systemwalker Centric Manager is used to collects Inventory information.

   ```
   DTP Installation directory\FJSVsbiis\bin\EtpSoftDic.exe
   ```

   Refer to *Systemwalker Desktop Patrol Reference Manual* for detailed information of the command of "EtpSoftDic.exe".

2. Modify the software dictionary format of Systemwalker Centric Manager

   Execute the following command, modify the software search condition output from "step 1" to the software dictionary format of Systemwalker Centric Manager.

   ```
   DTP Installation directory\FJSVsbiis\bin\SoftDicCMGR.exe
   ```

   Refer to *Systemwalker Desktop Patrol Reference Manual* for detailed information of the command of "SoftDicCMGR.exe".

   The software dictionary will be output to the following file.

   ```
   DTP Installation directory\FJSVsbiis\env\CMPRDINV.TXT
   ```

3. Registration of software dictionary in Systemwalker Centric Manager

   Save the software dictionary output from "step 2" to the directory under Systemwalker Centric Manager.

   The saving shall be carried out when the Software Dictionary Editor window of the resource distribution function of Systemwalker Centric Manager is not initiated.

   - UNIX condition

     Save to the directory under the Operation Management Client of Systemwalker Centric Manager.

     ```
     Systemwalker Centric Manager Installation directory\mpwalker.dm\mpdrmsop\etc
     ```

   - Windows condition

     Save to the directory under the Operation Management Server of Systemwalker Centric Manager.

     ```
     Systemwalker Centric Manager Installation directory\mpwalker.dm\mpdrmssv\etc
     ```

4. Distribute and use the software dictionary to each server/client of Systemwalker Centric Manager.

   By distributing and using the software dictionary, software information of the server/client of Systemwalker Centric Manager running in Windows can be collected.

   The software information of Systemwalker Centric Manager running in UNIX and part of the software information using an Agentless monitoring will not be collected.

   Refer to "Systemwalker Centric Manager Manual" for distribution method.

Settings of Systemwalker Desktop Patrol

Refer to "Settings of Systemwalker Desktop Patrol" for setup steps of Systemwalker Desktop Patrol.

In addition, the following settings must be completed in environment definition of the window of **Products Link Settings** without coexistence with Systemwalker Centric Manager.

- **Run as service**: Select **No**

Steps to Import Inventory information to Systemwalker Desktop Patrol

Take the following steps to import the Inventory information collected by Systemwalker Centric Manager to Systemwalker Desktop Patrol.

1. Perform the following operations on the Operation Management Server of Systemwalker Centric Manager.

   a. Create the folder to store Inventory information.

   b. Use command prompt to move to this folder, execute the following command.

   ```
   drmscsv -a merge -k inv -i hard -s distribution domain name -o hard.csv
   ```

   ```
   drmscsv -a merge -k inv -i soft -s distribution domain name -o soft.csv
   ```

   Specify the server name to be imported in Inventory information in "Distribution Domain Name".

   The file name designated in "-o option" must be one of the following.

   - hard.csv
   - soft.csv

   Specify name of the Operation Management Server in "-s option" when importing the Inventory information collected through an Agentless monitoring.

   The Inventory information which exports the above command is only for the distribution domain designated by the command and the client under the distribution domain. The Inventory information of the sever under the distribution domain designated by the command, or of the client outside of the distribution domain designated by the command, will not be exported.

   Refer to Systemwalker Centric Manager Manual for detailed information about the command.

   c. Repeat the steps from "a)" to "b)" when there are many servers to be imported with Inventory information. At this time, do not change the file name corresponding to the folder in each server.

2. Copy the folder of Inventory information export to any folder in CS.

3. Use the command under CS operation to import Inventory to Systemwalker Desktop Patrol.

   ```
   DTP Installation directory\FJSVsbiis\bin\InvSend.exe CMGR folder name
   ```

   Refer to *Systemwalker Desktop Patrol Reference Manual* for detailed information about the command of "InvSend.exe".

4. Repeat the step of "3." to when there are many servers to be imported with Inventory information.

14.2.2 Inventory Information Collection with CSV Linkage

Inventory information can be collected with CSV linkage by creating the CSV format file to record the PC's Inventory information and registering to Systemwalker Desktop Patrol.

Take the following steps.

1. Creation of CSV format file
2. Register to Systemwalker Desktop Patrol

Creation of CSV format file

Format of the CSV format file is based on information of the following CSV format (ASCII code).

- Data in unit of line(till new line)
- Each item to be indicated with double quotation marks """. Software operation status will not be indicated with double quotation marks """.

- Items are separated from each other by comma ",".
- Leave blank for no data item. (for example: marked as "," and ",,")

Due to the above reasons, double quotation marks """ and comma "," won't be used in item data. The data having used those marks won't be saved.

Item of software operation status won't be indicated with double quotation marks "". But if the item data includes comma "," and double quotation marks """, the item will be indicated with double quotation marks """. If the item data includes double quotation marks """, double quotation marks """ will be repeatedly marked as "".

Example)

Value of item data	Value recorded in CSV file
AA,AA	"AA,AA"
BB"BB	"BB""BB"

Format of one piece of information in each Inventory information is shown as below. "(mandatory)" item information means mandatory item. The Inventory information without item information is invalid. In addition, the item information of "(lowest limit needed)" is needed for normal operation of the function. Save virtual information when there is no information to save.

Hardware information

No.	Item	Item data format	Item type	Remarks
0	Client key(mandatory)	"Identification name of client"	String	Only key to identify client.
1	PC attribution (lowest limit needed)	"Attribution"	String	
2	CPU name (lowest limit needed)	"CPU"	String	Name of CPU.
3	Memory size(lowest limit needed)	"Memory size"	Number	Unit: KiloByte
4	Drive information (lowest limit needed)	"Drive name, drive type, capacity, available capacity,..."	"String, String, Number, Number"	Unit of capacity/ available capacity: KiloByte. Fixed character string for drive type (refer to *1). Can specify many.
5	Network card information (lowest limit needed)	"Name of network card, MAC address(mandatory),..."	"String, String"	Name of network drive and MAC address of network card (halfwidth 12 digits). Can specify many.
6	Host name(lowest limit needed)	"Full domain name,..."	String	host1 and host1.budgetmgr.com etc. Corresponding network card information. Can specify many.

No.	Item	Item data format	Item type	Remarks
7	IP address (mandatory)	"IP address,..."	String	IPv4: Address in xxx.xxx.xxx.xxx format. IPv6: Address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format. Corresponding network card information. Can specify many. Note - In dual stack environments, specify IPv4 and IPv6 addresses in that order, separated with a forward slash (/). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y - When specifying an IPv6 address only, precede it with a forward slash (/). Example: /yyyy:yyyy::y:y - Separate multiple IPv6 addresses with a semicolon (;). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y;zzzz:zzzz::z:z - Specify IPv6 addresses in RFC5952 format. - Do not specify multiple IPv4 addresses.
8	OS name(lowest limit needed)	"OS name"	String	Fixed character string for OS name(refer to *2).

No.	Item	Item data format	Item type	Remarks
9	BIOS version/date	"BIOS version, date"	"String, String"	Name and date of BIOS version. PhoenixBIOS 4.0 Release 6.0,06/02/97 and etc.
10	Computer name	"Computer name"	String	Host name without domain.
11	Domain name	"Domain name"	String	Suffix of domain.
12	Login name	"Login name"	String	Login user.
13	CPU Clock Speed	"CPU Clock Speed"	Number	CPU Clock Speed. Unit: MegaHertz
14	Number of actual installation	"Number of actual installation"	Number	Number of actually installed CPU. Unit: Numeral.
15	Detailed information of CPU	"Detailed information of CPU"	String	Detailed information of CPU.
16	Size of swap file	"Size of swap file"	Number	Unit: KiloByte
17	Name of keyboard type	"Keyboard type"	String	Type of keyboard.
18	Installation Language	"Language"	String	Type of language.
19	Name of mouse type	"Mouse type"	String	Type of mouse.
20	Number of mouse buttons	"Number of mouse buttons"	Number	Number of mouse buttons. Unit: Numeral
21	Manufacturer Name	"Manufacturer Name"	String	Manufacturing place of PC.
22	PC model	"PC model"	String	PC model(type)
23	PC serial	"PC serial"	String	PC serial number(PCID)
24	Session level cache, second level cache	"Session level cache, second level cache"	"Number, Number"	Size of Session level cache and second level cache. Unit: KiloByte
25	OS buliding number	"OS building number"	String	Construction number of Windows OS.
26	service pack	"service pack"	String	Number of service pack.
27	DOS version	"DOS version"	String	DOS Version.
28	User name	"User name"	String	Name of installed user of Windows OS.
29	Company name	"Company name"	String	Company name of installed user.
30	OS product ID	"OS product ID"	String	Product ID of Windows OS.

No.	Item	Item data format	Item type	Remarks
31	Windows directory name	"Windows directory"	String	Windows installation directory.
32	Name of system directory	"System directory"	String	Windows system directory.
33	Image resolution	"Width, height"	"Number, Number"	Monitor resolution.
34	Video adapter	"Video adapter"	String	Name of video adapter.
35	Size of video memory	"Size of video memory"	Number	Memory size of video adapter card Unit: KiloByte
36	Pixel	"Pixel"	Number	Display pixel. Unit: Numeral.
37	Monitor name	"Monitor name"	String	Name of monitor.
38	Name of Screen Saver	"Name of Screen Saver"	String	Name of screen capture tool.
39	Window update rate	"Window update rate"	Number	Cycle number of monitor. Unit: Hertz
40	Label	"Label,..."	String	Corresponding to drive information. Can specify many.
41	Type of file system	"Type of file system,..."	String	Corresponding to drive information. Can specify many.
42	Subnet mask	"Subnet mask,..."	String	Corresponding to network card information Can specify many. Specify the prefix length of IPv6 addresses. Note - In dual stack environments, specify IPv4 and IPv6 addresses in that order, separated with a forward slash (/). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y - When specifying an IPv6 address only, precede it

No.	Item	Item data format	Item type	Remarks
				with a forward slash (/). Example: /yyyy:yyyy::y:y - Separate multiple IPv6 addresses with a semicolon (;). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y;zzzz:zzzz::z:z - Specify IPv6 addresses in RFC5952 format. - Do not specify multiple IPv4 addresses.
43	Default gateway	"Default gateway,..."	String	Corresponding to network card information. Can specify many. Note - In dual stack environments, specify IPv4 and IPv6 addresses in that order, separated with a forward slash (/). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y - When specifying an IPv6 address only, precede it with a forward slash (/). Example: /yyyy:yyyy::y:y - Separate multiple IPv6 addresses with a semicolon (;). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y;zzzz:zzzz::z:z

No.	Item	Item data format	Item type	Remarks
				- Specify IPv6 addresses in RFC5952 format. - Do not specify multiple IPv4 addresses.
44	DHCP server	"DHCP server"	String	Name of DHCP server. Can specify many. Note - In dual stack environments, specify IPv4 and IPv6 addresses in that order, separated with a forward slash (/). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y - When specifying an IPv6 address only, precede it with a forward slash (/). Example: /yyyy:yyyy::y:y - Separate multiple IPv6 addresses with a semicolon (;). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y;zzzz:zzzz::z:z - Specify IPv6 addresses in RFC5952 format. - Do not specify multiple IPv4 addresses.
45	DNS server	"DNS server"	String	Name of DNS server. Can specify many. Note - In dual stack environments,

No.	Item	Item data format	Item type	Remarks
				specify IPv4 and IPv6 addresses in that order, separated with a forward slash (/). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y - When specifying an IPv6 address only, precede it with a forward slash (/). Example: /yyyy:yyyy::y:y - Separate multiple IPv6 addresses with a semicolon (;). Example: xxx.xxx.xxx.xxx/yyyy:yyyy::y:y;zzzz:zzzz::z:z - Specify IPv6 addresses in RFC5952 format. - Do not specify multiple IPv4 addresses.
46	Printer name	"Printer name,..."	String	Printer information: name of printer. Can specify many.
47	Printer type	"Printer type,..."	String	Printer information: type of printer. Corresponding to printer name. Can specify many.
48	CD-ROM device name	"CD-ROM device name"	String	Name of CD-ROM device.
49	Network path	"Network path,..."	String	Shared information: name of network patch. Corresponding to drive information. Can specify many.
50	Name of network provider	"Name of network provider,..."	String	Shared information: name of network provider.

No.	Item	Item data format	Item type	Remarks
				Corresponding to drive information. Can specify many.
51	Drive name	"Drive name,..."	String	Shared information: name of network drive. Corresponding to drive information. Can specify many.
52	Memory device locator	"Memory device locator,..."	String	Memory information: name of memory device locator. Can specify many.
53	Memory size	"Memory size,..."	Number	Memory information: Memory size of memory device localizer. Unit: KiloByte Corresponding to memory device localizer. Can specify many.
54	Name of disk vendor	"Name of disk vendor"	String	Disk information: manufacturer of hard disk.
55	Name of disk type	"Name of disk type"	String	Disk information: type of hard disk (type).
56	Disk capacity	"Disk capacity"	Number	Disk information: hard disk capacity. Unit: KiloByte
57	Disk IF	"Disk IF"	String	Disk information: I/F specification of hard disk.
58	Disk description	"Disk description"	String	Disk information: explanation about hard disk.

Name of drive type (*1)

Drive type	Value of drive type
Floppy disk	Floppy disk
Hard disk	Hard disk drive
CD-ROM	CD-ROM drive
RAM	RAM drive
Removable	Removable drive

Drive type	Value of drive type
Network	Network drive
Unknown	Unknown

OS name (*2)

OS	Value of OS name
Microsoft(R) Windows Vista(R) Home Basic	Windows Vista Home Basic
Microsoft(R) Windows Vista(R) Home Premium	Windows Vista Home Premium
Microsoft(R) Windows Vista(R) Business	Windows Vista Business
Microsoft(R) Windows Vista(R) Enterprise	Windows Vista Enterprise
Microsoft(R) Windows Vista(R) Ultimate	Windows Vista Ultimate
Microsoft(R) Windows Vista(R) Home Basic 64bit version	Windows Vista Home Basic (x64)
Microsoft(R) Windows Vista(R) Home Premium 64bit version	Windows Vista Home Premium (x64)
Microsoft(R) Windows Vista(R) Business 64bit version	Windows Vista Business (x64)
Microsoft(R) Windows Vista(R) Enterprise 64bit version	Windows Vista Enterprise (x64)
Microsoft(R) Windows Vista(R) Ultimate 64bit version	Windows Vista Ultimate (x64)
Windows Server(R) 2008 Standard	Windows Server 2008 Standard
Windows Server(R) 2008 Standard without Hyper-V	Windows Server 2008 Standard without Hyper-V
Windows Server(R) 2008 Enterprise	Windows Server 2008 Enterprise
Windows Server(R) 2008 Enterprise without Hyper-V	Windows Server 2008 Enterprise without Hyper-V
Windows Server(R) 2008 Datacenter	Windows Server 2008 Datacenter
Windows Server(R) 2008 Datacenter without Hyper-V	Windows Server 2008 Datacenter without Hyper-V
Windows(R) Web Server 2008	Windows Web Server 2008
Windows Server(R) 2008 Standard 64bit version	Windows Server 2008 Standard (x64)
Windows Server(R) 2008 Standard without Hyper-V 64bit version	Windows Server 2008 Standard without Hyper-V (x64)
Windows Server(R) 2008 Enterprise 64bit version	Windows Server 2008 Enterprise (x64)
Windows Server(R) 2008 Enterprise without Hyper-V 64bit version	Windows Server 2008 Enterprise without Hyper-V (x64)
Windows Server(R) 2008 Datacenter 64bit version	Windows Server 2008 Datacenter (x64)
Windows Server(R) 2008 Datacenter without Hyper-V 64bit version	Windows Server 2008 Datacenter without Hyper-V (x64)
Windows(R) Web Server 2008 64bit version	Windows Web Server 2008 (x64)
Windows(R) 7 Starter	Windows 7 Starter
Windows(R) 7 Home Premium	Windows 7 Home Premium
Windows(R) 7 Professional	Windows 7 Professional
Windows(R) 7 Ultimate	Windows 7 Ultimate
Windows(R) 7 Enterprise	Windows 7 Enterprise
Windows(R) 7 Home Premium 64bit version	Windows 7 Home Premium (x64)

OS	Value of OS name
Windows(R) 7 Professional 64bit version	Windows 7 Professional (x64)
Windows(R) 7 Ultimate 64bit version	Windows 7 Ultimate (x64)
Windows(R) 7 Enterprise 64bit version	Windows 7 Enterprise (x64)
Windows(R) 8	Windows 8
Windows(R) 8 Pro	Windows 8 Pro
Windows(R) 8 Enterprise	Windows 8 Enterprise
Windows(R) 8 64bit version	Windows 8 (x64)
Windows(R) 8 Pro 64bit version	Windows 8 Pro (x64)
Windows(R) 8 Enterprise 64bit version	Windows 8 Enterprise (x64)
Windows Server(R) 2012 Standard	Windows Server 2012 Standard
Windows Server(R) 2012 Essentials	Windows Server 2012 Essentials
Windows Server(R) 2012 Foundation	Windows Server 2012 Foundation
Windows Server(R) 2012 Datacenter	Windows Server 2012 Datacenter

Software information (retrieve file)

All software units compose 1 piece of information.

No.	Item	Item data format	Item type	Remarks
0	Client key (required)	"Identification name of client"	String	Only key to identify client.
1	File name (lowest limit required)	"File name"	String	File name and directory name to be searched.
2	File size	"File size"	Number	Unit: Byte
3	Update date	"YYYYMMDDhhmm"	Number	Date of file update (YYYYMMDDhhmm) Half-with 12bit.
4	Program name	"Dictionary code"	String	Software code of software dictionary. Data saved only when in use.

Software information (retrieve procedure name)

All software units compose 1 piece of information.

No.	Item	Item data format	Item type	Remarks
0	Client key (required)	"Identification name of client"	String	Only key to identify client.
1	Procedure name(lowest limit required)	"Program name"	String	Program name in Control Panel option **Add or Remove Programs** or

No.	Item	Item data format	Item type	Remarks
				Programs > **Programs and Features** (depending on the Windows version).

Software information (retrieve any key and value)

No.	Item	Item data format	Item type	Remarks
0	Client key (required)	"Identification name of client"	String	Only key to identify client.
1	Search key (lowest limit required)	"Registry key"	String	Key of retrieval object.
2	Name of search key	"Name of registry key"	String	Name of key of retrieval object.
3	Value of search key name	"Value of name of registry key"	String	Value of name of retrieval object key.

User information

All client units compose 1 piece of information. Any information in 1-10 can be stored in user information.

No.	Item	Item data format	Item type	Remarks
0	Client key (required)	"Identification name of client"	String	Only key to identify client.
1	User information 1	"Item name, content (value)"	"String, String"	Item name, any content.
2	User information 2	"Item name, content (value)"	"String, String"	Same as above
3	User information 3	"Item name, content (value)"	"String, String"	Same as above
4	User information 4	"Item name, content (value)"	"String, String"	Same as above
5	User information 5	"Item name, content (value)"	"String, String"	Same as above
6	User information 6	"Item name, content (value)"	"String, String"	Same as above
7	User information 7	"Item name, content (value)"	"String, String"	Same as above
8	User information 8	"Item name, content (value)"	"String, String"	Same as above
9	User information 9	"Item name, content (value)"	"String, String"	Same as above
10	User information 10	"Item name, content (value)"	"String, String"	Same as above

Software operation status

All client units compose 1 piece of information.

No.	Item	Item data format	Item type	Remarks
0	Client key(mandatory)	"Identification name of client"	String	Only key to identify client.
1	Name of operating file(lowest limit needed)	File name	String	File name of procedure operation.
2	"Reserved area"	-	-	Set null(same as ",,")
3	"Reserved area"	-	-	Set null(same as ",,")
4	Date of startup(lowest limit needed)	YYYY/MM/DD	Date and Time	Date of procedure startup.
5	"Reserved area"	-	-	Set null(same as ",,")
6	"Reserved area"	-	-	Set null(same as ",,")
7	"Reserved area"	-	-	Set null(same as ",,")
8	"Reserved area"	-	-	Set null(same as ",,")
9	Number of startups(lowest limit needed)	n	Number	Number of procedure startup times.
10	"Reserved area"	-	-	Set null(same as ",,")
11	"Reserved area"	-	-	Set null(same as ",,")
12	"Reserved area"	-	-	Set null(same as ",,")
13	"Reserved area"	-	-	Set null(same as ",,")
14	"Reserved area"	-	-	Set null(same as ",,")
15	"Reserved area"	-	-	Set null(same as ",,")
16	"Reserved area"	-	-	Set null(same as ",,")
17	"Reserved area"	-	-	Set null(same as ",,")
18	"Reserved area"	-	-	Set null(same as ",,")
19	"Reserved area"	-	-	Set null(same as ",,")
20	"Reserved area"	-	-	Set null(same as ",,")
21	"Reserved area"	-	-	Set null(same as ",,")
22	"Reserved area"	-	-	Set null(same as ",,")
23	"Reserved area"	-	-	Set null(same as ",,")

Example)

```
10001+USER01+PC1,LPLS153.EXE,,,2007/04/01,,,,,1,,,,,,,,,,,,,
10002+USER02+PC2,LPLS153.EXE,,,2007/04/02,,,,,2,,,,,,,,,,,,,
10003+USER03+PC3,LPLS153.EXE,,,2007/03/01,,,,,1,,,,,,,,,,,,,
```

Registration to Systemwalker Desktop Patrol

Register the created CSV format file to Systemwalker Desktop Patrol.

Take the following steps.

1. Set up the file of Inventory information registration.

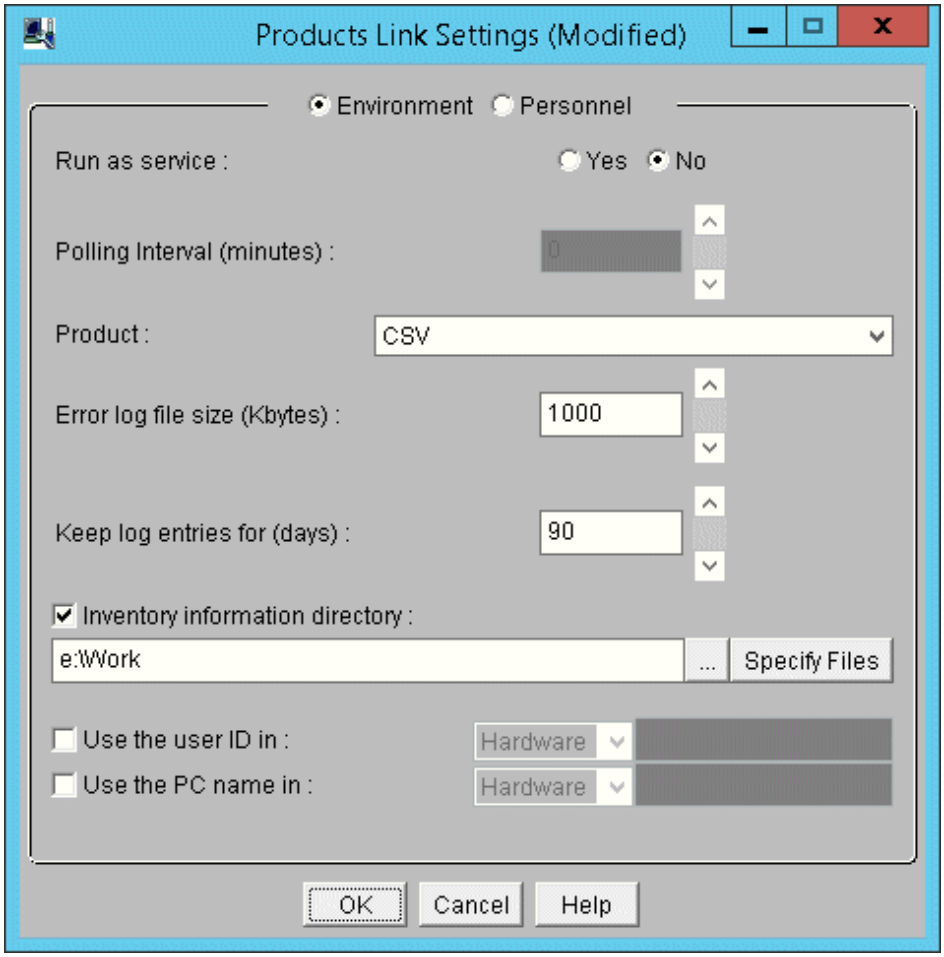
   - Registration to CS

     Select **Start** > **Procedure** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Link with Other Products - Environment Setup**, or **Apps** > **Systemwalker Desktop Patrol** > **Products Link Settings**.

   - Registration to DS

     Double-click "iisSettings.exe" in "DTP installation directory\FJSVsbiis\bin".

   The window of **Products Link Settings** will be displayed.



2. Enter the following information, Click the **OK** button.

   In addition, refer to "14.2.1 Inventory Information Collection with Systemwalker Centric Manager" for other information.

   - Select **Yes** or **No** from the single choice button of **Run as service**.

     When **Yes** is selected

     The Inventory information will be automatically collect according to polling interval.

     When **No** is selected

     Use command prompt to execute the following command for the file of Inventory information export. Input the parameter of "CSV".

     ```
     DTP Installation directory\FJSVsbiis\bin\InvSend.exe CSV
     ```

   - Select **CSV** in drop-down list of **product**.

   - Enter path of the CSV format file created in the textbox of **Inventory information directory** (need to specify file name).

- For **Use the User ID in**, set random information in the hardware information and user information of the collected Inventory information.
- For **Use the PC Name**, set random information in the hardware information and user information of the collected Inventory information.

14.3 Import to Asset Ledger

The CSV file of Inventory information output from other products can be imported directly to the asset ledger of Systemwalker Desktop Patrol for application.

In addition, only the machine's information can be registered from Inventory information of other products.

Template editing

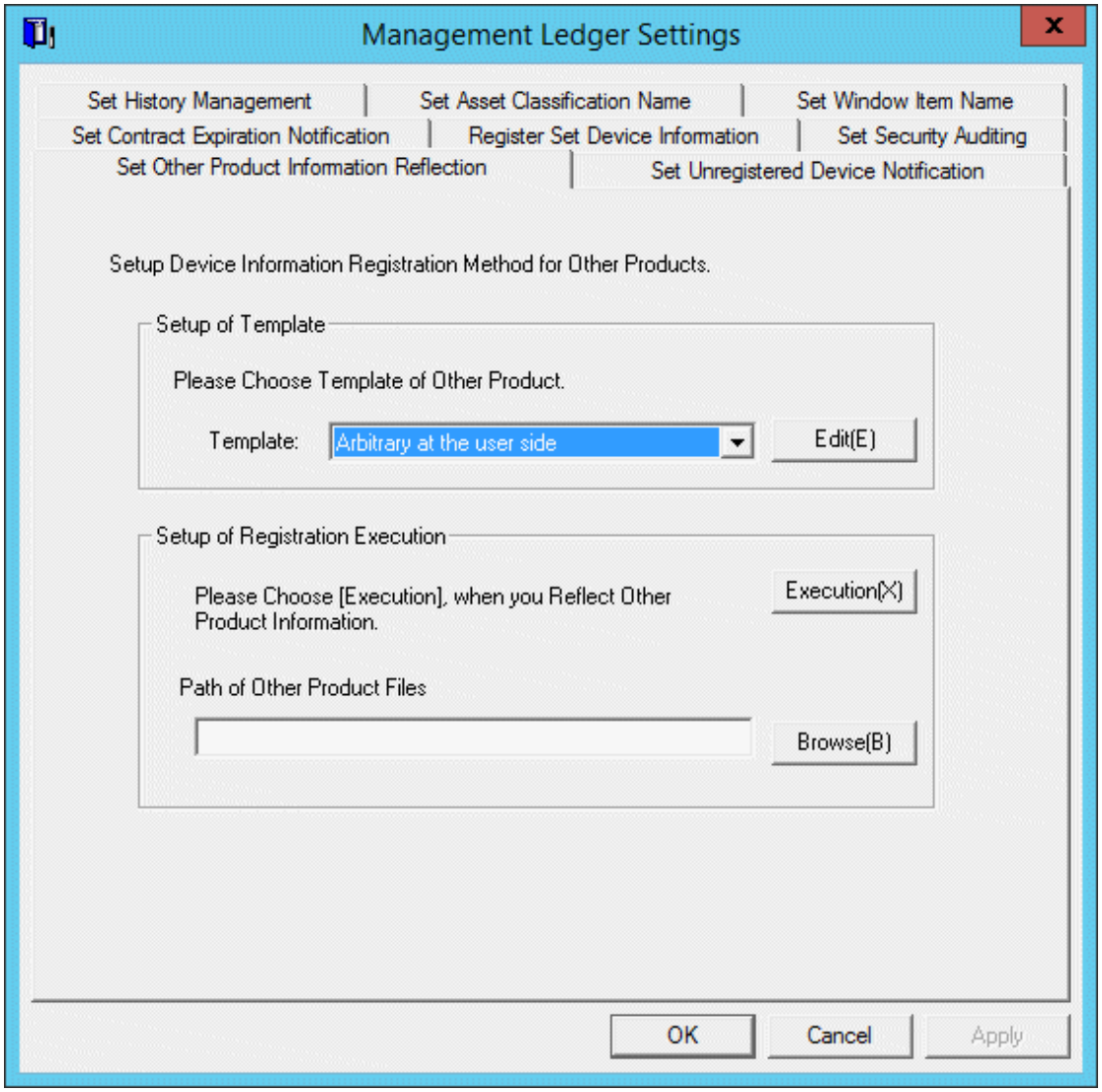
Take the following steps.

1. In CS, select **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

   The **Managed Ledger Settings** window will be displayed.

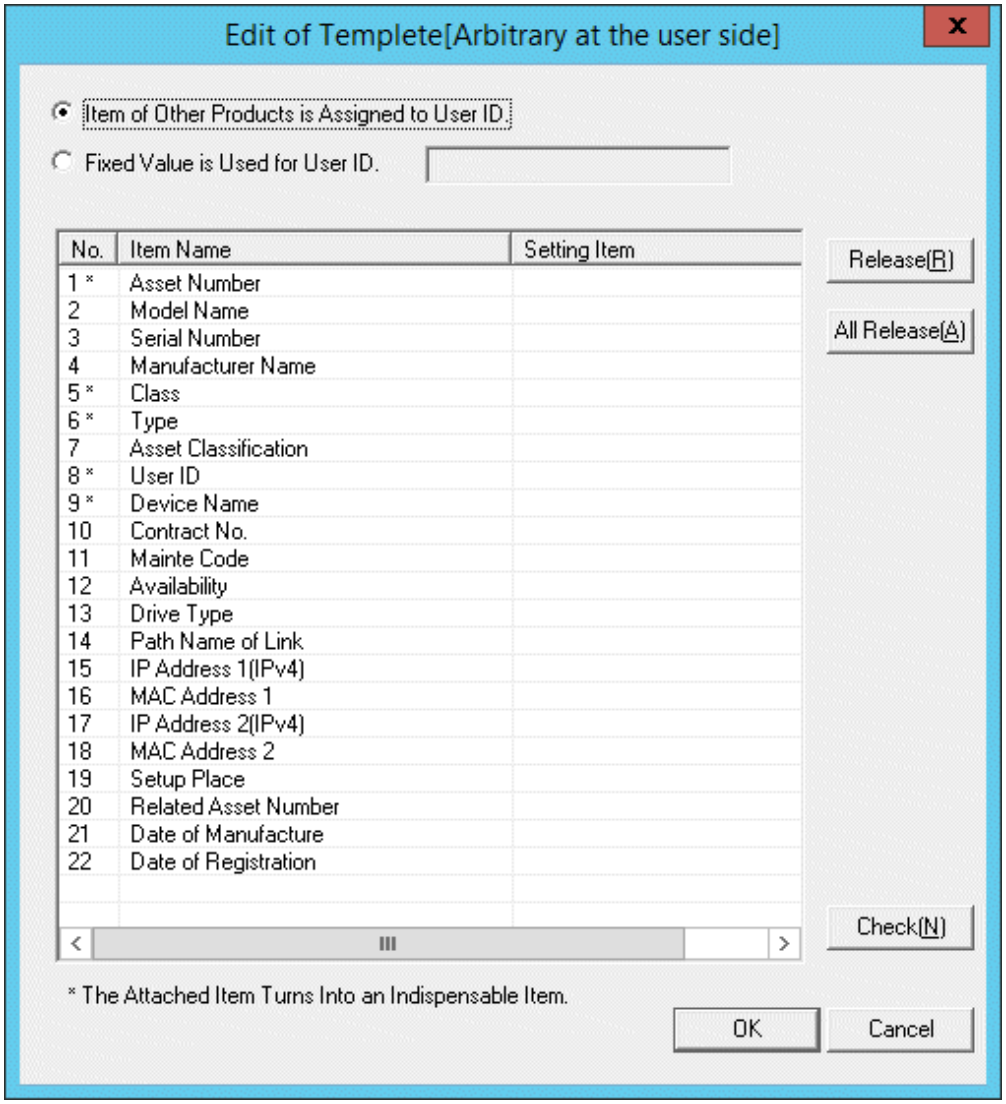
2. Click the **Set Other Product Information Reflection** tab.

   The following window will be displayed.



3. Select the template of other product to be linked, click the **Edit** button.

   The following window will be displayed.

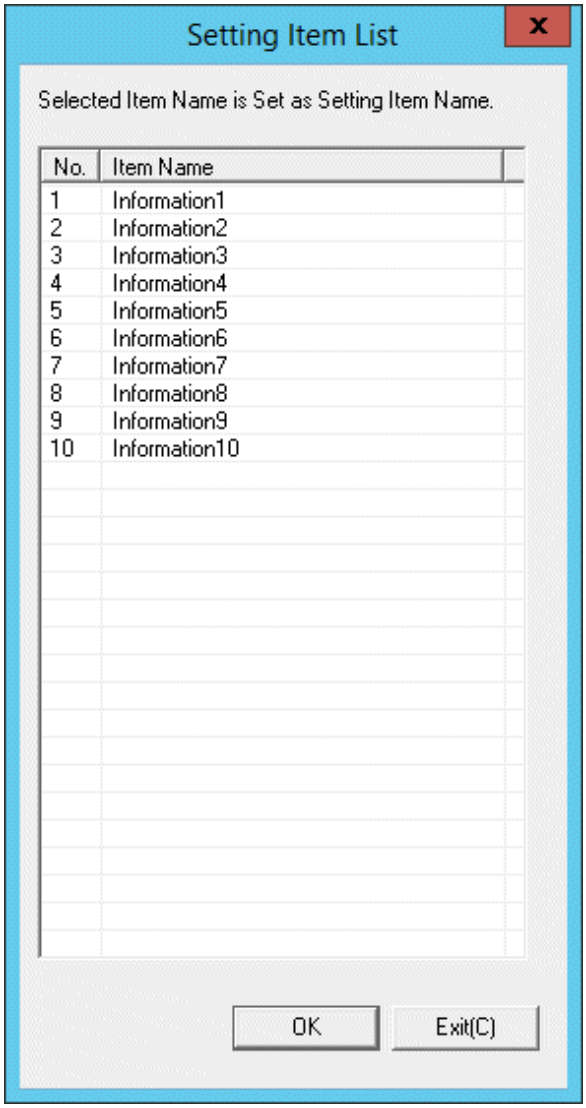


4. Select the Item of Other Products is Assigned to User ID, or use fixed value.

   When fixed value is used, it's necessary to specify the user ID registered in the designated master data.

5. Select item name from the list.

   Item list of CSV file output from other products will be displayed.



   The item name displayed here is to display the item of standard output contents of each product. To change CSV export contents and sequence and etc of each product, first change the following file to be consistent with this CSV output contents, then execute.

   a. The editing window to be displayed on notepad and other for the item definition file of CSV file of each product.

      File name: "DTP Installation target folder\DTPA\Conv_NameList.dat"

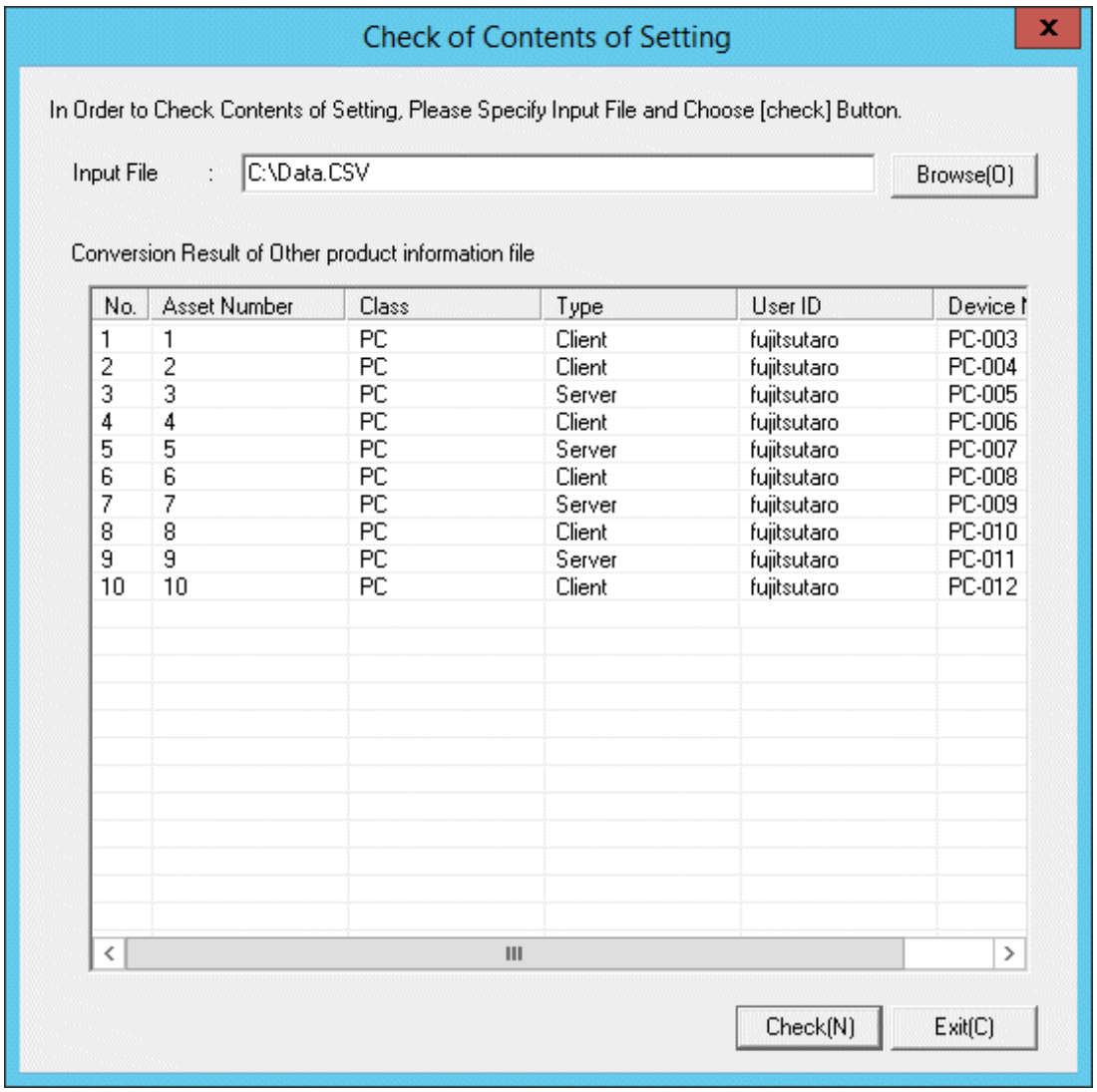
   b. All the corresponding products to be saved as record separated by comma. As to the object's product line, name will be recorded corresponding to the actual item name starting the 4th project.

   c. Cover and save this file after modification.

      In addition, item of random settings exists in the line 4, this value can be modified.

6. Select item name of other product corresponding to the item name selected from the list in the **Edit of Template** window, click the **OK** button.

7. In the **Edit of Template** window, click the **Check** button. The following window will be displayed.



8. Specify path of the CSV file output from other product in **Input file** and click the **Check** button. The file change result will appear below the window.
9. Click the **Close** button.
10. Click the **Apply** button in the window of **Management Ledger Settings**.

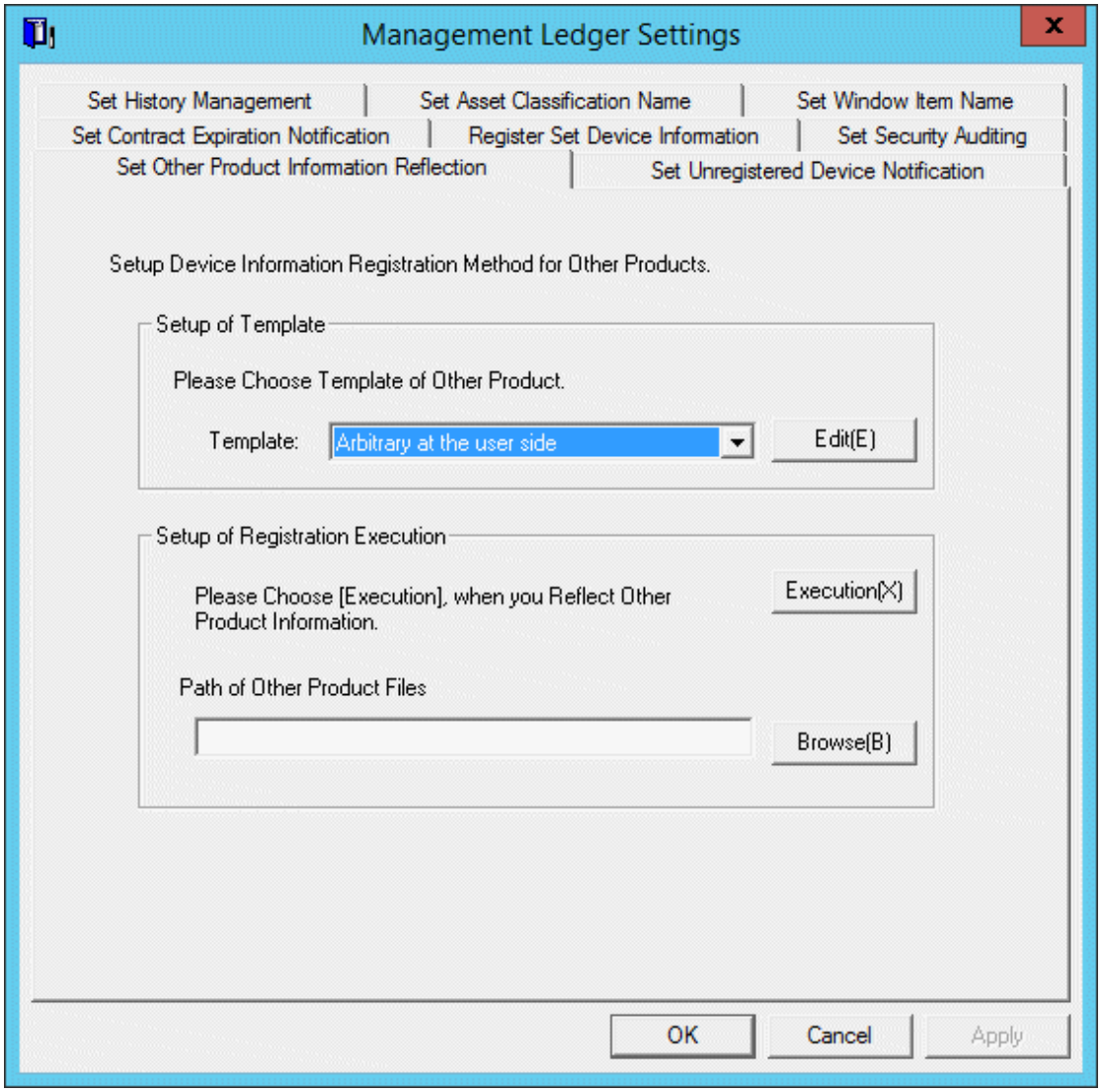
Import operation

Take the following steps.

1. In CS, select **Start** > **Procedure** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Managed Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol** > **Management Ledger Settings**.

2. Click the tab of **Set Other Product Information Reflection**.

   The following window will be displayed.



3. Select a Template.
4. Specify path of the CSV file output from other product in the path of information file of other product.
5. Click the **Execution** button, other product information will be reflected in the asset ledger.